计算机网络 HTTP 实验报告

姓名：陈鹤影　　　　学号：PB21061287　　　　日期：2022.9.18

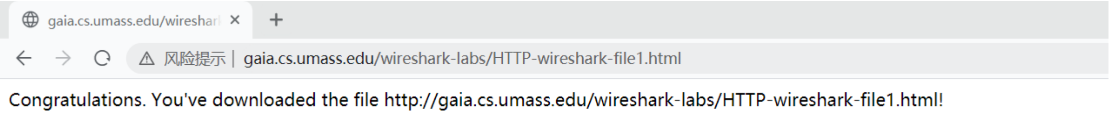
一、　实验目的：

1. 巩固 Wireshark 的使用方法
2. 通过嗅探实验了解条件 GET/response 交互，分析 HTTP 报文格式，检索大型 HTML 文件，检索嵌入网页对象以及了解 HTTP 身份验证和安全性。

二、　实验流程及问题回答：

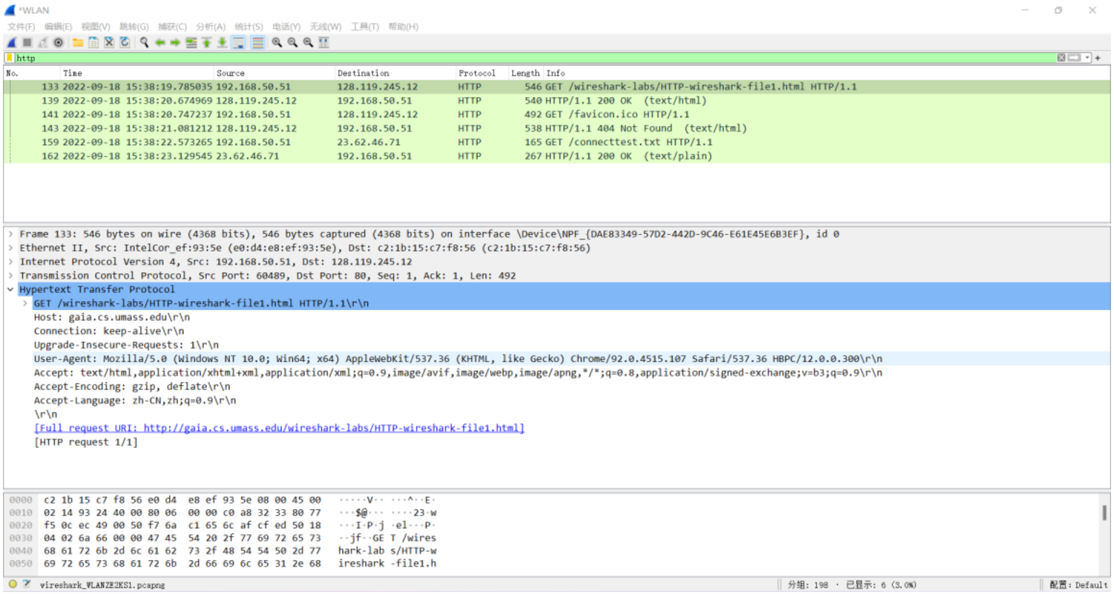
Step 1：The Basic HTTP GET/response interaction

打开浏览器和 Wireshark，并选择 http 过滤模式。等待一定时间，开启抓包。登入 http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html 网站，当 HTML 文件显示成功后，停止抓包。显示如下：


gaia.cs.umass.edu/wireshar
风险提示 | gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!

（图 1-1 HTML 文件显示界面）


*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) 帮助(H)

```
http
```

```
No.    Time                       Source          Destination     Protocol Length Info
   133 2022-09-18 15:38:19.785035 192.168.50.51   128.119.245.12  HTTP      546 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   139 2022-09-18 15:38:20.674969 128.119.245.12  192.168.50.51   HTTP      540 HTTP/1.1 200 OK  (text/html)
   141 2022-09-18 15:38:20.747237 192.168.50.51   128.119.245.12  HTTP      492 GET /favicon.ico HTTP/1.1
   143 2022-09-18 15:38:21.081212 128.119.245.12  192.168.50.51   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
   159 2022-09-18 15:38:22.573265 192.168.50.51   23.62.46.71     HTTP      165 GET /connecttest.txt HTTP/1.1
   162 2022-09-18 15:38:23.129545 23.62.46.71     192.168.50.51   HTTP      267 HTTP/1.1 200 OK  (text/plain)
```

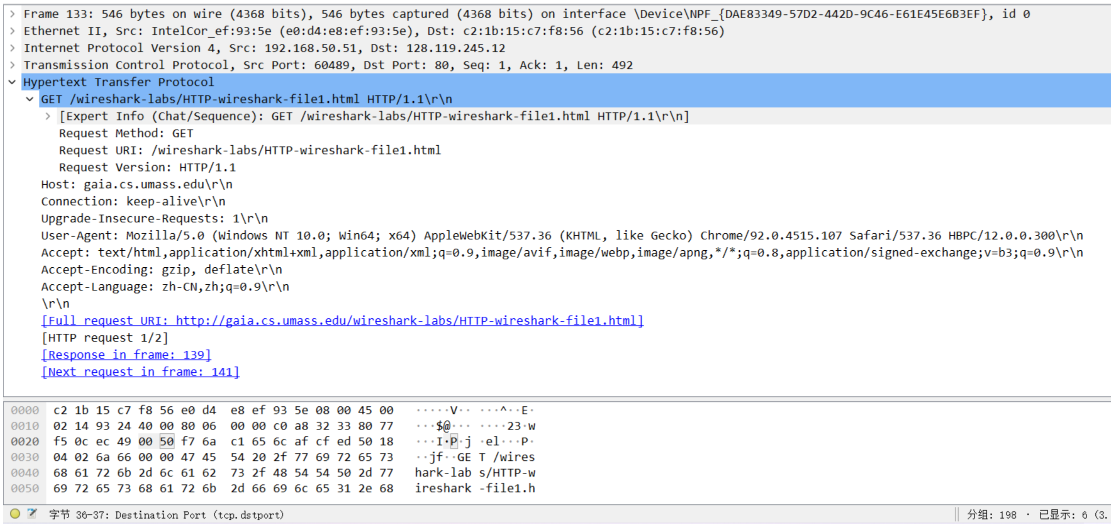
```
> Frame 133: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60489, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
v 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/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
```

```
0000  c2 1b 15 c7 f8 56 e0 d4  e8 ef 93 5e 08 00 45 00   ·····V·· ···^··E·
0010  02 14 93 24 40 00 80 06  00 00 c0 a8 32 33 80 77   ···$@··· ····23·w
0020  f5 0c ec 49 00 50 f7 6a  c1 65 6c af cf ed 50 18   ···I·P·j ·el···P·
0030  04 02 6a 66 00 00 47 45  54 20 2f 77 69 72 65 73   ··jf··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 31 2e 68   ireshark -file1.h
```

（图 1-2 Wireshark 抓包显示界面）

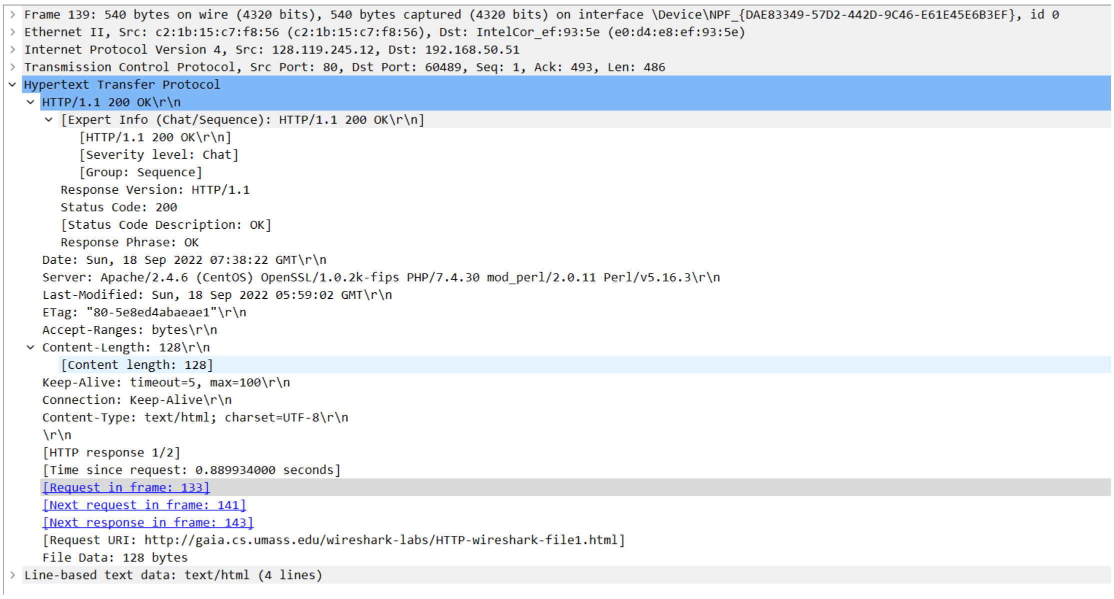
其中成功观察到浏览器向服务器请求对应 HTML 文件，服务器返回 OK 报文。

报文内容如下：



```
> Frame 133: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60489, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 139]
    [Next request in frame: 141]

0000  c2 1b 15 c7 f8 56 e0 d4  e8 ef 93 5e 08 00 45 00   ·····V·· ···^··E·
0010  02 14 93 24 40 00 80 06  00 00 c0 a8 32 33 80 77   ···$@··· ····23·w
0020  f5 0c ec 49 00 50 f7 6a  c1 65 6c af cf ed 50 18   ···I·P·j ·el···P·
0030  04 02 6a 66 00 00 47 45  54 20 2f 77 69 72 65 73   ··jf··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 31 2e 68   ireshark -file1.h

字节 36-37: Destination Port (tcp.dstport)        分组: 198 · 已显示: 6 (3.
```

（图 1-3 GET 请求报文）



```
> Frame 139: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.50.51
> Transmission Control Protocol, Src Port: 80, Dst Port: 60489, Seq: 1, Ack: 493, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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: Sun, 18 Sep 2022 07:38:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 18 Sep 2022 05:59:02 GMT\r\n
    ETag: "80-5e8ed4abaeae1"\r\n
    Accept-Ranges: bytes\r\n
  v 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 1/2]
    [Time since request: 0.889934000 seconds]
    [Request in frame: 133]
    [Next request in frame: 141]
    [Next response in frame: 143]
    [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)
```

（图 1-4 OK 响应报文）

Q&A：(具体位置见图 1-5、1-6)

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

Ans： browser HTTP version ： 1.1 。

sever HTTP version ： 1.1 。

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

Ans： 可以接受简体中文，即 zh-CN,zh(华语区-中国大陆)。

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

Ans： my IP: 192.168.50.51。

sever IP:128.119.245.12。

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

Ans： 200（代表 OK）。

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

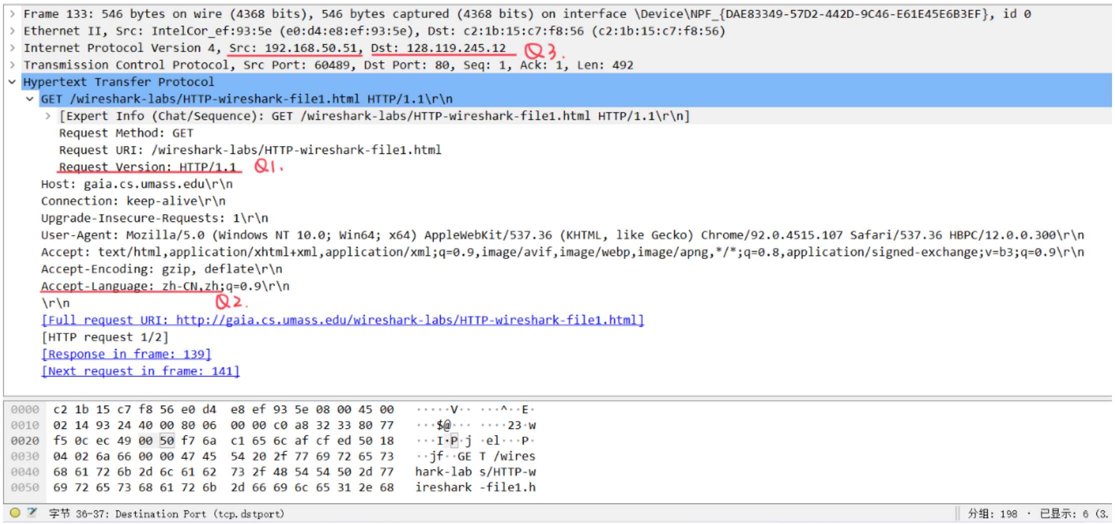
Ans： Sun, 18 Sep 2022 05:59:02 GMT。

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

Ans： 128 bytes。

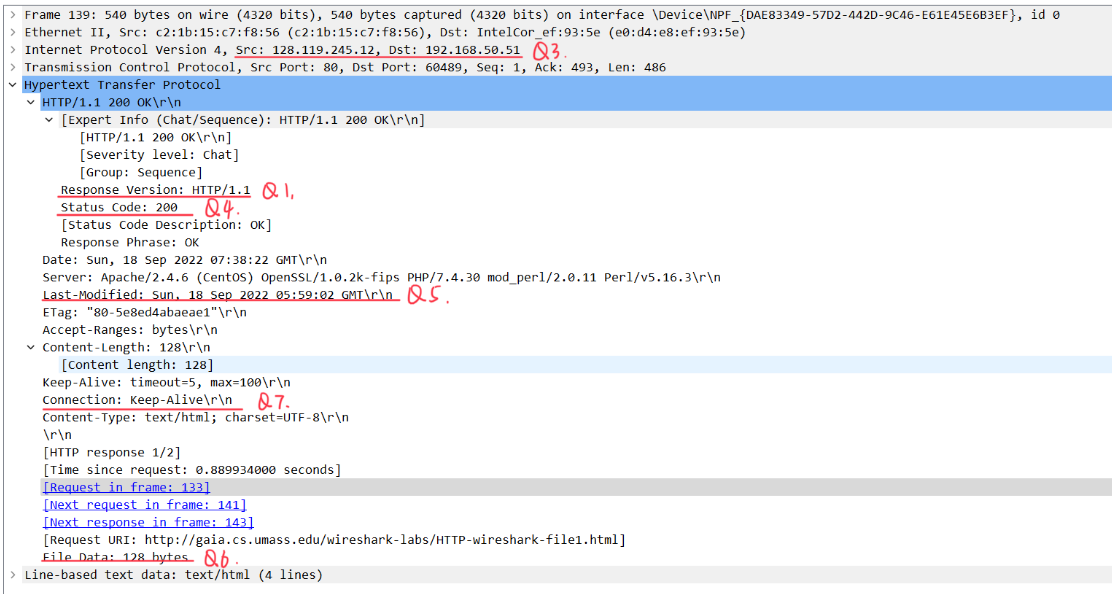
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Ans： 例如 Connection 字段。



```
> Frame 133: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12  Q3.
> Transmission Control Protocol, Src Port: 60489, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1  Q1.
    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/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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
    \r\n                         Q2.
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 139]
    [Next request in frame: 141]

0000  c2 1b 15 c7 f8 56 e0 d4  e8 ef 93 5e 08 00 45 00   ·····V·· ···^··E·
0010  02 14 93 24 40 00 80 06  00 00 c0 a8 32 33 80 77   ···$@··· ····23·w
0020  f5 0c ec 49 00 50 f7 6a  c1 65 6c af cf ed 50 18   ···I·P·j ·el···P·
0030  04 02 6a 66 00 00 47 45  54 20 2f 77 69 72 65 73   ··jf··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 31 2e 68   ireshark -file1.h

字节 36-37: Destination Port (tcp.dstport)        分组: 198 · 已显示: 6 (3.
```

（图 1-5 GET 请求报文标记）

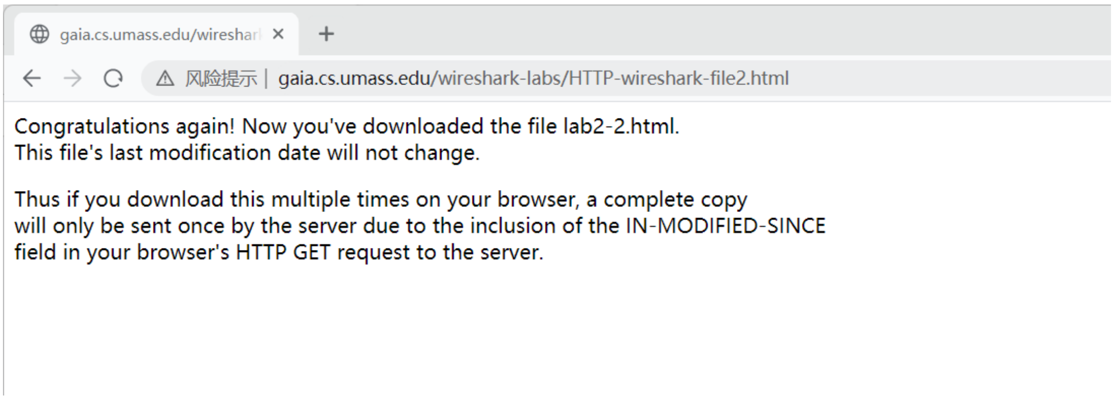


```
> Frame 139: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.50.51  Q3.
> Transmission Control Protocol, Src Port: 80, Dst Port: 60489, Seq: 1, Ack: 493, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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  Q1.
      Status Code: 200  Q4.
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Sun, 18 Sep 2022 07:38:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 18 Sep 2022 05:59:02 GMT\r\n  Q5.
    ETag: "80-5e8ed4abaeae1"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 128\r\n
      [Content length: 128]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n  Q7.
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.889934000 seconds]
    [Request in frame: 133]
    [Next request in frame: 141]
    [Next response in frame: 143]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes  Q6.
> Line-based text data: text/html (4 lines)
```

（图 1-6 OK 响应报文标记）

Step 2：The HTTP CONDITIONAL GET/response interaction

清除浏览器缓存（这里选用华为浏览器），操作步骤如下：选择历史记录->清除缓存。打开 Wireshark 抓包并登入以下 URL：http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html 。观察到如下界面：

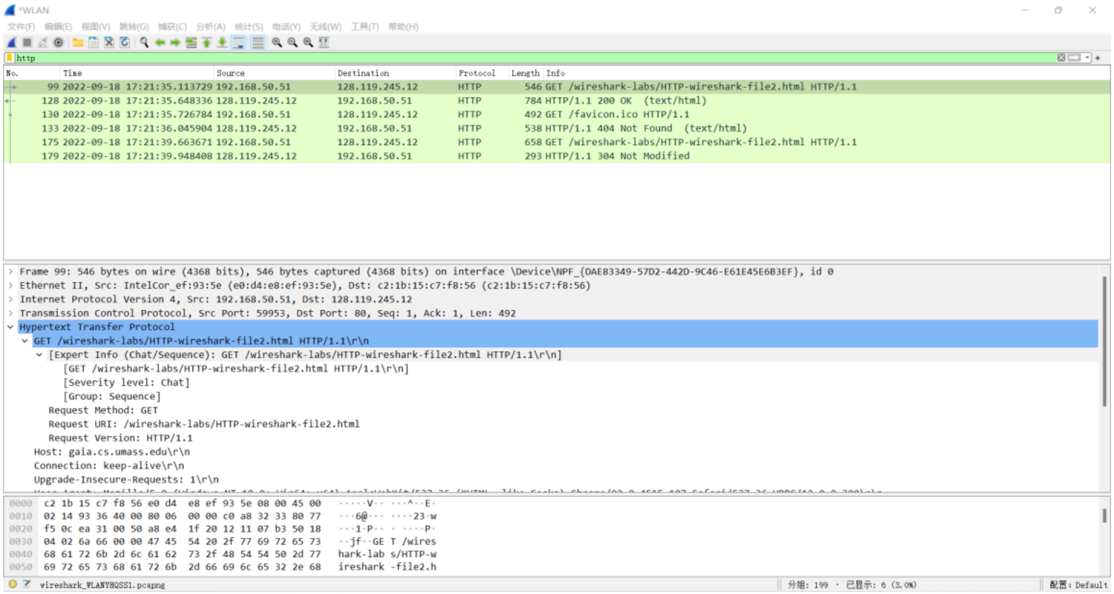

gaia.cs.umass.edu/wireshar
风险提示 | gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

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

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

（图 1-7 登入界面）

在短时间内再次登入上述 URL（或直接刷新）（实验过程中选择 http 过滤），Wireshark 抓包结果如图 1-8。


*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) 帮助(H)
http

```
No.    Time                       Source          Destination     Protocol  Length Info
    99 2022-09-18 17:21:35.113729 192.168.50.51   128.119.245.12  HTTP       546 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   128 2022-09-18 17:21:35.648336 128.119.245.12  192.168.50.51   HTTP       784 HTTP/1.1 200 OK  (text/html)
   130 2022-09-18 17:21:35.726784 192.168.50.51   128.119.245.12  HTTP       492 GET /favicon.ico HTTP/1.1
   133 2022-09-18 17:21:36.045904 128.119.245.12  192.168.50.51   HTTP       538 HTTP/1.1 404 Not Found  (text/html)
   175 2022-09-18 17:21:39.663671 192.168.50.51   128.119.245.12  HTTP       658 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   179 2022-09-18 17:21:39.948408 128.119.245.12  192.168.50.51   HTTP       293 HTTP/1.1 304 Not Modified
```

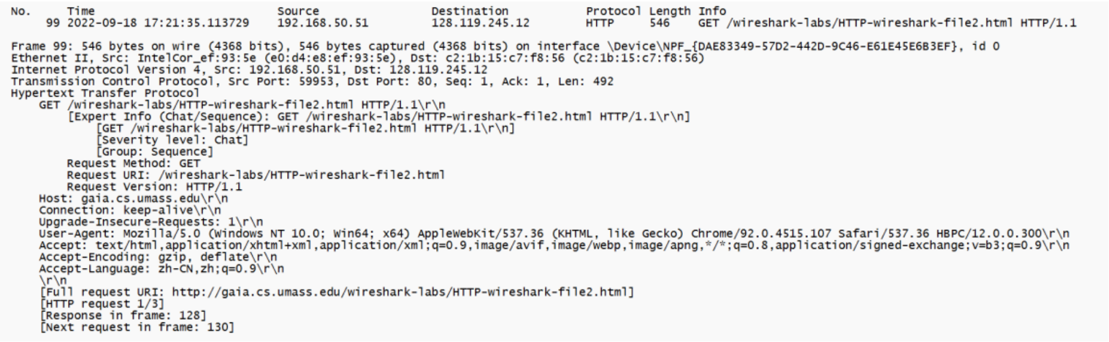
```
> Frame 99: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59953, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

```
0000  c2 1b 15 c7 f8 56 e0 d4  e8 ef 93 5e 08 00 45 00   ·····V·· ···^··E·
0010  02 14 93 36 40 00 80 06  00 00 c0 a8 32 33 80 77   ···6@··· ····23·w
0020  f5 0c ea 31 00 50 a8 e4  1f 20 12 11 07 b3 50 18   ···1·P·· · ····P·
0030  04 02 6a 66 00 00 47 45  54 20 2f 77 69 72 65 73   ··jf··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 32 2e 68   ireshark -file2.h
```

wireshark_WLANYHQSS1.pcapng　分组: 199 · 已显示: 6 (3.0%)　配置: Default

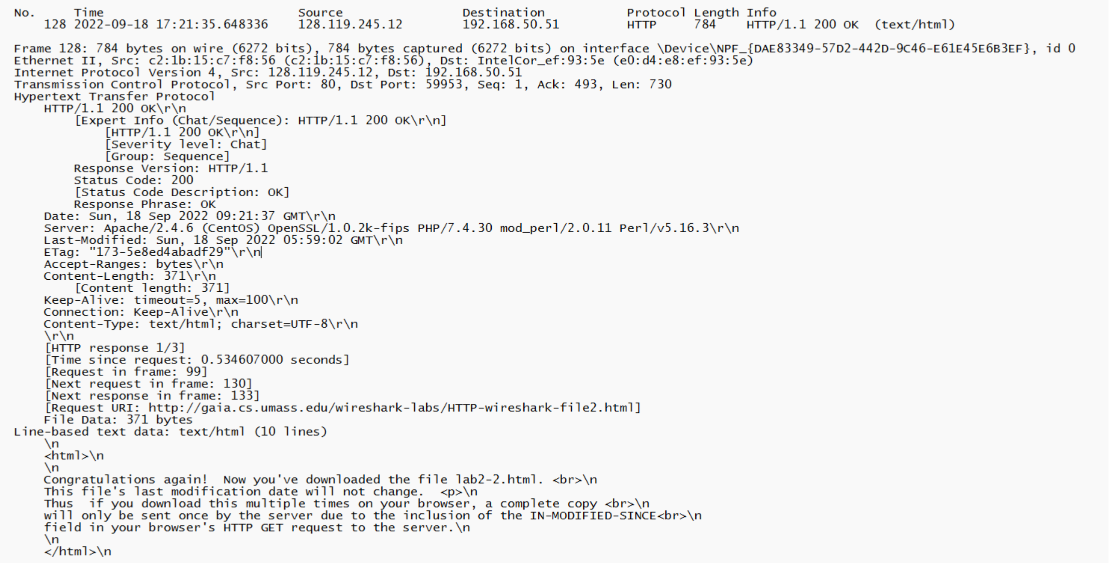
（图 1-8 Wireshark 抓包结果）

报文打印如下：



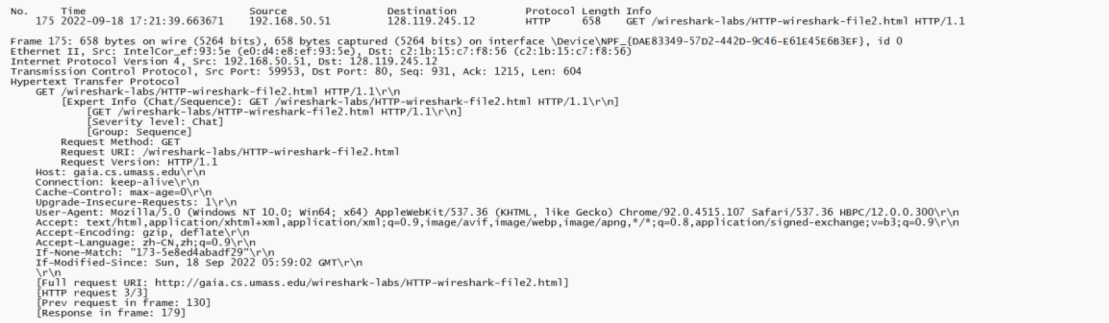
```
No.     Time                       Source                Destination           Protocol Length Info
     99 2022-09-18 17:21:35.113729 192.168.50.51         128.119.245.12        HTTP     546    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 99: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59953, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
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]
            [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/3]
    [Response in frame: 128]
    [Next request in frame: 130]
```

（图 1-9 第一次 GET 报文）



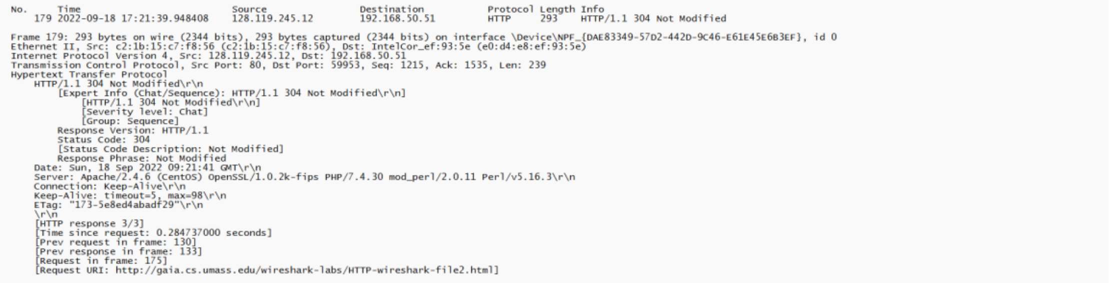
```
No.     Time                          Source                Destination           Protocol Length Info
    128 2022-09-18 17:21:35.648336    128.119.245.12        192.168.50.51         HTTP     784    HTTP/1.1 200 OK  (text/html)

Frame 128: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.50.51
Transmission Control Protocol, Src Port: 80, Dst Port: 59953, Seq: 1, Ack: 493, Len: 730
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: Sun, 18 Sep 2022 09:21:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 18 Sep 2022 05:59:02 GMT\r\n
    ETag: "173-5e8ed4abadf29"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
        [Content length: 371]
    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 1/3]
    [Time since request: 0.534607000 seconds]
    [Request in frame: 99]
    [Next request in frame: 130]
    [Next response in frame: 133]
    [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)
    \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
```

（图 1-10 第一次 OK 报文）



```
No.     Time                          Source                Destination           Protocol Length Info
    175 2022-09-18 17:21:39.663671    192.168.50.51         128.119.245.12        HTTP     658    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 175: 658 bytes on wire (5264 bits), 658 bytes captured (5264 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59953, Dst Port: 80, Seq: 931, Ack: 1215, Len: 604
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]
            [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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: "173-5e8ed4abadf29"\r\n
    If-Modified-Since: Sun, 18 Sep 2022 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 3/3]
    [Prev request in frame: 130]
    [Response in frame: 179]
```

（图 1-11 第二次 GET 报文）



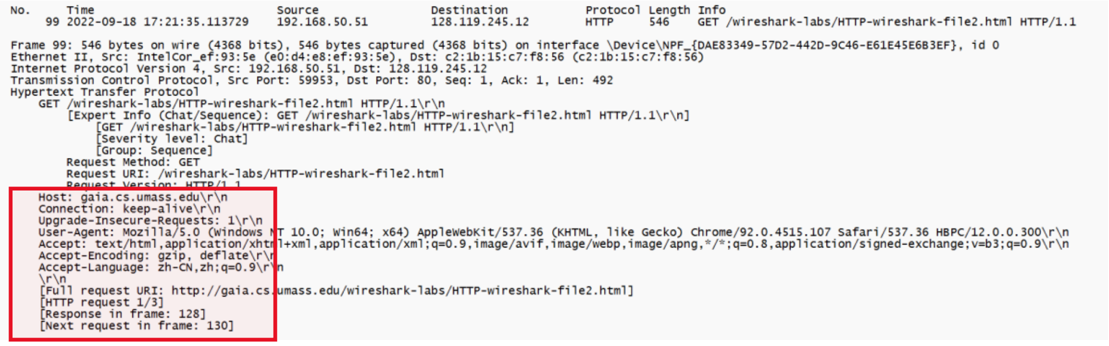
```
No.     Time                          Source                Destination           Protocol Length Info
    179 2022-09-18 17:21:39.948408    128.119.245.12        192.168.50.51         HTTP     293    HTTP/1.1 304 Not Modified

Frame 179: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.50.51
Transmission Control Protocol, Src Port: 80, Dst Port: 59953, Seq: 1215, Ack: 1535, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
            [HTTP/1.1 304 Not Modified\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Sun, 18 Sep 2022 09:21:41 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=98\r\n
    ETag: "173-5e8ed4abadf29"\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.284737000 seconds]
    [Prev request in frame: 130]
    [Prev response in frame: 133]
    [Request in frame: 175]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

（图 1-12 第二次 OK 报文）

Q&A：

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?

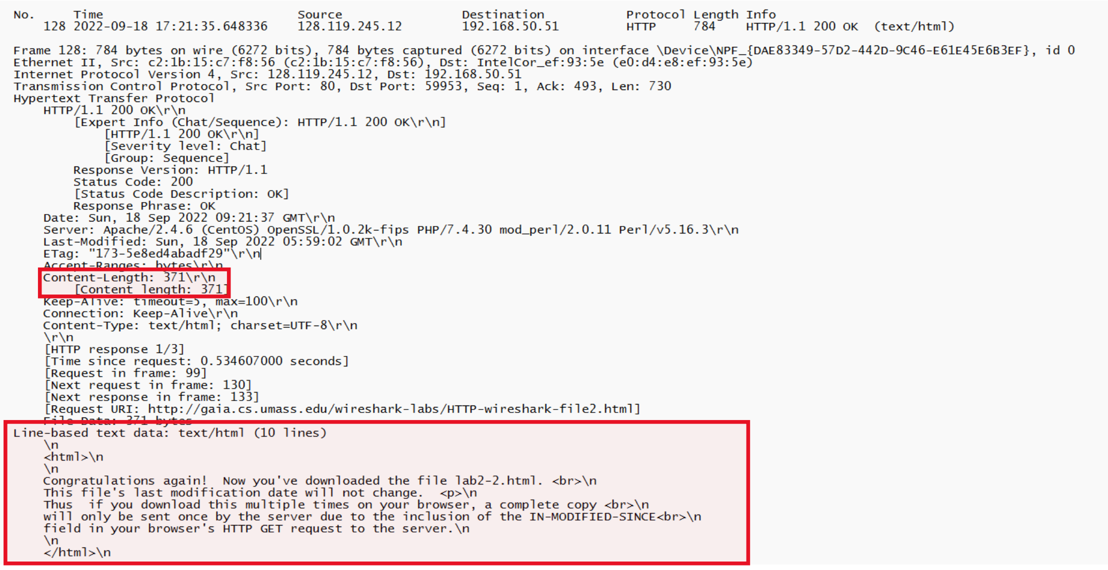
Ans：没有。



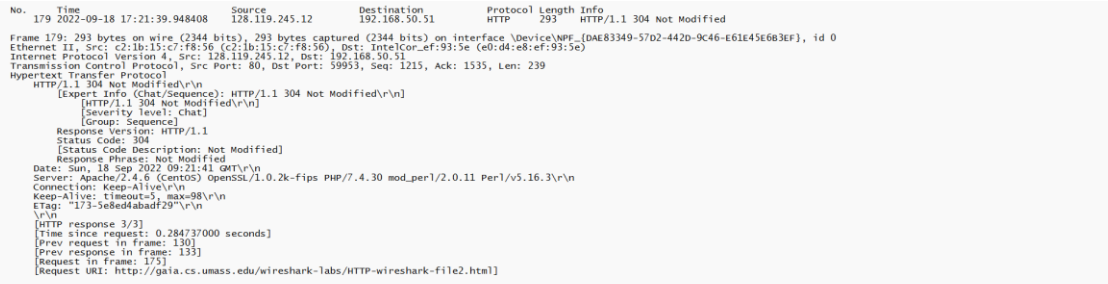
```
No.     Time                          Source                Destination           Protocol Length Info
     99 2022-09-18 17:21:35.113729    192.168.50.51         128.119.245.12        HTTP     546    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 99: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59953, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
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]
            [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/3]
    [Response in frame: 128]
    [Next request in frame: 130]
```

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

Ans：服务器在第一次响应时明确返回了文件内容，在第二次响应时没有。从是否有 Content Length 段和 Line-based text data 段可知。



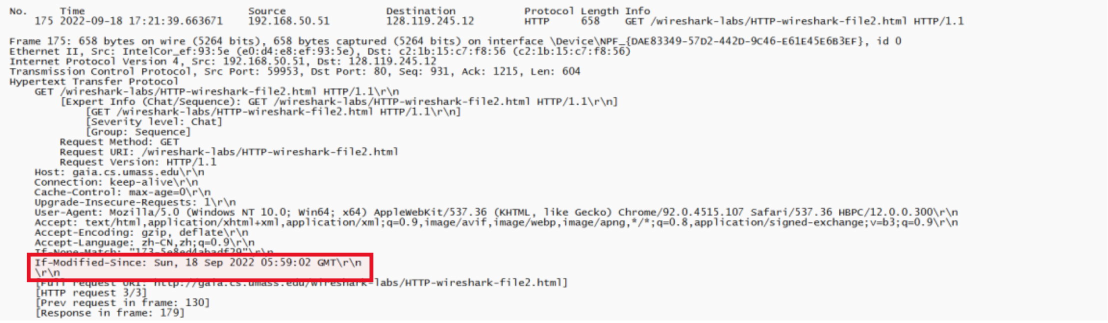
```
No.     Time                          Source                Destination           Protocol Length Info
    128 2022-09-18 17:21:35.648336    128.119.245.12        192.168.50.51         HTTP     784    HTTP/1.1 200 OK  (text/html)

Frame 128: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.50.51
Transmission Control Protocol, Src Port: 80, Dst Port: 59953, Seq: 1, Ack: 493, Len: 730
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: Sun, 18 Sep 2022 09:21:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 18 Sep 2022 05:59:02 GMT\r\n
    ETag: "173-5e8ed4abadf29"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
        [Content length: 371]
    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 1/3]
    [Time since request: 0.534607000 seconds]
    [Request in frame: 99]
    [Next request in frame: 130]
    [Next response in frame: 133]
    [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)
    \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
```



```
No.     Time                          Source                Destination           Protocol Length Info
    179 2022-09-18 17:21:39.948408    128.119.245.12        192.168.50.51         HTTP     293    HTTP/1.1 304 Not Modified

Frame 179: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.50.51
Transmission Control Protocol, Src Port: 80, Dst Port: 59953, Seq: 1215, Ack: 1535, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
            [HTTP/1.1 304 Not Modified\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Sun, 18 Sep 2022 09:21:41 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=98\r\n
    ETag: "173-5e8ed4abadf29"\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.284737000 seconds]
    [Prev request in frame: 130]
    [Prev response in frame: 133]
    [Request in frame: 175]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

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?

Ans： Yes. Following information is ‘Sun, 18 Sep 2022 05：59：02 GMT\r\n’这是第一次响应报文返回的最后修改时间。



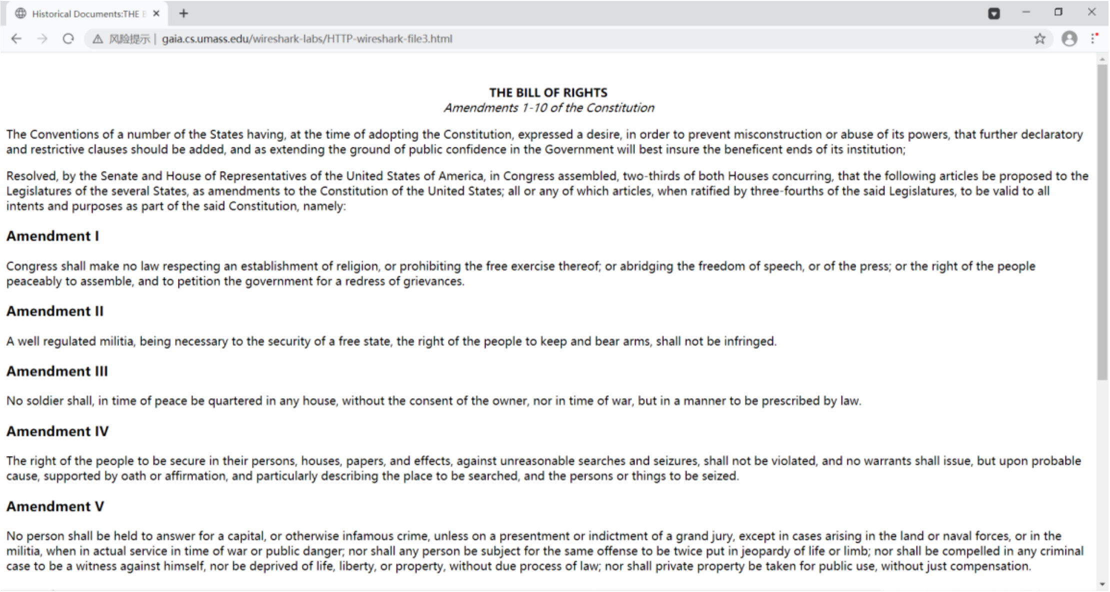
```
No.     Time                          Source                Destination           Protocol Length Info
    175 2022-09-18 17:21:39.663671    192.168.50.51         128.119.245.12        HTTP     658    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 175: 658 bytes on wire (5264 bits), 658 bytes captured (5264 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59953, Dst Port: 80, Seq: 931, Ack: 1215, Len: 604
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]
            [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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: "173-5e8ed4abadf29"\r\n
    If-Modified-Since: Sun, 18 Sep 2022 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 3/3]
    [Prev request in frame: 130]
    [Response in frame: 179]
```

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.

Ans：HTTP status code and phrase：304 Not Modified。服务器没有明确地返回文件内容。因为报文显示从上一次获取文件，文件内容并未修改，由于缓存机制，浏览器可以直接从缓存区域读取文件内容，服务器不用再次发送文件。

Step 3：Retrieving Long Documents

打开浏览器并清除缓存内容，打开 Wireshark 抓包并登入以下 URL：http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html 。观察到如下界面：


Historical Documents:THE
风险提示 | 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

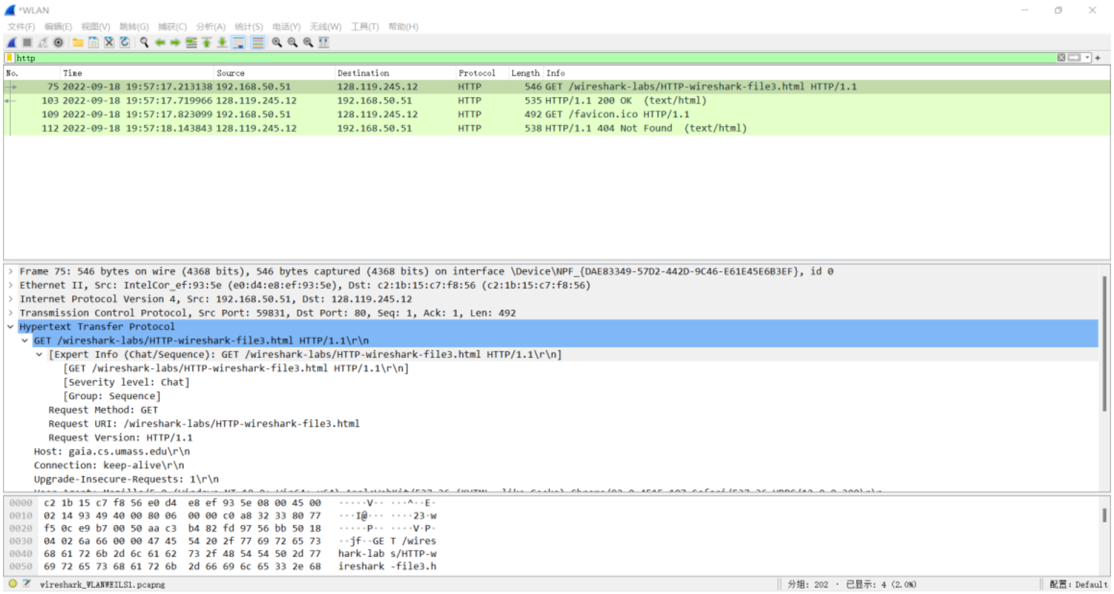
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the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

（图 1-13 浏览器登入界面显示）

实验过程中选择 http 过滤，Wireshark 抓包结果如图 1-14（注意 HTTP 协议中不包含“Continuation”报文）。


*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) 帮助(H)

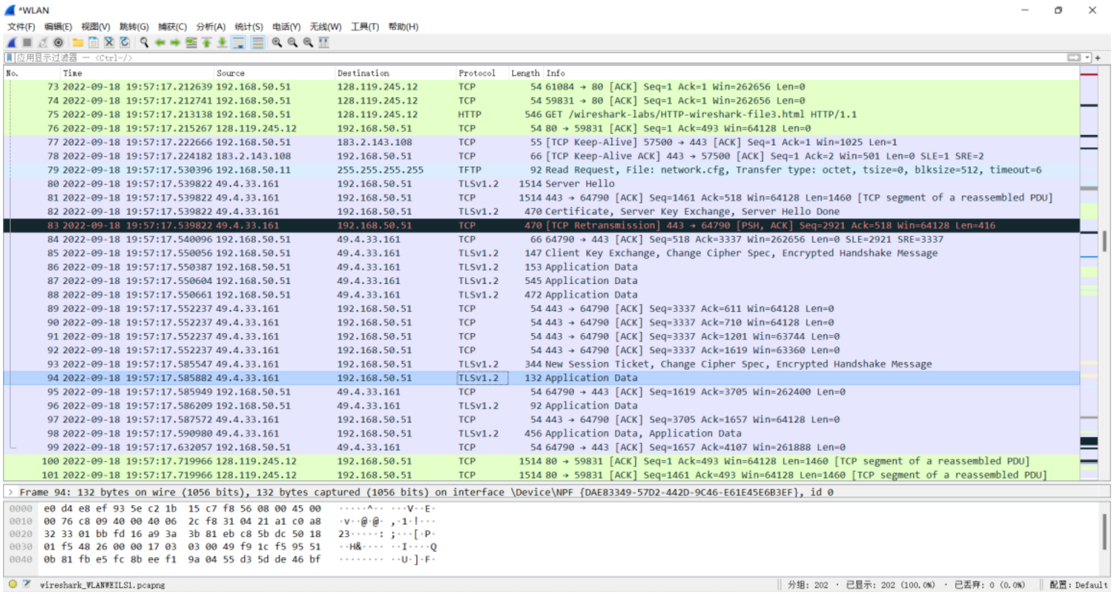
http

```
No.    Time                        Source          Destination     Protocol  Length Info
    75 2022-09-18 19:57:17.213138 192.168.50.51   128.119.245.12  HTTP       546 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   103 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51   HTTP       535 HTTP/1.1 200 OK  (text/html)
   109 2022-09-18 19:57:17.823099 192.168.50.51   128.119.245.12  HTTP       492 GET /favicon.ico HTTP/1.1
   112 2022-09-18 19:57:18.143843 128.119.245.12  192.168.50.51   HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 75: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59831, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

```
0000  c2 1b 15 c7 f8 56 e0 d4  e8 ef 93 5e 08 00 45 00   ·····V·· ···^··E·
0010  02 14 93 49 40 00 80 06  00 00 c0 a8 32 33 80 77   ···I@··· ····23·w
0020  f5 0c e9 b7 00 50 aa c3  b4 82 fd 97 56 bb 50 18   ·····P·· ····V·P·
0030  04 02 6a 66 00 00 47 45  54 20 2f 77 69 72 65 73   ··jf··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
```

wireshark_WLANWEILS1.pcapng　　分组: 202 · 已显示: 4 (2.0%)　　配置: Default



*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) 帮助(H)
应用显示过滤器 … <Ctrl-/>

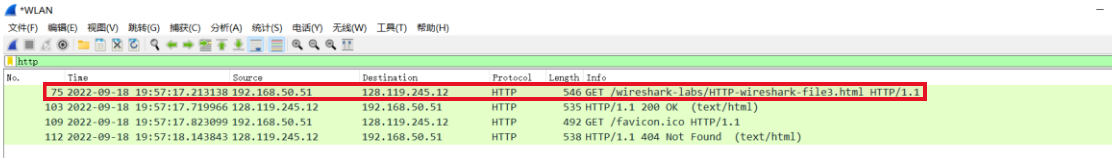
```
No.   Time                       Source          Destination      Protocol Length Info
   73 2022-09-18 19:57:17.212639 192.168.50.51   128.119.245.12   TCP        54 61084 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
   74 2022-09-18 19:57:17.212741 192.168.50.51   128.119.245.12   TCP        54 59831 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
   75 2022-09-18 19:57:17.213138 192.168.50.51   128.119.245.12   HTTP      546 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   76 2022-09-18 19:57:17.215267 128.119.245.12  192.168.50.51    TCP        54 80 → 59831 [ACK] Seq=1 Ack=493 Win=64128 Len=0
   77 2022-09-18 19:57:17.222666 192.168.50.51   183.2.143.108    TCP        55 [TCP Keep-Alive] 57500 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1
   78 2022-09-18 19:57:17.224182 183.2.143.108   192.168.50.51    TCP        66 [TCP Keep-Alive ACK] 443 → 57500 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
   79 2022-09-18 19:57:17.530396 192.168.50.11   255.255.255.255  TFTP       92 Read Request, File: network.cfg, Transfer type: octet, tsize=0, blksize=512, timeout=6
   80 2022-09-18 19:57:17.539822 49.4.33.161     192.168.50.51    TLSv1.2  1514 Server Hello
   81 2022-09-18 19:57:17.539822 49.4.33.161     192.168.50.51    TCP      1514 443 → 64790 [ACK] Seq=1461 Ack=518 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
   82 2022-09-18 19:57:17.539822 49.4.33.161     192.168.50.51    TLSv1.2   470 Certificate, Server Key Exchange, Server Hello Done
   83 2022-09-18 19:57:17.539822 49.4.33.161     192.168.50.51    TCP       470 [TCP Retransmission] 443 → 64790 [PSH, ACK] Seq=2921 Ack=518 Win=64128 Len=416
   84 2022-09-18 19:57:17.540096 192.168.50.51   49.4.33.161      TCP        66 64790 → 443 [ACK] Seq=518 Ack=3337 Win=262656 Len=0 SLE=2921 SRE=3337
   85 2022-09-18 19:57:17.550056 192.168.50.51   49.4.33.161      TLSv1.2   147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   86 2022-09-18 19:57:17.550387 192.168.50.51   49.4.33.161      TLSv1.2   153 Application Data
   87 2022-09-18 19:57:17.550604 192.168.50.51   49.4.33.161      TLSv1.2   545 Application Data
   88 2022-09-18 19:57:17.550661 192.168.50.51   49.4.33.161      TLSv1.2   472 Application Data
   89 2022-09-18 19:57:17.552237 49.4.33.161     192.168.50.51    TCP        54 443 → 64790 [ACK] Seq=3337 Ack=611 Win=64128 Len=0
   90 2022-09-18 19:57:17.552237 49.4.33.161     192.168.50.51    TCP        54 443 → 64790 [ACK] Seq=3337 Ack=710 Win=64128 Len=0
   91 2022-09-18 19:57:17.552237 49.4.33.161     192.168.50.51    TCP        54 443 → 64790 [ACK] Seq=3337 Ack=1201 Win=63744 Len=0
   92 2022-09-18 19:57:17.552237 49.4.33.161     192.168.50.51    TCP        54 443 → 64790 [ACK] Seq=3337 Ack=1619 Win=63360 Len=0
   93 2022-09-18 19:57:17.585547 49.4.33.161     192.168.50.51    TLSv1.2   344 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
   94 2022-09-18 19:57:17.585882 49.4.33.161     192.168.50.51    TLSv1.2   132 Application Data
   95 2022-09-18 19:57:17.585949 192.168.50.51   49.4.33.161      TCP        54 64790 → 443 [ACK] Seq=1619 Ack=3705 Win=262400 Len=0
   96 2022-09-18 19:57:17.586209 192.168.50.51   49.4.33.161      TLSv1.2    92 Application Data
   97 2022-09-18 19:57:17.587572 49.4.33.161     192.168.50.51    TCP        54 443 → 64790 [ACK] Seq=3705 Ack=1657 Win=64128 Len=0
   98 2022-09-18 19:57:17.590980 49.4.33.161     192.168.50.51    TLSv1.2   456 Application Data, Application Data
   99 2022-09-18 19:57:17.632057 192.168.50.51   49.4.33.161      TCP        54 64790 → 443 [ACK] Seq=1657 Ack=4107 Win=261888 Len=0
  100 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    TCP      1514 80 → 59831 [ACK] Seq=1 Ack=493 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  101 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    TCP      1514 80 → 59831 [ACK] Seq=1461 Ack=493 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
> Frame 94: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface \Device\NPF {DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
0000  e0 d4 e8 ef 93 5e c2 1b  15 c7 f8 56 08 00 45 00   ·····^·· ···V··E·
0010  00 76 c8 09 40 00 40 06  2c f8 31 04 21 a1 c0 a8   ·v··@·@· ,·1·!···
0020  32 33 01 bb fd 16 a9 3a  3b 81 eb c8 5b dc 50 18   23·····: ;···[·P·
0030  01 f5 48 26 00 00 17 03  03 00 49 f9 1c f5 95 51   ··H&···· ··I····Q
0040  0b 81 fb e5 fc 8b ee f1  9a 04 55 d3 5d de 46 bf   ········ ··U·]·F·
wireshark_WLANWEILS1.pcapng        分组: 202 · 已显示: 202 (100.0%) · 已丢弃: 0 (0.0%)    配置: Default
```

（图 1-14 Wireshark 抓包结果）

Q&A：

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?

Ans： 一共发送了 2 个 GET request messages(在不忽略 favicon 请求的情况下，若忽略，则为 1 个 message)；The first one（number 75）.

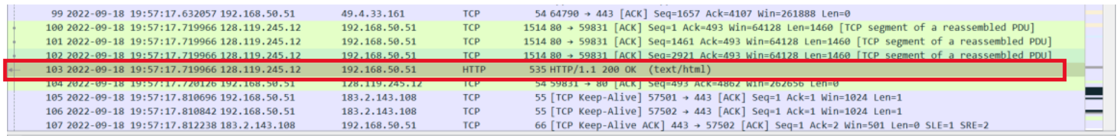


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http

```
No.   Time                       Source          Destination      Protocol Length Info
   75 2022-09-18 19:57:17.213138 192.168.50.51   128.119.245.12   HTTP      546 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  103 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    HTTP      535 HTTP/1.1 200 OK  (text/html)
  109 2022-09-18 19:57:17.823099 192.168.50.51   128.119.245.12   HTTP      492 GET /favicon.ico HTTP/1.1
  112 2022-09-18 19:57:18.143843 128.119.245.12  192.168.50.51    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

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

Ans： 103;(200 OK);



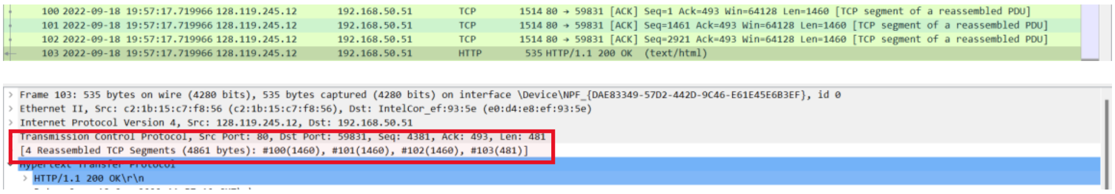
```
   99 2022-09-18 19:57:17.632057 192.168.50.51   49.4.33.161      TCP        54 64790 → 443 [ACK] Seq=1657 Ack=4107 Win=261888 Len=0
  100 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    TCP      1514 80 → 59831 [ACK] Seq=1 Ack=493 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  101 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    TCP      1514 80 → 59831 [ACK] Seq=1461 Ack=493 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  102 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    TCP      1514 80 → 59831 [ACK] Seq=2921 Ack=493 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  103 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    HTTP      535 HTTP/1.1 200 OK  (text/html)
  104 2022-09-18 19:57:17.720126 192.168.50.51   128.119.245.12   TCP        54 59831 → 80 [ACK] Seq=493 Ack=4862 Win=262656 Len=0
  105 2022-09-18 19:57:17.810696 192.168.50.51   183.2.143.108    TCP        55 [TCP Keep-Alive] 57501 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1
  106 2022-09-18 19:57:17.810842 192.168.50.51   183.2.143.108    TCP        55 [TCP Keep-Alive] 57502 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1
  107 2022-09-18 19:57:17.812238 183.2.143.108   192.168.50.51    TCP        66 [TCP Keep-Alive ACK] 443 → 57502 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
```

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

Ans： 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?

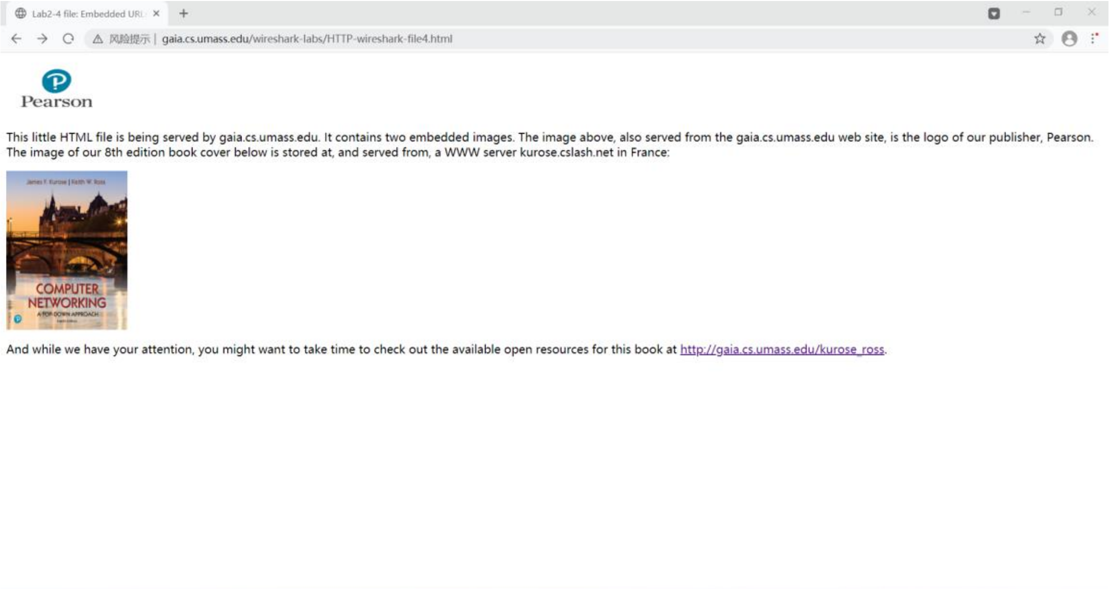
Ans： 4（分别为#100、#101、#102、#103）.



```
  100 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    TCP      1514 80 → 59831 [ACK] Seq=1 Ack=493 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  101 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    TCP      1514 80 → 59831 [ACK] Seq=1461 Ack=493 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  102 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    TCP      1514 80 → 59831 [ACK] Seq=2921 Ack=493 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  103 2022-09-18 19:57:17.719966 128.119.245.12  192.168.50.51    HTTP      535 HTTP/1.1 200 OK  (text/html)

> Frame 103: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.50.51
  Transmission Control Protocol, Src Port: 80, Dst Port: 59831, Seq: 4381, Ack: 493, Len: 481
  [4 Reassembled TCP Segments (4861 bytes): #100(1460), #101(1460), #102(1460), #103(481)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
```

Step 4：HTML Documents with Embedded Objects

打开浏览器并清除缓存内容，打开 Wireshark 抓包并登入以下 URL：http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html 。观察到如下界面：

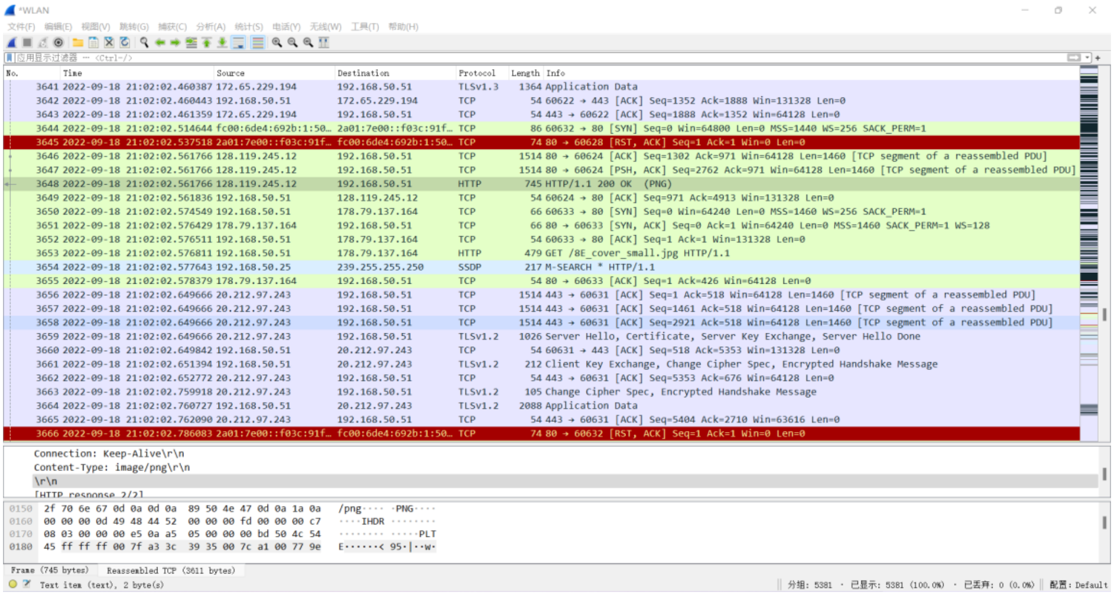

Lab2-4 file: Embedded URL
风险提示 | gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
Pearson

This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France:

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

（图 1-15 浏览器登入界面显示）

Wireshark 抓包结果如图 1-16。

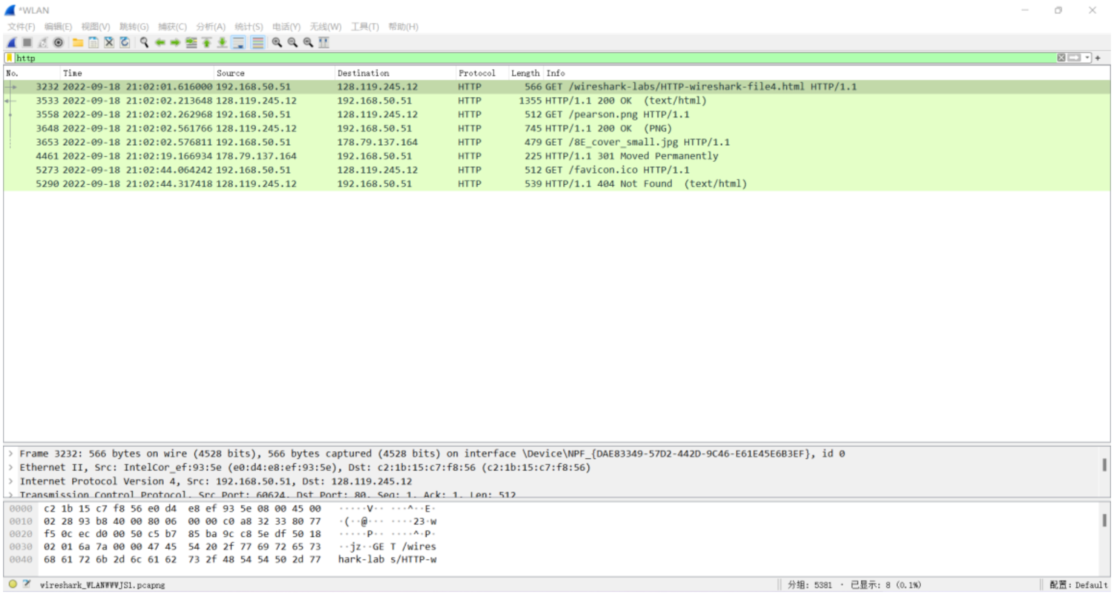

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time                       Source                 Destination            Protocol Length Info
 3641 2022-09-18 21:02:02.460387 172.65.229.194         192.168.50.51          TLSv1.3  1364 Application Data
 3642 2022-09-18 21:02:02.460443 192.168.50.51          172.65.229.194         TCP        54 60622 → 443 [ACK] Seq=1352 Ack=1888 Win=131328 Len=0
 3643 2022-09-18 21:02:02.461359 172.65.229.194         192.168.50.51          TCP        54 443 → 60622 [ACK] Seq=1888 Ack=1352 Win=64128 Len=0
 3644 2022-09-18 21:02:02.514644 fc00:6de4:692b:1:50…   2a01:7e00::f03c:91f…   TCP        86 60632 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
 3645 2022-09-18 21:02:02.537518 2a01:7e00::f03c:91f…   fc00:6de4:692b:1:50…   TCP        74 80 → 60628 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3646 2022-09-18 21:02:02.561766 128.119.245.12         192.168.50.51          TCP      1514 80 → 60624 [ACK] Seq=1302 Ack=971 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 3647 2022-09-18 21:02:02.561766 128.119.245.12         192.168.50.51          TCP      1514 80 → 60624 [PSH, ACK] Seq=2762 Ack=971 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 3648 2022-09-18 21:02:02.561766 128.119.245.12         192.168.50.51          HTTP      745 HTTP/1.1 200 OK  (PNG)
 3649 2022-09-18 21:02:02.561836 192.168.50.51          128.119.245.12         TCP        54 60624 → 80 [ACK] Seq=971 Ack=4913 Win=131328 Len=0
 3650 2022-09-18 21:02:02.574549 192.168.50.51          178.79.137.164         TCP        66 60633 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3651 2022-09-18 21:02:02.576429 178.79.137.164         192.168.50.51          TCP        66 80 → 60633 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 3652 2022-09-18 21:02:02.576511 192.168.50.51          178.79.137.164         TCP        54 60633 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 3653 2022-09-18 21:02:02.576811 192.168.50.51          178.79.137.164         HTTP      479 GET /8E_cover_small.jpg HTTP/1.1
 3654 2022-09-18 21:02:02.577643 192.168.50.25          239.255.255.250        SSDP      217 M-SEARCH * HTTP/1.1
 3655 2022-09-18 21:02:02.578379 178.79.137.164         192.168.50.51          TCP        54 80 → 60633 [ACK] Seq=1 Ack=426 Win=64128 Len=0
 3656 2022-09-18 21:02:02.649666 20.212.97.243          192.168.50.51          TCP      1514 443 → 60631 [ACK] Seq=1 Ack=518 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 3657 2022-09-18 21:02:02.649666 20.212.97.243          192.168.50.51          TCP      1514 443 → 60631 [ACK] Seq=1461 Ack=518 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 3658 2022-09-18 21:02:02.649666 20.212.97.243          192.168.50.51          TCP      1514 443 → 60631 [ACK] Seq=2921 Ack=518 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 3659 2022-09-18 21:02:02.649666 20.212.97.243          192.168.50.51          TLSv1.2  1026 Server Hello, Certificate, Server Key Exchange, Server Hello Done
 3660 2022-09-18 21:02:02.649842 192.168.50.51          20.212.97.243          TCP        54 60631 → 443 [ACK] Seq=518 Ack=5353 Win=131328 Len=0
 3661 2022-09-18 21:02:02.651394 192.168.50.51          20.212.97.243          TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 3662 2022-09-18 21:02:02.652772 20.212.97.243          192.168.50.51          TCP        54 443 → 60631 [ACK] Seq=5353 Ack=676 Win=64128 Len=0
 3663 2022-09-18 21:02:02.759918 20.212.97.243          192.168.50.51          TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
 3664 2022-09-18 21:02:02.760727 192.168.50.51          20.212.97.243          TLSv1.2  2088 Application Data
 3665 2022-09-18 21:02:02.762090 20.212.97.243          192.168.50.51          TCP        54 443 → 60631 [ACK] Seq=5404 Ack=2710 Win=63616 Len=0
 3666 2022-09-18 21:02:02.786083 2a01:7e00::f03c:91f…   fc00:6de4:692b:1:50…   TCP        74 80 → 60632 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
    Connection: Keep-Alive\r\n
    Content-Type: image/png\r\n
    \r\n
    [HTTP response 2/2]
```

```
0150  2f 70 6e 67 0d 0a 0d 0a  89 50 4e 47 0d 0a 1a 0a   /png···· ·PNG····
0160  00 00 00 0d 49 48 44 52  00 00 00 fd 00 00 00 c7   ····IHDR ········
0170  08 03 00 00 00 e5 0a a5  05 00 00 00 bd 50 4c 54   ········ ·····PLT
0180  45 ff ff ff 00 7f a3 3c  39 35 00 7c a1 00 77 9e   E······< 95·|··w·
```

```
Frame (745 bytes)   Reassembled TCP (3611 bytes)
Text item (text), 2 byte(s)      分组: 5381 · 已显示: 5381 (100.0%) · 已丢弃: 0 (0.0%) | 配置: Default
```


*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) 帮助(H)
http

```
No.    Time                        Source          Destination     Protocol  Length Info
  3232 2022-09-18 21:02:01.616000 192.168.50.51   128.119.245.12  HTTP       566 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  3533 2022-09-18 21:02:02.213648 128.119.245.12  192.168.50.51   HTTP      1355 HTTP/1.1 200 OK  (text/html)
  3558 2022-09-18 21:02:02.262968 192.168.50.51   128.119.245.12  HTTP       512 GET /pearson.png HTTP/1.1
  3648 2022-09-18 21:02:02.561766 128.119.245.12  192.168.50.51   HTTP       745 HTTP/1.1 200 OK  (PNG)
  3653 2022-09-18 21:02:02.576811 192.168.50.51   178.79.137.164  HTTP       479 GET /8E_cover_small.jpg HTTP/1.1
  4461 2022-09-18 21:02:19.166934 178.79.137.164  192.168.50.51   HTTP       225 HTTP/1.1 301 Moved Permanently
  5273 2022-09-18 21:02:44.064242 192.168.50.51   128.119.245.12  HTTP       512 GET /favicon.ico HTTP/1.1
  5290 2022-09-18 21:02:44.317418 128.119.245.12  192.168.50.51   HTTP       539 HTTP/1.1 404 Not Found  (text/html)

> Frame 3232: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60624, Dst Port: 80, Seq: 1, Ack: 1, Len: 512

0000  c2 1b 15 c7 f8 56 e0 d4  e8 ef 93 5e 08 00 45 00   ·····V·· ···^··E·
0010  02 28 93 b8 40 00 80 06  00 00 c0 a8 32 33 80 77   ·(··@··· ····23·w
0020  f5 0c ec d0 00 50 c5 b7  85 ba 9c c8 5e df 50 18   ·····P·· ····^·P·
0030  02 01 6a 7a 00 00 47 45  54 20 2f 77 69 72 65 73   ··jz··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

wireshark_WLANWWWJS1.pcapng      分组: 5381 · 已显示: 8 (0.1%)      配置: Default
```

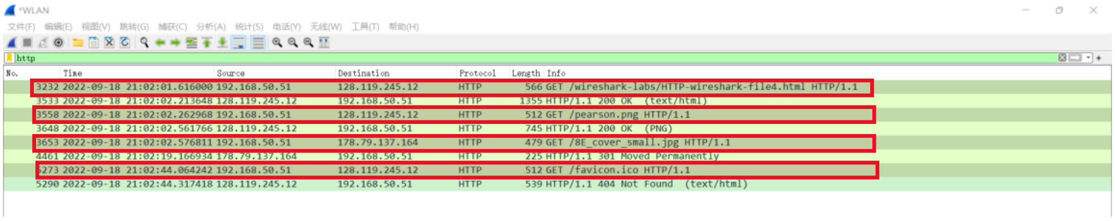
（图 1-16 Wireshark 抓包结果）

Q&A：

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

Ans： My browser sent 4 HTTP GET request messages in total(在不忽略 favicon 请求的情况下，若忽略，则为 3 个 messages).

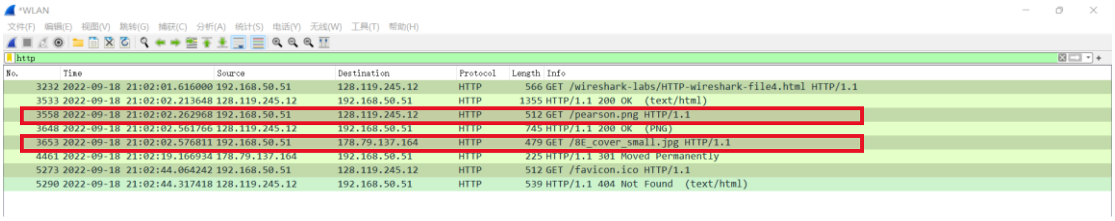
Adresses:前两个（以及最后一个）的地址均为 128.119.245.12。第三个的地址为 178.79.137.164。


*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) 帮助(H)
http

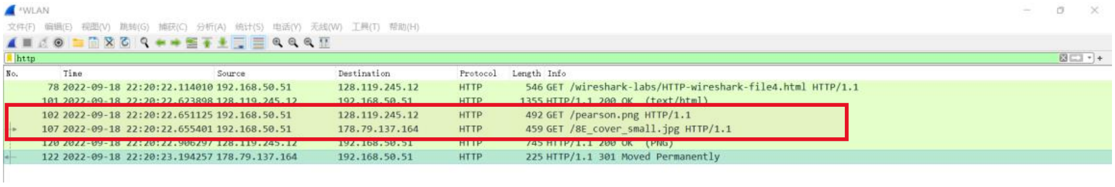
```
No.    Time                        Source          Destination     Protocol  Length Info
  3232 2022-09-18 21:02:01.616000 192.168.50.51   128.119.245.12  HTTP       566 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  3533 2022-09-18 21:02:02.213648 128.119.245.12  192.168.50.51   HTTP      1355 HTTP/1.1 200 OK  (text/html)
  3558 2022-09-18 21:02:02.262968 192.168.50.51   128.119.245.12  HTTP       512 GET /pearson.png HTTP/1.1
  3648 2022-09-18 21:02:02.561766 128.119.245.12  192.168.50.51   HTTP       745 HTTP/1.1 200 OK  (PNG)
  3653 2022-09-18 21:02:02.576811 192.168.50.51   178.79.137.164  HTTP       479 GET /8E_cover_small.jpg HTTP/1.1
  4461 2022-09-18 21:02:19.166934 178.79.137.164  192.168.50.51   HTTP       225 HTTP/1.1 301 Moved Permanently
  5273 2022-09-18 21:02:44.064242 192.168.50.51   128.119.245.12  HTTP       512 GET /favicon.ico HTTP/1.1
  5290 2022-09-18 21:02:44.317418 128.119.245.12  192.168.50.51   HTTP       539 HTTP/1.1 404 Not Found  (text/html)
```

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.

Ans： 并行的。在第一次实验（Microsoft Edge）结果中实验结果显示两个包并不是同时发送的（实验结果如下）。第一个 GET 包在 21：02：02.262968 时发送，在 21：02：02.561766 时收到回复。而第二个包在 21：02：02.576811 时才发送。为保证准确性，以下换用另一个浏览器（华为浏览器）再次试验。实验结果如下：两个包发送时间间隔极小，可以证明二者是并行发送的。分析得出，两次实验结果存在差异的可能原因是不同浏览器的处理方式不同以及两张图片请求的服务器不同，请求时间等具有一定差异。


*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) 帮助(H)
http

```
No.    Time                        Source          Destination     Protocol  Length Info
  3232 2022-09-18 21:02:01.616000 192.168.50.51   128.119.245.12  HTTP       566 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  3533 2022-09-18 21:02:02.213648 128.119.245.12  192.168.50.51   HTTP      1355 HTTP/1.1 200 OK  (text/html)
  3558 2022-09-18 21:02:02.262968 192.168.50.51   128.119.245.12  HTTP       512 GET /pearson.png HTTP/1.1
  3648 2022-09-18 21:02:02.561766 128.119.245.12  192.168.50.51   HTTP       745 HTTP/1.1 200 OK  (PNG)
  3653 2022-09-18 21:02:02.576811 192.168.50.51   178.79.137.164  HTTP       479 GET /8E_cover_small.jpg HTTP/1.1
  4461 2022-09-18 21:02:19.166934 178.79.137.164  192.168.50.51   HTTP       225 HTTP/1.1 301 Moved Permanently
  5273 2022-09-18 21:02:44.064242 192.168.50.51   128.119.245.12  HTTP       512 GET /favicon.ico HTTP/1.1
  5290 2022-09-18 21:02:44.317418 128.119.245.12  192.168.50.51   HTTP       539 HTTP/1.1 404 Not Found  (text/html)
```

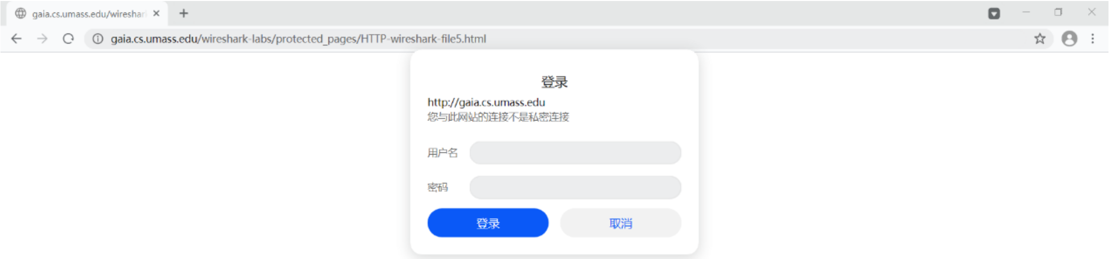


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
http
No.     Time                        Source          Destination     Protocol  Length Info
     78 2022-09-18 22:20:22.114010 192.168.50.51   128.119.245.12  HTTP         546 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
    101 2022-09-18 22:20:22.623898 128.119.245.12  192.168.50.51   HTTP        1355 HTTP/1.1 200 OK  (text/html)
    102 2022-09-18 22:20:22.651125 192.168.50.51   128.119.245.12  HTTP         492 GET /pearson.png HTTP/1.1
    107 2022-09-18 22:20:22.655401 192.168.50.51   178.79.137.164  HTTP         459 GET /8E_cover_small.jpg HTTP/1.1
    120 2022-09-18 22:20:22.906297 128.119.245.12  192.168.50.51   HTTP         745 HTTP/1.1 200 OK  (PNG)
    122 2022-09-18 22:20:23.194257 178.79.137.164  192.168.50.51   HTTP         225 HTTP/1.1 301 Moved Permanently
```

Step 5：HTTP Authentication

打开浏览器并清除缓存内容，重启浏览器。打开 Wireshark 抓包并登入以下 URL：http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html 。观察到如下界面：

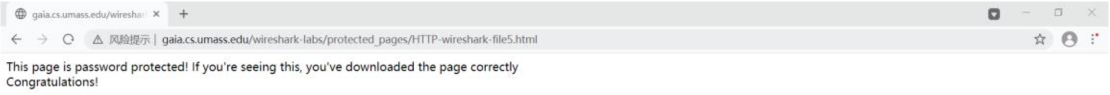


gaia.cs.umass.edu/wiresha
gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
登录

http://gaia.cs.umass.edu
您与此网站的连接不是私密连接

（图 1-17 浏览器登入界面显示）

输入用户名和密码，观察到如下界面：

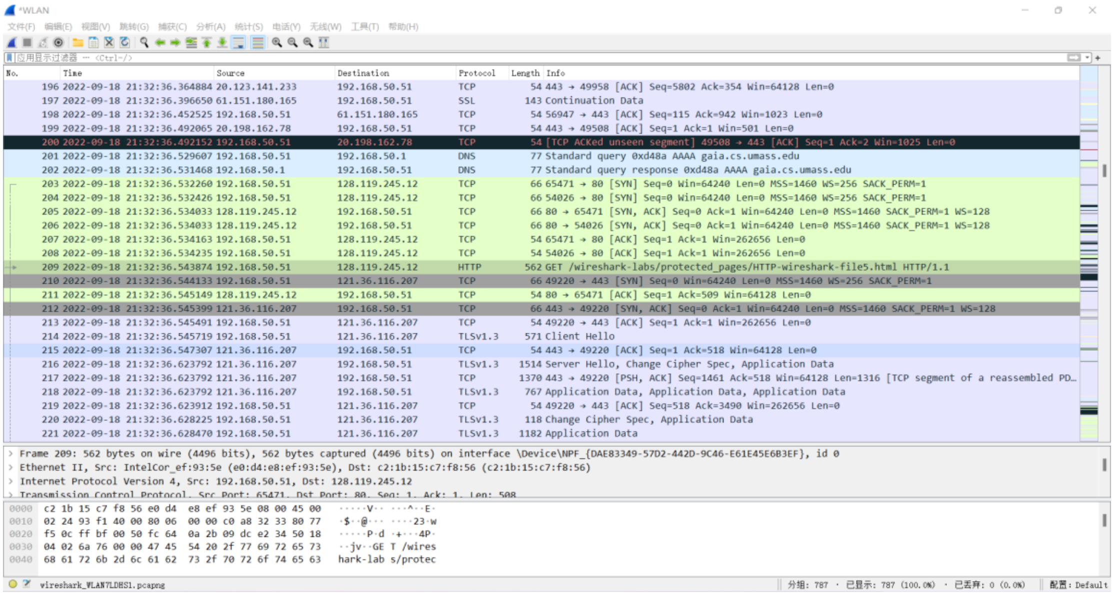


gaia.cs.umass.edu/wiresha
风险提示 | gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

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

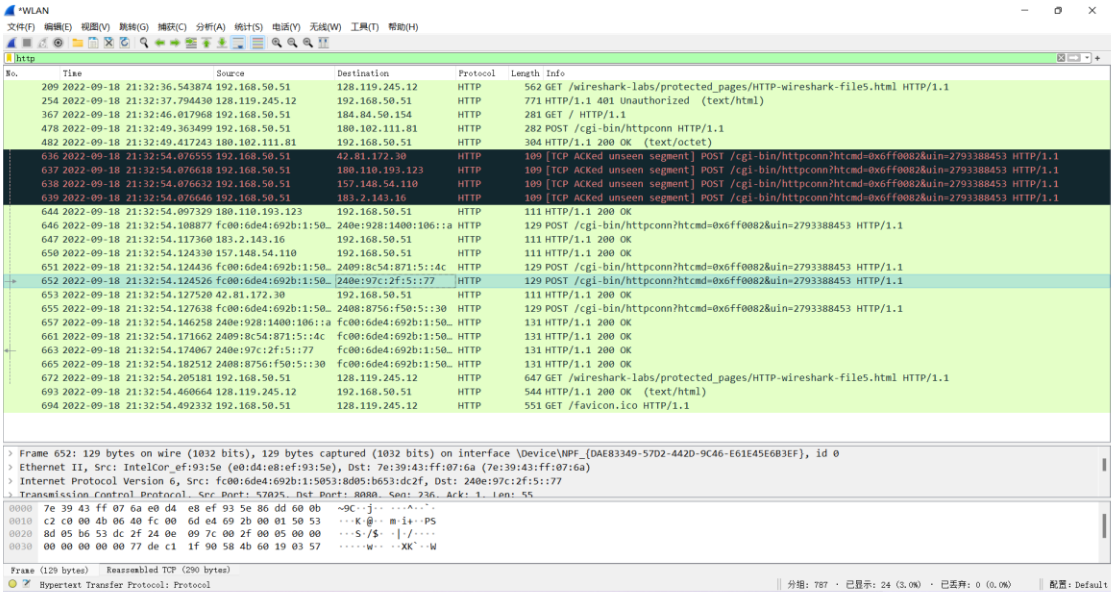
（图 1-18 输入密码后成功登入显示）

Wireshark 抓包显示如下：



*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) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.     Time                        Source          Destination     Protocol  Length Info
    196 2022-09-18 21:32:36.364884 20.123.141.233  192.168.50.51   TCP           54 443 → 49958 [ACK] Seq=5802 Ack=354 Win=64128 Len=0
    197 2022-09-18 21:32:36.396650 61.151.180.165  192.168.50.51   SSL          143 Continuation Data
    198 2022-09-18 21:32:36.452525 192.168.50.51   61.151.180.165  TCP           54 56947 → 443 [ACK] Seq=115 Ack=942 Win=1023 Len=0
    199 2022-09-18 21:32:36.492065 20.198.162.78   192.168.50.51   TCP           54 443 → 49508 [ACK] Seq=1 Ack=1 Win=501 Len=0
    200 2022-09-18 21:32:36.492152 192.168.50.51   20.198.162.78   TCP           54 [TCP ACKed unseen segment] 49508 → 443 [ACK] Seq=1 Ack=2 Win=1025 Len=0
    201 2022-09-18 21:32:36.529607 192.168.50.51   192.168.50.1    DNS           77 Standard query 0xd48a AAAA gaia.cs.umass.edu
    202 2022-09-18 21:32:36.531468 192.168.50.1    192.168.50.51   DNS           77 Standard query response 0xd48a AAAA gaia.cs.umass.edu
    203 2022-09-18 21:32:36.532260 192.168.50.51   128.119.245.12  TCP           66 65471 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    204 2022-09-18 21:32:36.532426 192.168.50.51   128.119.245.12  TCP           66 54026 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    205 2022-09-18 21:32:36.534033 128.119.245.12  192.168.50.51   TCP           66 80 → 65471 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
    206 2022-09-18 21:32:36.534033 128.119.245.12  192.168.50.51   TCP           66 80 → 54026 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
    207 2022-09-18 21:32:36.534163 192.168.50.51   128.119.245.12  TCP           54 65471 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
    208 2022-09-18 21:32:36.534235 192.168.50.51   128.119.245.12  TCP           54 54026 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
    209 2022-09-18 21:32:36.543874 192.168.50.51   128.119.245.12  HTTP         562 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    210 2022-09-18 21:32:36.544133 192.168.50.51   121.36.116.207  TCP           66 49220 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    211 2022-09-18 21:32:36.545149 128.119.245.12  192.168.50.51   TCP           54 80 → 65471 [ACK] Seq=1 Ack=509 Win=64128 Len=0
    212 2022-09-18 21:32:36.545399 121.36.116.207  192.168.50.51   TCP           66 443 → 49220 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
    213 2022-09-18 21:32:36.545491 192.168.50.51   121.36.116.207  TCP           54 49220 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
    214 2022-09-18 21:32:36.545719 192.168.50.51   121.36.116.207  TLSv1.3      571 Client Hello
    215 2022-09-18 21:32:36.547307 121.36.116.207  192.168.50.51   TCP           54 443 → 49220 [ACK] Seq=1 Ack=518 Win=64128 Len=0
    216 2022-09-18 21:32:36.623792 121.36.116.207  192.168.50.51   TLSv1.3     1514 Server Hello, Change Cipher Spec, Application Data
    217 2022-09-18 21:32:36.623792 121.36.116.207  192.168.50.51   TCP         1370 443 → 49220 [PSH, ACK] Seq=1461 Ack=518 Win=64128 Len=1316 [TCP segment of a reassembled PD…
    218 2022-09-18 21:32:36.623792 121.36.116.207  192.168.50.51   TLSv1.3      767 Application Data, Application Data, Application Data
    219 2022-09-18 21:32:36.623912 192.168.50.51   121.36.116.207  TCP           54 49220 → 443 [ACK] Seq=518 Ack=3490 Win=262656 Len=0
    220 2022-09-18 21:32:36.628225 192.168.50.51   121.36.116.207  TLSv1.3      118 Change Cipher Spec, Application Data
    221 2022-09-18 21:32:36.628470 192.168.50.51   121.36.116.207  TLSv1.3     1182 Application Data

> Frame 209: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 65471, Dst Port: 80, Seq: 1, Ack: 1, Len: 508

0000  c2 1b 15 c7 f8 56 e0 d4  e8 ef 93 5e 08 00 45 00   ·····V·· ···^··E·
0010  02 24 93 f1 40 00 80 06  00 00 c0 a8 32 33 80 77   ·$··@··· ····23·w
0020  f5 0c ff bf 00 50 fc 64  0a 2b 09 dc e2 34 50 18   ·····P·d ·+···4P·
0030  04 02 6a 76 00 00 47 45  54 20 2f 77 69 72 65 73   ··jv··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec

wireshark_WLAN7LDHS1.pcapng        分组: 787 · 已显示: 787 (100.0%) · 已丢弃: 0 (0.0%)    配置: Default
```


*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) 帮助(H)
http

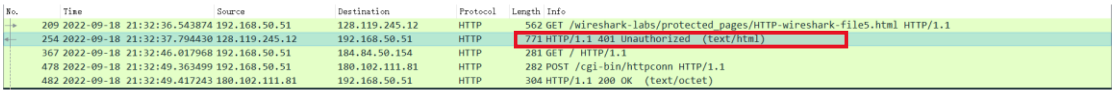
```
No.     Time                       Source                 Destination            Protocol  Length Info
    209 2022-09-18 21:32:36.543874 192.168.50.51          128.119.245.12         HTTP       562 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    254 2022-09-18 21:32:37.794430 128.119.245.12         192.168.50.51          HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
    367 2022-09-18 21:32:46.017968 192.168.50.51          184.84.50.154          HTTP       281 GET / HTTP/1.1
    478 2022-09-18 21:32:49.363499 192.168.50.51          180.102.111.81         HTTP       282 POST /cgi-bin/httpconn HTTP/1.1
    482 2022-09-18 21:32:49.417243 180.102.111.81         192.168.50.51          HTTP       304 HTTP/1.1 200 OK  (text/octet)
    636 2022-09-18 21:32:54.076555 192.168.50.51          42.81.172.30           HTTP       109 [TCP ACKed unseen segment] POST /cgi-bin/httpconn?htcmd=0x6ff0082&uin=2793388453 HTTP/1.1
    637 2022-09-18 21:32:54.076618 192.168.50.51          180.110.193.123        HTTP       109 [TCP ACKed unseen segment] POST /cgi-bin/httpconn?htcmd=0x6ff0082&uin=2793388453 HTTP/1.1
    638 2022-09-18 21:32:54.076632 192.168.50.51          157.148.54.110         HTTP       109 [TCP ACKed unseen segment] POST /cgi-bin/httpconn?htcmd=0x6ff0082&uin=2793388453 HTTP/1.1
    639 2022-09-18 21:32:54.076646 192.168.50.51          183.2.143.16           HTTP       109 [TCP ACKed unseen segment] POST /cgi-bin/httpconn?htcmd=0x6ff0082&uin=2793388453 HTTP/1.1
    644 2022-09-18 21:32:54.097329 180.110.193.123        192.168.50.51          HTTP       111 HTTP/1.1 200 OK
    646 2022-09-18 21:32:54.108877 fc00:6de4:692b:1:50…   240e:928:1400:106::a   HTTP       129 POST /cgi-bin/httpconn?htcmd=0x6ff0082&uin=2793388453 HTTP/1.1
    647 2022-09-18 21:32:54.117360 183.2.143.16           192.168.50.51          HTTP       111 HTTP/1.1 200 OK
    650 2022-09-18 21:32:54.124330 157.148.54.110         192.168.50.51          HTTP       111 HTTP/1.1 200 OK
    651 2022-09-18 21:32:54.124436 fc00:6de4:692b:1:50…   2409:8c54:871:5::4c    HTTP       129 POST /cgi-bin/httpconn?htcmd=0x6ff0082&uin=2793388453 HTTP/1.1
    652 2022-09-18 21:32:54.124526 fc00:6de4:692b:1:50…   240e:97c:2f:5::77      HTTP       129 POST /cgi-bin/httpconn?htcmd=0x6ff0082&uin=2793388453 HTTP/1.1
    653 2022-09-18 21:32:54.127520 42.81.172.30           192.168.50.51          HTTP       111 HTTP/1.1 200 OK
    655 2022-09-18 21:32:54.127638 fc00:6de4:692b:1:50…   2408:8756:f50:5::30    HTTP       129 POST /cgi-bin/httpconn?htcmd=0x6ff0082&uin=2793388453 HTTP/1.1
    657 2022-09-18 21:32:54.146258 240e:928:1400:106::a   fc00:6de4:692b:1:50…   HTTP       131 HTTP/1.1 200 OK
    661 2022-09-18 21:32:54.171662 2409:8c54:871:5::4c    fc00:6de4:692b:1:50…   HTTP       131 HTTP/1.1 200 OK
    663 2022-09-18 21:32:54.174067 240e:97c:2f:5::77      fc00:6de4:692b:1:50…   HTTP       131 HTTP/1.1 200 OK
    665 2022-09-18 21:32:54.182512 2408:8756:f50:5::30    fc00:6de4:692b:1:50…   HTTP       131 HTTP/1.1 200 OK
    672 2022-09-18 21:32:54.205181 192.168.50.51          128.119.245.12         HTTP       647 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    693 2022-09-18 21:32:54.460664 128.119.245.12         192.168.50.51          HTTP       544 HTTP/1.1 200 OK  (text/html)
    694 2022-09-18 21:32:54.492332 192.168.50.51          128.119.245.12         HTTP       551 GET /favicon.ico HTTP/1.1

> Frame 652: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: 7e:39:43:ff:07:6a (7e:39:43:ff:07:6a)
> Internet Protocol Version 6, Src: fc00:6de4:692b:1:5053:8d05:b653:dc2f, Dst: 240e:97c:2f:5::77
> Transmission Control Protocol, Src Port: 57025, Dst Port: 8080, Seq: 236, Ack: 1, Len: 55

0000  7e 39 43 ff 07 6a e0 d4  e8 ef 93 5e 86 dd 60 0b   ~9C··j·· ···^··`·
0010  c2 c0 00 4b 06 40 fc 00  6d e4 69 2b 00 01 50 53   ···K·@·· m·i+··PS
0020  8d 05 b6 53 dc 2f 24 0e  09 7c 00 2f 00 05 00 00   ···S·/$· ·|·/····
0030  00 00 00 00 00 77 de c1  1f 90 58 4b 60 19 03 57   ·····w·· ··XK`··W

Frame (129 bytes)   Reassembled TCP (290 bytes)
Hypertext Transfer Protocol: Protocol            分组: 787 · 已显示: 24 (3.0%) · 已丢弃: 0 (0.0%)    配置: Default
```

（图 1-19 Wireshark 抓包显示）

Q&A:

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

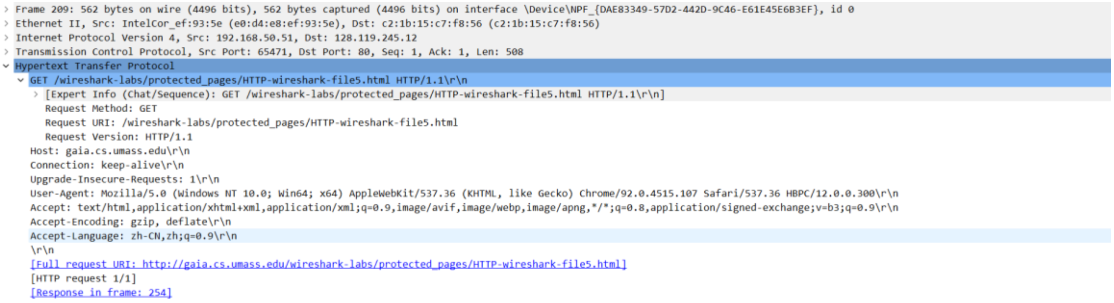
Ans： 401 Unauthorized。



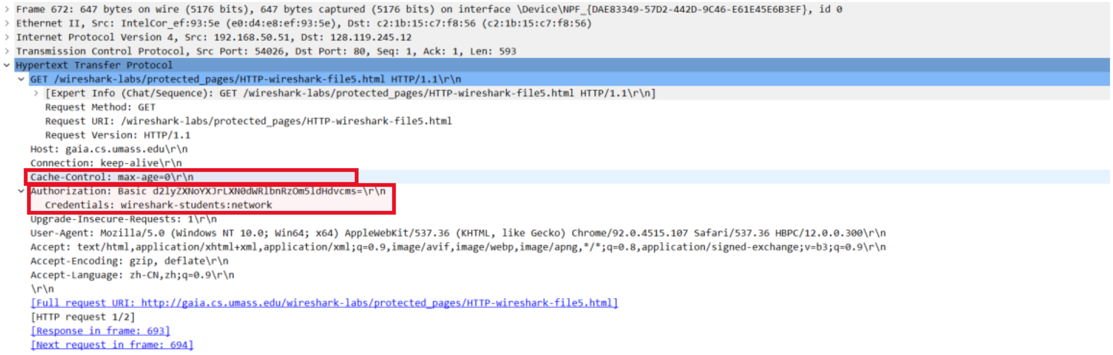
```
No.     Time                       Source                 Destination            Protocol  Length Info
    209 2022-09-18 21:32:36.543874 192.168.50.51          128.119.245.12         HTTP       562 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    254 2022-09-18 21:32:37.794430 128.119.245.12         192.168.50.51          HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
    367 2022-09-18 21:32:46.017968 192.168.50.51          184.84.50.154          HTTP       281 GET / HTTP/1.1
    478 2022-09-18 21:32:49.363499 192.168.50.51          180.102.111.81         HTTP       282 POST /cgi-bin/httpconn HTTP/1.1
    482 2022-09-18 21:32:49.417243 180.102.111.81         192.168.50.51          HTTP       304 HTTP/1.1 200 OK  (text/octet)
```

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

Ans： 增添了 Cache-Control 和 Authorization 两个部分（对比如下图）。



```
> Frame 209: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 65471, Dst Port: 80, Seq: 1, Ack: 1, Len: 508
v Hypertext Transfer Protocol
  v 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/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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
    \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: 254]
```



```
> Frame 672: 647 bytes on wire (5176 bits), 647 bytes captured (5176 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: c2:1b:15:c7:f8:56 (c2:1b:15:c7:f8:56)
> Internet Protocol Version 4, Src: 192.168.50.51, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54026, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
v Hypertext Transfer Protocol
  v 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
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 HBPC/12.0.0.300\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/2]
    [Response in frame: 693]
    [Next request in frame: 694]
```

三、 补充内容：

favicon

在第一次抓包过程中，观察到 Wireshark 除了抓到了相应的 GET/OK 包，在过程也向服务器发送 GET /favicon.ico HTTP/1.1 报文。查阅资料了解到：favicon，即 Favorites Icon 的缩写，是指显示在浏览器收藏夹、地址栏和标签标题前面的个性化图标。 以图标的方式区别不同的网站。由于实验网址中并未进行相关的设置，浏览器返回 404 Not Found 报文，并记录进错误日志。

缓存控制

在 http 中，控制缓存开关的字段有两个：Pragma 和 Cache-Control。其中 Pragma 含有 Pragma 和 Expires 两个字段。当 Pragma 字段的值为 no-cache 时，表示禁用缓存，Expires 的值为一个 GMT 时间，表示该缓存的有效时间。如果一个报文中同时出现 Pragma 和 Cache-Control 时，以 Pragma 为准。同时出现 Cache-Control 和 Expires 时，以 Cache-Control 为准。即优先级从高到低为 Pragma -> Cache-Control -> Expires
值得注意的是，Cache-Control 除了在响应中使用，在请求中也可以使用。

Base64 编码

Base64 即包括小写字母 a-z、大写字母 A-Z、数字 0-9、符号"+"、"/"一共 64 个字符的字符集，(若算上“=”，实际是 65 个字符)。将任何符号转换为该字符集中的字符的过程叫 base64 编码。在编码时，需要首先将字符串（图片等）转换成二进制序列，然后按每 6 个二进制位为一组，分成若干组，如果不足 6 位，则低位补 0。每 6 位组成一个新的字节，高位补 00，构成一个新的二进制序列，最后根据 base64 索引表中的值找到对应的字符从而构成相应的字符列。