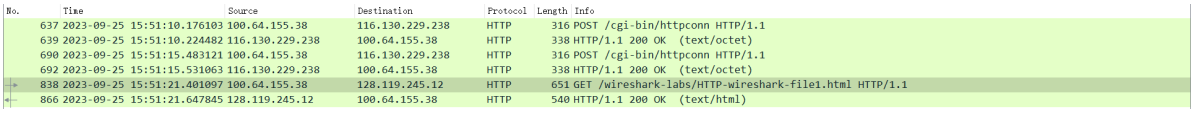
计网实验2

第一部分

T1

> 您的浏览器是否运行HTTP版本1.0或1.1？服务器运行什么版本的HTTP？



No.	Time	Source	Destination	Protocol	Length	Info
637	2023-09-25 15:51:10.176103	100.64.155.38	116.130.229.238	HTTP	316	POST /cgi-bin/httpconn HTTP/1.1
639	2023-09-25 15:51:10.224482	116.130.229.238	100.64.155.38	HTTP	338	HTTP/1.1 200 OK (text/octet)
690	2023-09-25 15:51:15.483121	100.64.155.38	116.130.229.238	HTTP	316	POST /cgi-bin/httpconn HTTP/1.1
692	2023-09-25 15:51:15.531063	116.130.229.238	100.64.155.38	HTTP	338	HTTP/1.1 200 OK (text/octet)
838	2023-09-25 15:51:21.401097	100.64.155.38	128.119.245.12	HTTP	651	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
866	2023-09-25 15:51:21.647845	128.119.245.12	100.64.155.38	HTTP	540	HTTP/1.1 200 OK (text/html)

由图，可以看出浏览器和服务器均为HTTP/1.1

T2

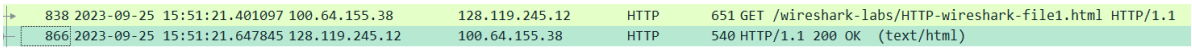
> 您的浏览器向服务器指示了它能接受哪种语言？

```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
If-None-Match: "80-6062826f122e0"\r\n
```

accept-language这一行，展示了浏览器更能接受中文，也可以接受英文（包含英式、美式或者其他英语）

T3

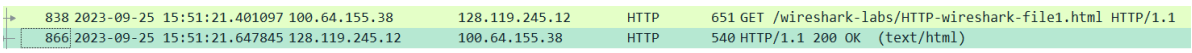
> 您的计算机的IP地址是什么？ http://gaia.cs.umass.edu服务器地址呢？



我的ip地址是100.64.155.38，http://gaia.cs.umass.edu服务器地址是128.119.245.12

T4

> 服务器返回到浏览器的状态代码是什么？



第二行返回浏览器，代码为200

T5

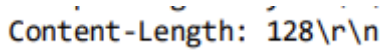
> 服务器上HTML文件的最近一次修改是什么时候？

```
Last-Modified: Mon, 25 Sep 2023 05:59:02 GMT\r\n
```

2023年9月25日 5:59:02

T6

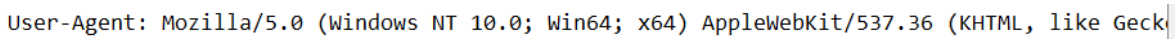
> 服务器返回多少字节的内容到您的浏览器？



128

T7

> 通过检查分组内容窗口中的原始数据，你是否看到有协议头在分组列表窗口中未显示？ 如果是，请举一个例子。



例如这个在分组列表窗口中未显示，在details中显示了

第二部分

T8

> 检查第一个从您浏览器到服务器的HTTP GET请求的内容。您在HTTP GET中看到了“**IF-MODIFIED-SINCE**”首部字段吗？

```
> Frame 150: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface \Device
> Ethernet II, Src: IntelCor_f3:ce:f6 (e8:84:a5:f3:ce:f6), Dst: HuaweiTe_8a:5d:45 (c8:33:e5:8a:
> Internet Protocol Version 4, Src: 100.64.155.38, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 12395, Dst Port: 80, Seq: 1, Ack: 1, Len: 512
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 188]
```

没有

T9

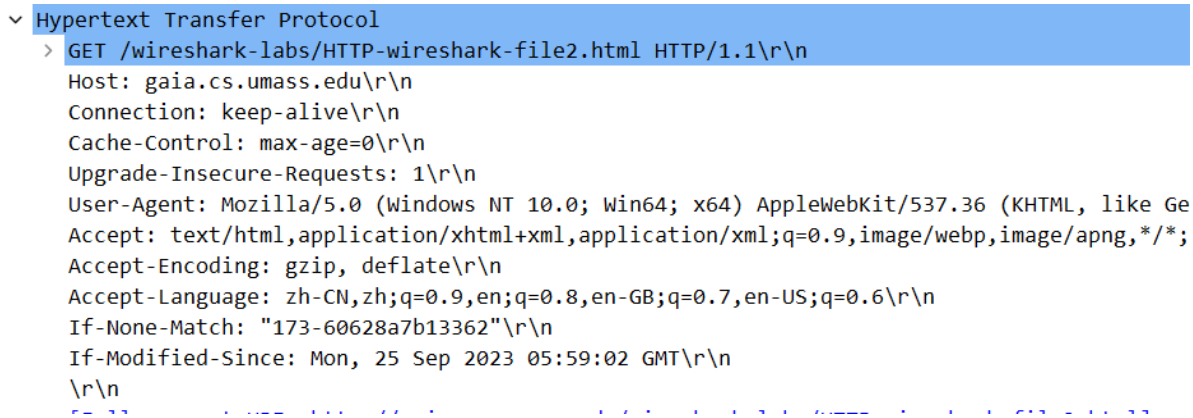
> 检查服务器响应的内容。服务器是否显式返回文件的内容？ 你是怎么知道的？

```
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.278589000 seconds]
    [Request in frame: 150]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
v Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

由上图可以看出，显式返回了文件内容

T10

> 现在，检查第二个HTTP GET请求的内容。 您在HTTP GET中看到了“**IF-MODIFIED-SINCE**”首部字段吗？ 如果是，“**IF-MODIFIED-SINCE**”首部字段包含哪些信息？



有，包含了上次修改的时间，与上一次中的last-modified时间相同，都是2023.9.25 5:59:02

T11

> 针对第二个HTTP GET，从服务器响应的HTTP状态码和短语是什么？服务器是否明确地返回文件的内容？请解释。

```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Mon, 25 Sep 2023 10:12:32 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "173-60628a7b13362"\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.276416000 seconds]
  [Request in frame: 89]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

可以看出，状态码和短语是304 Not Modified

没有明确返回，因为请求对象没有被修改，返回的话会浪费资源

第三部分

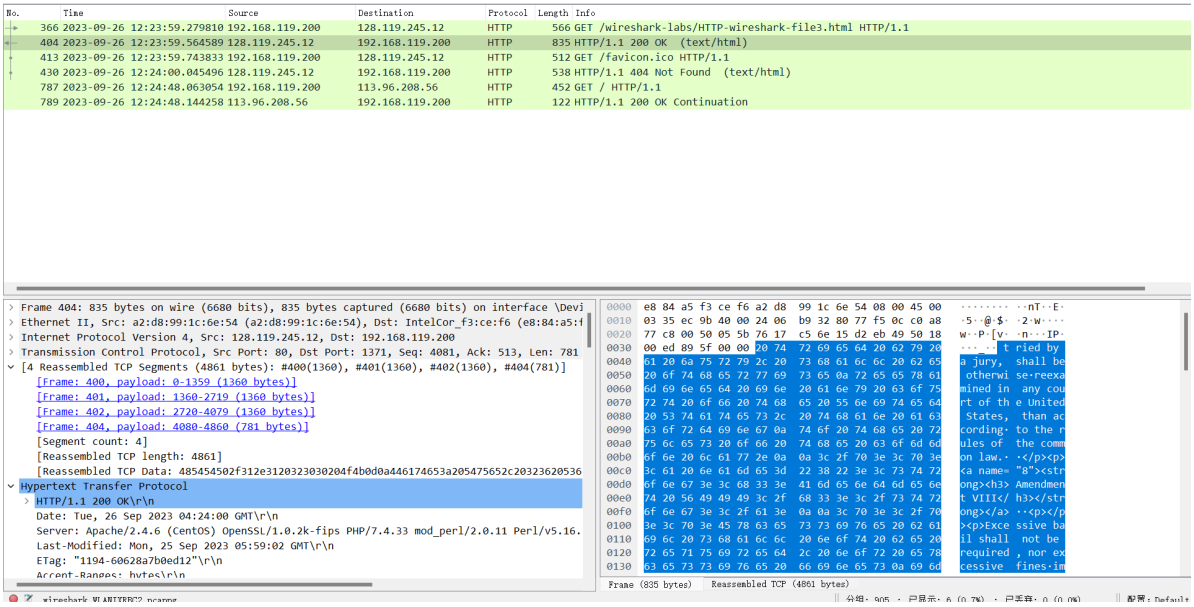
T12

> 您的浏览器发送多少HTTP GET请求报文？哪个分组包含了美国权利法案的消息？

一条；四个都包含了

T13

> 哪个分组包含响应HTTP GET请求的状态码和短语？



404那条

T14

> 响应中的状态码和短语是什么？

200 OK

T15

> 需要多少包含数据的TCP报文段来执行单个HTTP响应和权利法案文本？

```
[4 Reassembled TCP Segments (4861 bytes): #400(1360), #401(1360), #402(1360), #404(781)]
   [Frame: 400, payload: 0-1359 (1360 bytes)]
   [Frame: 401, payload: 1360-2719 (1360 bytes)]
   [Frame: 402, payload: 2720-4079 (1360 bytes)]
   [Frame: 404, payload: 4080-4860 (781 bytes)]
   [Segment count: 4]
   [Reassembled TCP length: 4861]
   [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205475652c20323620536
```

4个

第四部分

T16

> 您的浏览器发送了几个HTTP GET请求报文？ 这些GET请求发送到哪个IP地址？

No.	Time	Source	Destination	Protocol	Length	Info
138	2023-09-27 14:39:27.497631	100.64.191.48	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file4.htm
159	2023-09-27 14:39:27.765072	128.119.245.12	100.64.191.48	HTTP	1355	HTTP/1.1 200 OK (text/html)
170	2023-09-27 14:39:27.821743	100.64.191.48	128.119.245.12	HTTP	512	GET /pearson.png HTTP/1.1
202	2023-09-27 14:39:28.089157	128.119.245.12	100.64.191.48	HTTP	905	HTTP/1.1 200 OK (PNG)
241	2023-09-27 14:39:29.026431	100.64.191.48	178.79.137.164	HTTP	479	GET /8E_cover_small.jpg HTTP/1.1
250	2023-09-27 14:39:29.372168	178.79.137.164	100.64.191.48	HTTP	225	HTTP/1.1 301 Moved Permanently

三个

两个到128.119.245.12

一个到178.79.137.164

T17

> 浏览器从两个网站串行还是并行下载了两张图片？请说明。

串行，第一张确认后才开始第二次请求

第五部分

T18

> 对于您的浏览器的初始HTTP GET消息，服务器响应（状态码和短语）是什么响应？

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

状态码：401

短语：Unauthorized

T19

> 当您的浏览器第二次发送HTTP GET消息时，HTTP GET消息中包含哪些新字段？

```
> Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
```

Authorization这个新字段