中国科学技术大学计算机学院
《计算机网络》实验报告

实验题目：lab2 利用 Wireshark 观察 http 报文

学生姓名：张舒恒

学生学号：PB19030888

专业：计算机科学与技术

授课老师：华蓓

完成日期：2021 年 9 月 21 日

一、实验目的

1、 熟悉并掌握 wireshark；

2、 通过捕获观察并分析 http 报文，理解 http；

二、实验原理

Wireshark 是一个 packet 分析工具，可以抓取 packet，并分析出详细信息。Wireshark 使用 wincap 作为接口，直接与网卡进行 packet 交换，监听共享网络上传送的 packet。

三、实验环境

1、 硬件： pc 一台

2、 软件： Win10 Professional 1703

Wireshark2.4.0

四、实验过程

1、Wireshark 的安装

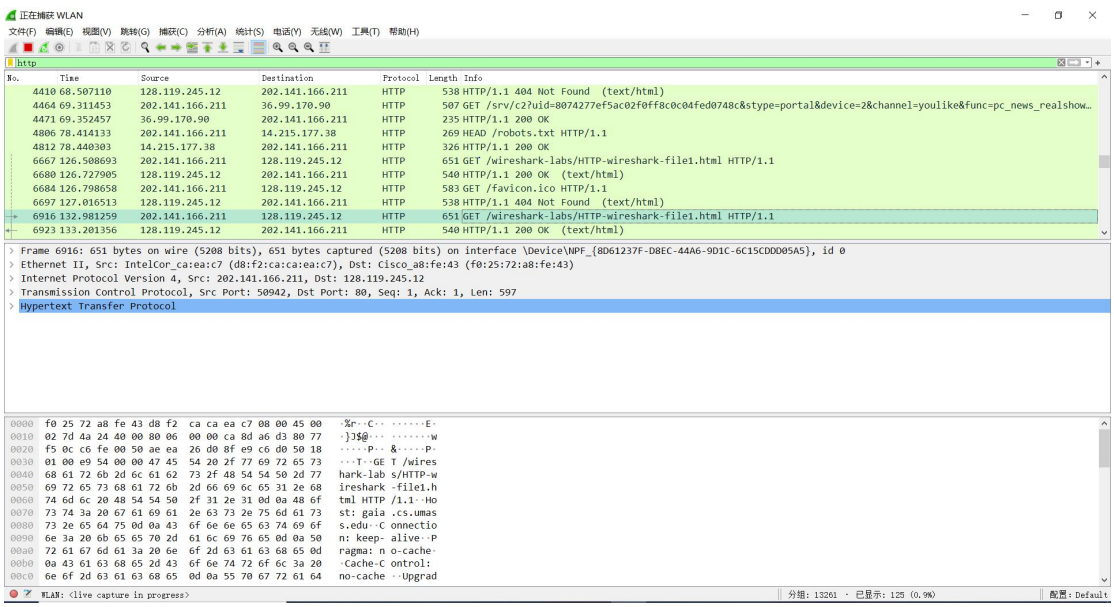
实验 1 已完成

2、利用 Wireshark 观察 http 报文并回答问题

•The Basic HTTP GET/response interaction

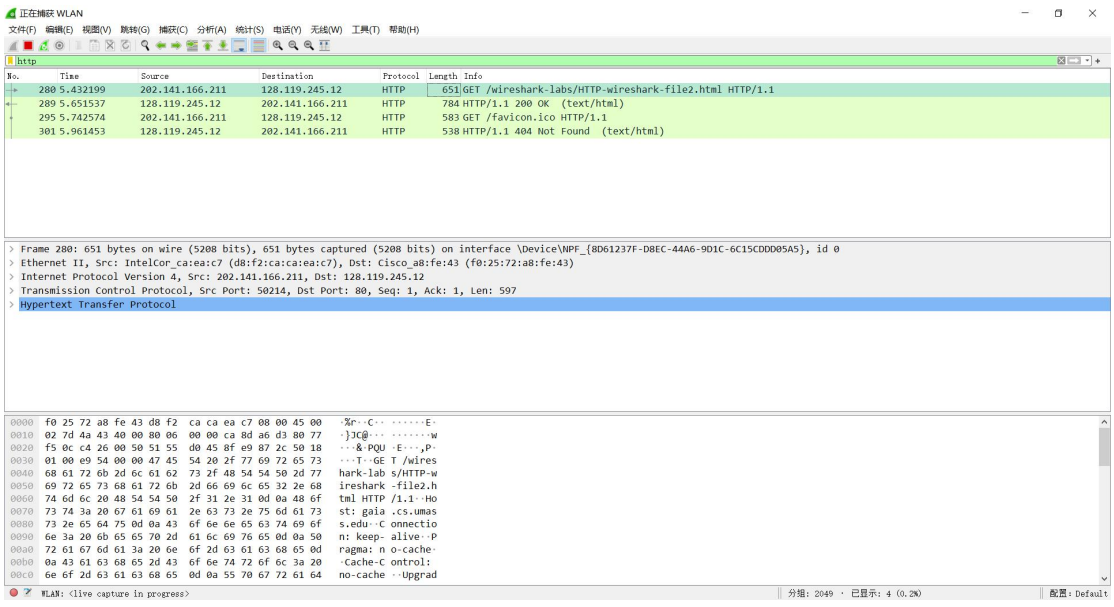
打开 edge，打开 wireshark，稍等片刻，开始捕获同时设置过滤为“http”，打开 

停止捕获。得到下图：



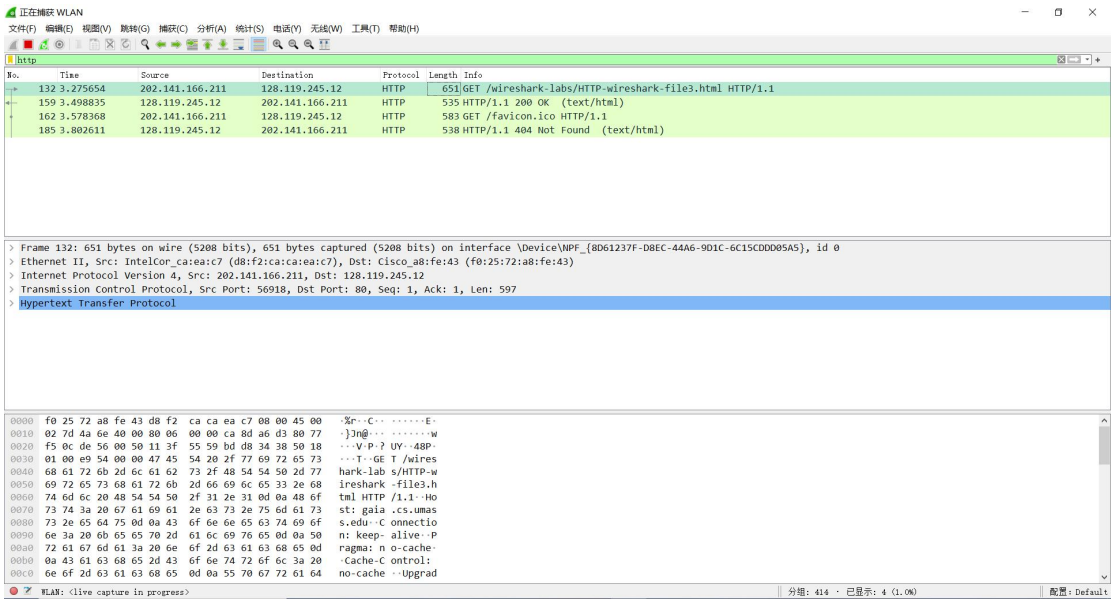
•The HTTP CONDITIONAL GET/response interaction

清除浏览器缓存，重新打开 wireshark 开始捕获，重新打开浏览器，打开网页 http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html，并快速刷新一次，停止捕获。观察 wireshark 中 http 报文。得到下图：



•Retrieving Long Documents

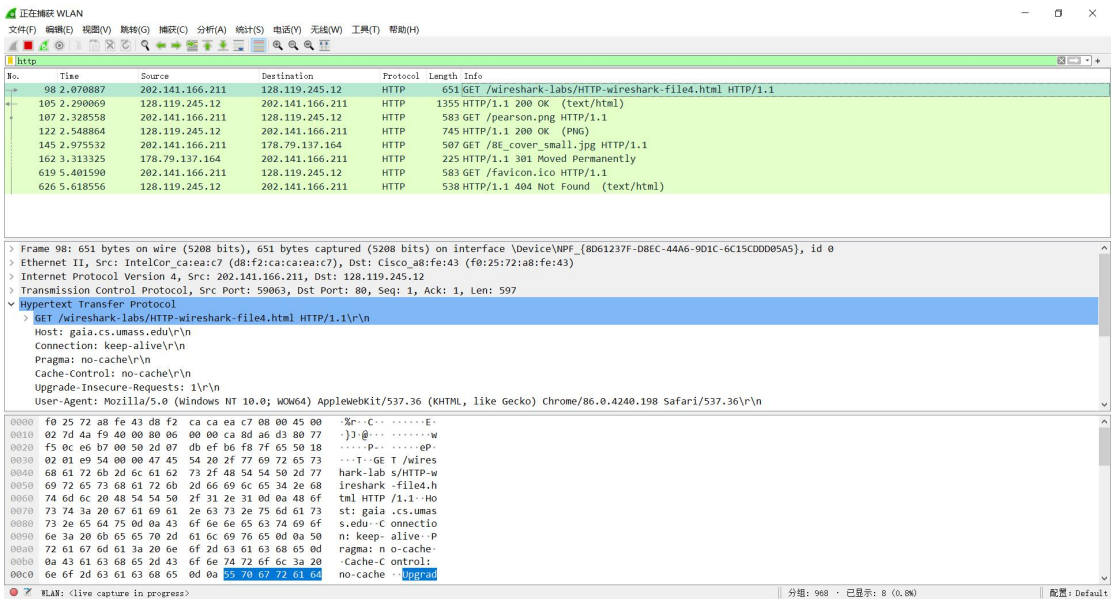
清除浏览器缓存，打开 wireshark 开始捕获，打开网页 http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html，停止捕获，得到：



•HTML Documents with Embedded Objects

清除浏览器缓存，打开 wireshark 开始捕获，打开网页

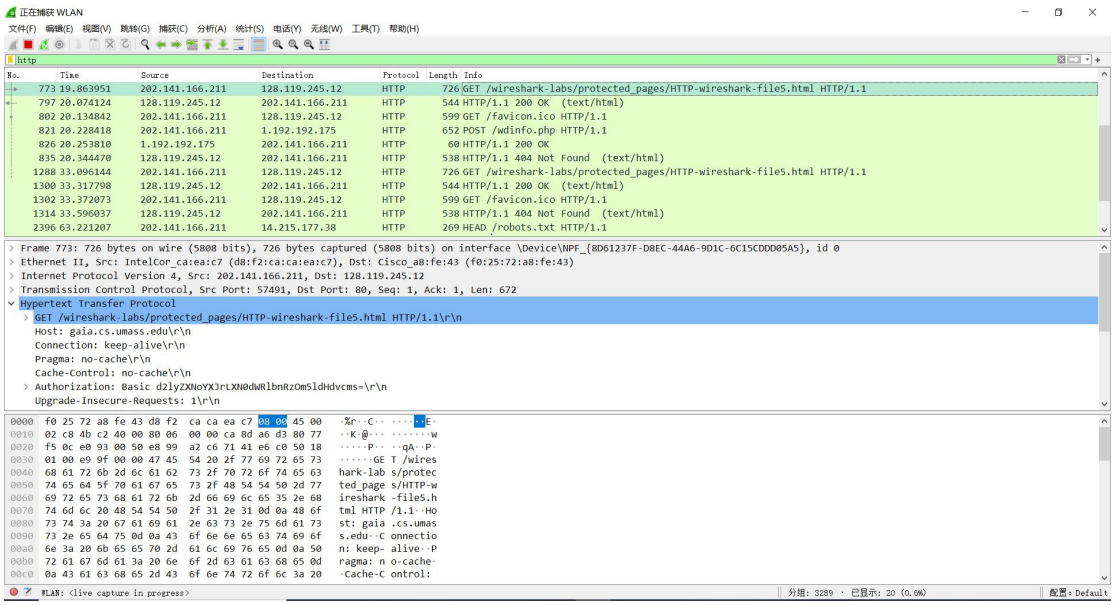
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html 等到两张图片加载完毕，停止捕获。得到下图：



•HTTP Authentication

清除浏览器缓存，开始捕获，打开网页

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html 并输入用户名密码，加载完毕之后停止捕获。得到下图



五、问题回答

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

答：都是 HTTP 1.1

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

答：中文 `Accept-Language: zh-CN,zh;q=0.9\r\n`

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

答：我的是 202.141.166.211，服务器的是 128.119.245.12

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

答：200 `Status Code: 200`

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

答：
```
Last-Modified: Tue, 21 Sep 2021 05:59:01 GMT\r\n
```

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

答：128 字节
```
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.

答：没有。仅有两条 HTTP 请求。

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?

答：没有

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

答：第一次的回应确实返回了文件内容，因为这次的报文里包含了 Content-Type:text/html 和 Content-Length。

```
> 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
```

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?

答：有。`If-Modified-Since: Wed, 22 Sep 2021 05:59:01 GMT\r\n`

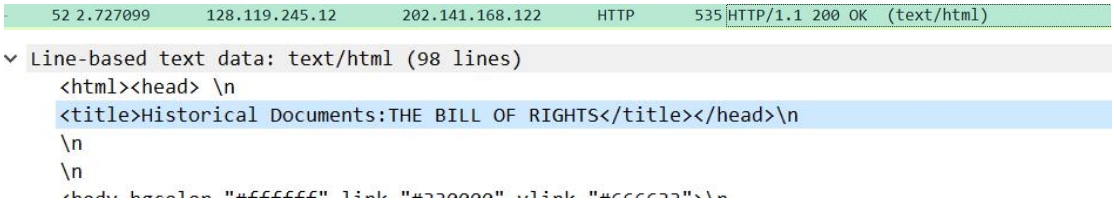
它后面是上一次 response 时发送的文件 Last-Modified 对应的时间。

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.

答：304 Not Modified。没有实际发送文件内容。因为这次的 response 没有 Content-Type，Content-Length，说明没有文件内容发过来

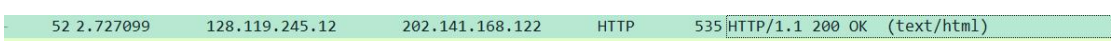
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

答：1 个，52



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

答：52，状态代码是 200 OK。



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

答：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?

答：4 个

```
[4 Reassembled TCP Segments (4861 bytes): #49(1460), #50(1460), #51(1460), #52(481)]
    [Frame: 49, payload: 0-1459 (1460 bytes)]
    [Frame: 50, payload: 1460-2919 (1460 bytes)]
    [Frame: 51, payload: 2920-4379 (1460 bytes)]
    [Frame: 52, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205765642c203232205365702032…]
```

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

答：3 个。发往 gaia.cs.umass.edu（128.119.245.12）。

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.

答：parallel，因为 person.png 发出后没等到 person.png 的 response 回来，就已经发送了 cover_5th_ed.jpg 的 get 请求了

174	19:12:12.489430	192.168.43.174	128.119.245.12	HTTP	518 GET /pearson.png HTTP/1.1
191	19:12:12.815431	192.168.43.174	128.119.240.90	HTTP	532 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
198	19:12:12.842127	128.119.245.12	192.168.43.174	HTTP	946 HTTP/1.1 200 OK (PNG)
202	19:12:12.881447	192.168.43.174	128.119.245.12	HTTP	328 GET /favicon.ico HTTP/1.1
225	19:12:13.222090	128.119.245.12	192.168.43.174	HTTP	539 HTTP/1.1 404 Not Found (text/html)
237	19:12:13.447085	192.168.43.174	128.119.240.90	HTTP	532 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
358	19:12:14.725647	128.119.240.90	192.168.43.174	HTTP	626 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?

答：401 Unauthorized

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

答：Authorizations：Basic

```
Connection: Keep-Alive\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
\r\n
```

六、实验总结

通过本次实验我学会了利用 Wireshark 观察 http 报文，并详细分析了 http 报文结构和细节。