

**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： PB18000006**

**姓 名： 范翔宇**

**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 11 月 14 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、 实验条件

- 1、 硬件条件： 联想拯救者 Y7000:

i5-8300H 2.30GHz

16G 内存

Intel UHD Graphics 630

- 2、 软件条件： Win10

Wireshark3.4.0

## 四、 实验过程

- 1、 Wireshark 的安装

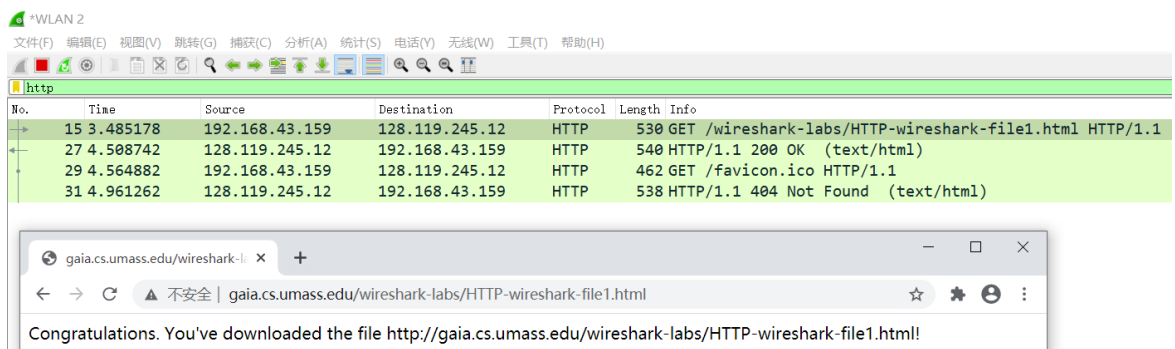
到官网 <https://www.wireshark.org/#download> 下载 windows 64bit 版。

## 2、 利用 Wireshark 观察 http 报文并回答问题

- The Basic HTTP GET/response interaction

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

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> 打开后，停止捕获，得到：

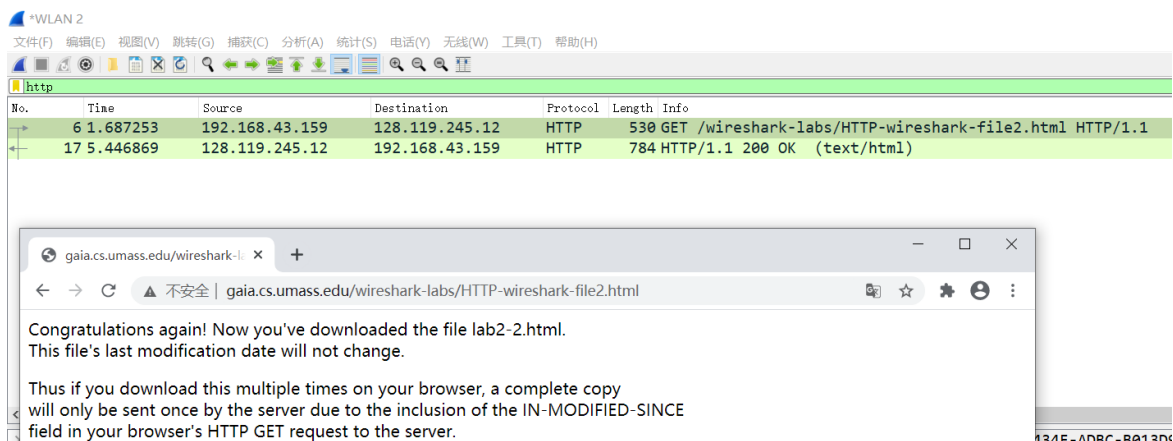


- The HTTP CONDITIONAL GET/response interaction

清除浏览器缓存，重新打开 wireshark 开始捕获，重新打开浏览器，

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> 打开，并快速刷新一次，停止捕获。观察 wireshark 中 http 报文。

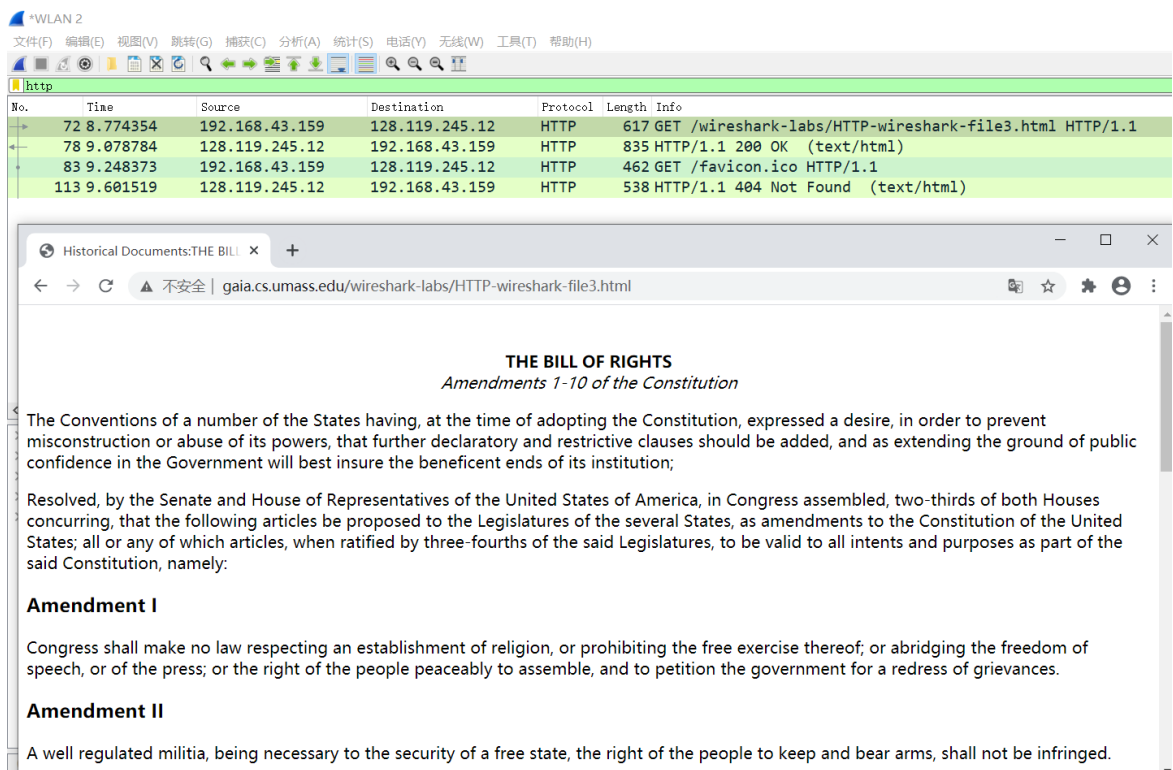
得到：



## • Retrieving Long Documents

清除浏览器缓存，打开 wireshark 开始捕获，打开网页

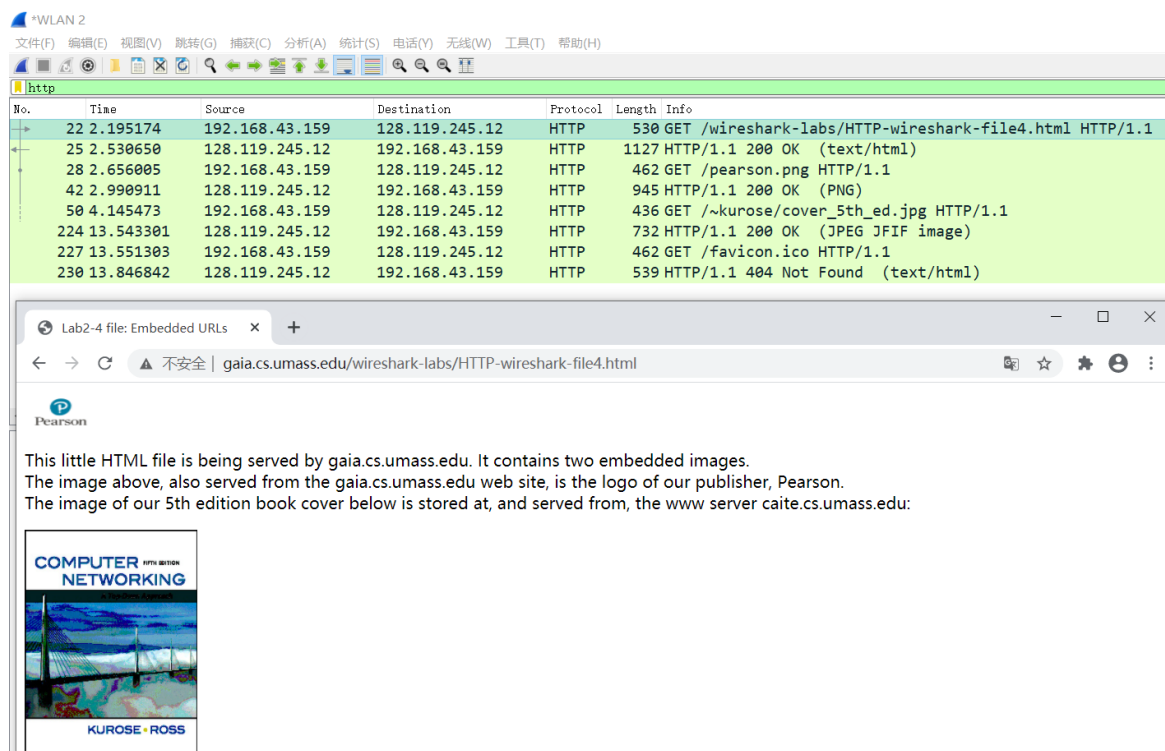
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>, 停止捕获，得到：



## • 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：

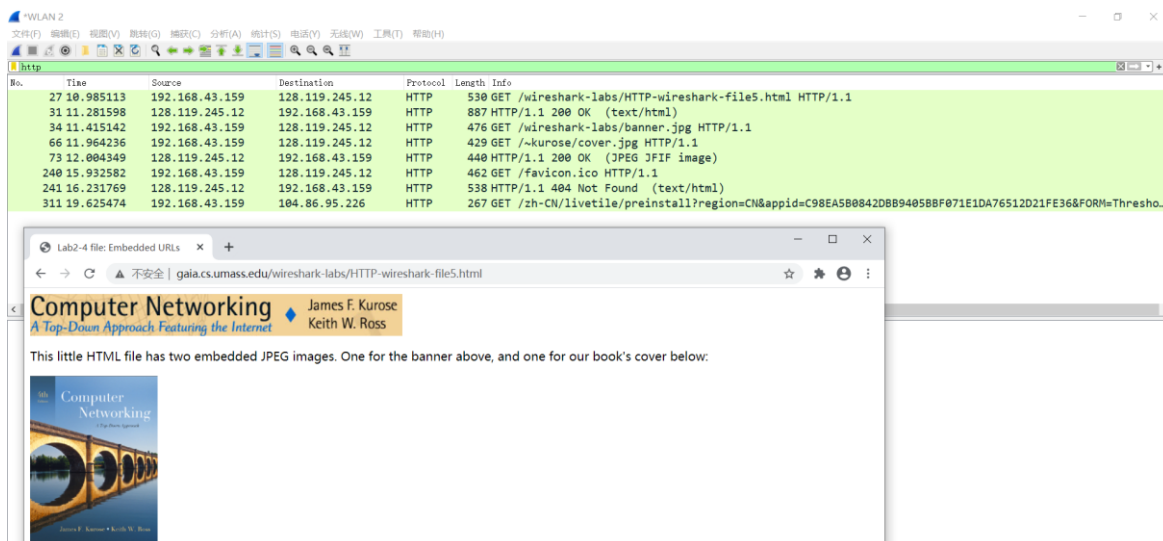


The image shows a Wireshark packet capture of an HTTP transaction and a screenshot of the corresponding web browser. The Wireshark interface displays a list of packets, with the selected packet being an HTTP GET request for the HTML file. The browser screenshot shows the HTML content, which includes two embedded images: the Pearson logo and the cover of the book 'Computer Networking: A Top-Down Approach' by Kurose and Ross.

No.	Time	Source	Destination	Protocol	Length	Info
22	2.195174	192.168.43.159	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
25	2.530650	128.119.245.12	192.168.43.159	HTTP	1127	HTTP/1.1 200 OK (text/html)
28	2.656005	192.168.43.159	128.119.245.12	HTTP	462	GET /pearson.png HTTP/1.1
42	2.990911	128.119.245.12	192.168.43.159	HTTP	945	HTTP/1.1 200 OK (PNG)
50	4.145473	192.168.43.159	128.119.245.12	HTTP	436	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
224	13.543301	128.119.245.12	192.168.43.159	HTTP	732	HTTP/1.1 200 OK (JPEG JFIF image)
227	13.551303	192.168.43.159	128.119.245.12	HTTP	462	GET /favicon.ico HTTP/1.1
230	13.846842	128.119.245.12	192.168.43.159	HTTP	539	HTTP/1.1 404 Not Found (text/html)

清除浏览器缓存，打开 wireshark 开始捕获，打开网页

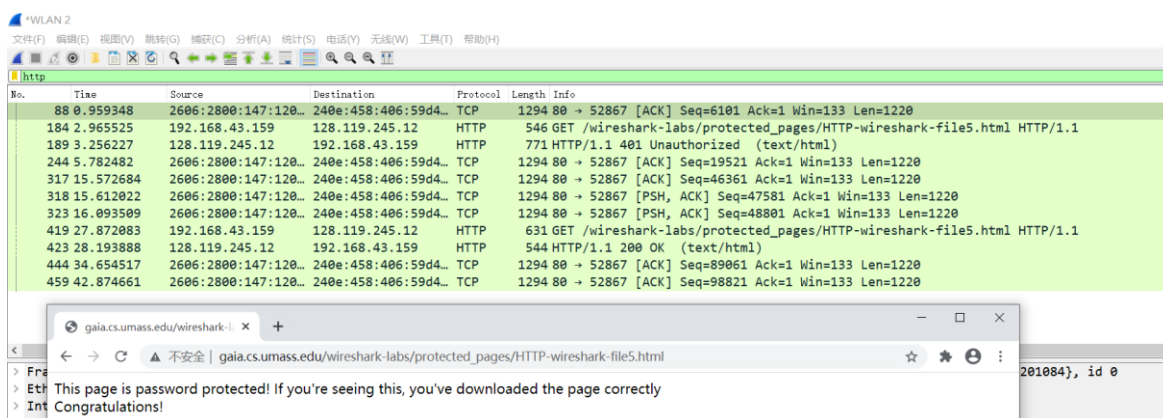
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html> 等到两张图片加载完毕，停止捕获。得到：



## • 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](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、 结果分析

以下是《http 报文抓取及分析》对应的回答

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，如下图：

32	21.541278	192.168.43.159	128.119.245.12	HTTP	530 GET /wireshark-labs/HTTP-wireshark-file1.html	HTTP/1.1
37	21.841566	128.119.245.12	192.168.43.159	HTTP	540 HTTP/1.1 200 OK (text/html)	

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

答：简体中文（大陆使用）、简体中文。如下图：

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 192.168.43.159，服务器的是 128.119.245.12

5	1.612609	192.168.43.159	128.119.245.12	HTTP	530 GET /wireshark-labs/HTTP-wireshark-file1.html	HTTP/1.1
---	----------	----------------	----------------	------	---	----------

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

Status Code: 200

答：200 [Status Code Description: OK]

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

答：Last-Modified: Sat, 14 Nov 2020 06:59:02 GMT\r\n

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

答：128 字节，如下图

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：Server, Last-Modified 等

Date: Sat, 14 Nov 2020 10:02:17 GMT\r\n  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod\_perl/2.0.11 Perl/v5.16.3\r\n  
Last-Modified: Sat, 14 Nov 2020 06:59:02 GMT\r\n  
ETag: "80-5b40bae1a9518"\r\n  
Accept-Ranges: bytes\r\n

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
  [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
```

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: Sat, 14 Nov 2020 06:59:02 GMT\r\n
```

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

```
Last-Modified: Sat, 14 Nov 2020 06:59:02 GMT\r\n
```

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file?

Explain.

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

```
Status Code: 304
[Status Code Description: Not Modified]
```

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

答：1个

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



```

TCP payload (781 bytes)
TCP segment data (781 bytes)
v [4 Reassembled TCP Segments (4861 bytes): #27(1360), #28(1360), #30(1360), #31(781)]
  [Frame: 27, payload: 0-1359 (1360 bytes)]
  [Frame: 28, payload: 1360-2719 (1360 bytes)]
  [Frame: 30, payload: 2720-4079 (1360 bytes)]
  [Frame: 31, payload: 4080-4860 (781 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a205361742c203134204e6f762032...]

```

答：4个。

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

答：200 OK

**Status Code: 200**

**[Status Code Description: OK]**

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

答：没有。正如 lab 的 pdf 里面提到的

long, and at 4500 bytes is too large to fit in one TCP packet. The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment (see Figure 1.20 in the text). Each TCP segment is recorded as a separate packet by Wireshark, and the fact that the single HTTP response was fragmented across multiple TCP packets is indicated by the “Continuation” phrase displayed by Wireshark. We stress here that there is no “Continuation” message in HTTP!

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

答：一共4个。均发往gaia.cs.umass.edu (128.119.245.12)。

367	9.713560	192.168.43.159	128.119.245.12	HTTP	530 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
377	10.668007	128.119.245.12	192.168.43.159	HTTP	1127 HTTP/1.1 200 OK (text/html)
380	10.845226	192.168.43.159	128.119.245.12	HTTP	462 GET /pearson.png HTTP/1.1
414	11.153330	128.119.245.12	192.168.43.159	HTTP	945 HTTP/1.1 200 OK (PNG)
431	11.204157	192.168.43.159	128.119.245.12	HTTP	436 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
681	16.159064	192.168.43.159	128.119.245.12	HTTP	462 GET /favicon.ico HTTP/1.1
691	16.465654	128.119.245.12	192.168.43.159	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.

(从回答这题的时候，已经改了视图，增加了 CN 时间栏)

答：并行。两个图片是连续请求，不需要等第一个请求得到回复后才继

续第二次请求。存在不需要等第一个请求得到回复后才继续第二次请求的情况，说明是并行的：

57	2020-11-14 22:50:17.481240	192.168.43.159	128.119.245.12	HTTP	462 GET /pearson.png HTTP/1.1
66	2020-11-14 22:50:17.807744	192.168.43.159	128.119.245.12	HTTP	436 GET /~kurose/cover_5th_ed.jpg HTTP/1.1

答：401 Unauthorized

414	19.768808	192.168.43.159	128.119.245.12	HTTP	546 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
423	20.226273	128.119.245.12	192.168.43.159	HTTP	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?

答：Authorizations: Basic

▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n  
Credentials: wireshark-students:network

以下是《Wireshark 简介》对应的回答

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

答：TCP UDP HTTP TLSv1.2 OICQ ARP DNS RTPproxy NBNS MDNS

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 packetlisting 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*.)

答：约 0.36s

No.	Time	Source	Destination	Protocol	Length	Info
21	2020-11-14 21:43:08.858078	192.168.43.159	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
27	2020-11-14 21:43:09.233382	128.119.245.12	192.168.43.159	HTTP	540	HTTP/1.1 200 OK (text/html)

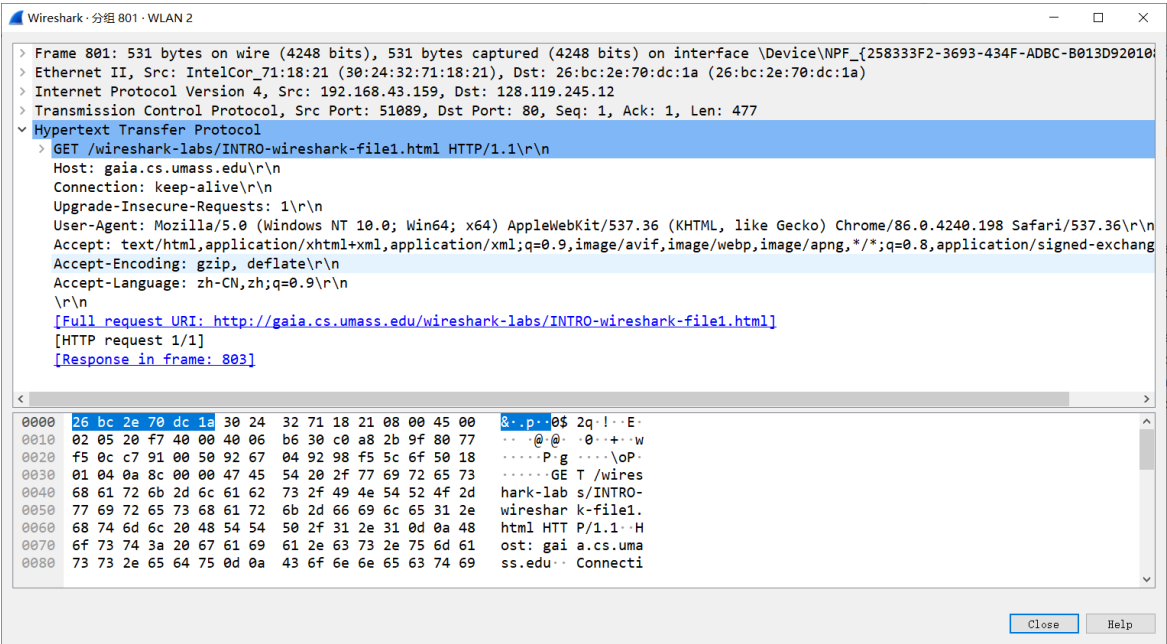
3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

答：128.119.245.12 192.168.43.159（本地）

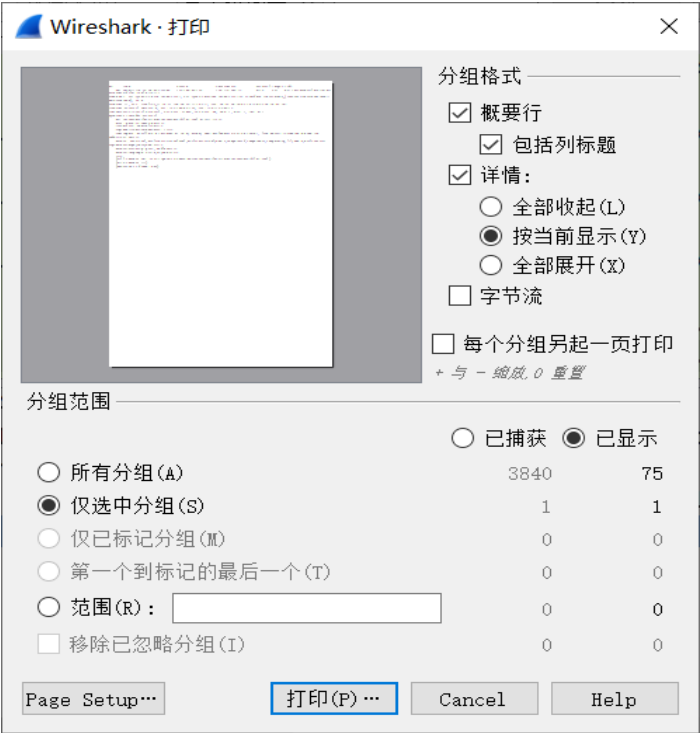
4. Print the two HTTP messages displayed in step 9 above. To do so, select *Print* from the Wireshark *File* command menu, and select “*Selected Packet Only*” and “*Print as displayed*” and then click OK.

答：

按步骤来~



没有打印机，大致操作是这样的



打印下来效果应该是这样的~

No.	Time	Source	Destination	Protocol	Length	Info
801	2020-11-14 23:26:45.223268	192.168.43.159	128.119.245.12	HTTP	531	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 801: 531 bytes on wire (4248 bits), 531 bytes captured (4248 bits) on interface \Device\NPF\_{258333F2-3693-434F-ADBC-B013D9201084}, id 0  
 Ethernet II, Src: IntelCor 71:18:21 (30:24:32:71:18:21), Dst: 26:bc:2e:70:dc:1a (26:bc:2e:70:dc:1a)  
 Internet Protocol Version 4, Src: 192.168.43.159, Dst: 128.119.245.12  
 Transmission Control Protocol, Src Port: 51089, Dst Port: 80, Seq: 1, Ack: 1, Len: 477  
 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
 Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 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
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]  
 [HTTP request 1/1]  
 [Response in frame: 803]

## 以下是《ppt》对应的回答

### 1. 分析 HTTP 中 *get* 和 *post* 请求方式的区别。

答：

- 通常意义上的区别：

GET 一般用于查询信息，

POST 一般用于改变信息。

- 原理上的区别：

根据 HTTP 规范，GET 用于信息的获取，应该是安全并且幂等的。

根据 HTTP 规范，POST 表示可能修改服务器上的资源的请求，是非幂等的。

- 实际中的区别：

1. GET 请求将请求的数据附在 URL 之后，

POST 将请求的数据放在 HTTP 包的包体中。而实际中浏览器或者操作系统可能对 url 长度进行限制，所以 GET, POST 此时所能传输的信息有区别。

2. POST 的安全性别 GET 高。

对于密码等隐私数据，GET 会放在 url 上，而 POST 不会。