WireShark 实验-HTTP

专业班级： 信息安全智息技术班　　**学号：** 21307130076　　**姓名：** 杨乙

【实验目的】

探索 HTTP 协议的几个方面：基本的 GET/response 交互，HTTP 消息格式等。

【实验结果】

```
No.     Time           Source                Destination           Protocol Length Info
   7600 3.677394       192.168.1.104 3       128.119.245.12 3      HTTP     578    GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1
Frame 7600: 578 bytes on wire (4624 bits), 578 bytes captured (4624 bits) on interface \Device\NPF_{84F30BE1-7874-473F-
BB1D-9A7FAE3D946F}, id 0
Ethernet II, Src: IntelCor_0e:b9:c4 (98:8d:46:0e:b9:c4), Dst: Tp-LinkT_45:e9:4e (3c:06:a7:45:e9:4e)
Internet Protocol Version 4, Src: 192.168.1.104, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60496, Dst Port: 80, Seq: 1, Ack: 870072584, Len: 512
Hypertext Transfer Protocol
    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 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/110.0.0.0 Safari/
537.36 Edg/110.0.1587.57\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\r\n
    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 2
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 7718]
```

```
No.     Time           Source                Destination           Protocol Length Info
   7718 3.920614       128.119.245.12        192.168.1.104         HTTP     552    HTTP/1.1 200 OK  (text/html)
Frame 7718: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{84F30BE1-7874-473F-
BB1D-9A7FAE3D946F}, id 0
Ethernet II, Src: Tp-LinkT_45:e9:4e (3c:06:a7:45:e9:4e), Dst: IntelCor_0e:b9:c4 (98:8d:46:0e:b9:c4)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.104
Transmission Control Protocol, Src Port: 80, Dst Port: 60496, Seq: 870072584, Ack: 513, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1 1
        Status Code: 200 4
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 27 Feb 2023 12:35:17 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\r\n
    Last-Modified: Mon, 27 Feb 2023 06:59:01 GMT\r\n 5
    ETag: "80-5f5a903938b20"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.243220000 seconds]
    [Request in frame: 7600]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes 6
Line-based text data: text/html (4 lines)
```

（答案出现的具体位置见消息中的标注）

1. 浏览器是运行的 HTTP 版本：HTTP 1.1
   服务器运行的 HTTP 版本号：HTTP 1.1

2. 浏览器从服务器接受哪种语言：
   优先接收简体中文（zh-CN），其次分别是中文（zh）、英语（en）、英式英语（en-GB）、美式英语（en-US），q 表示出现在它之前的语言的权重

3. 我的计算机 IP 地址：192.168.1.104
   gaia.cs.umass.edu 服务器地址：128.119.245.12

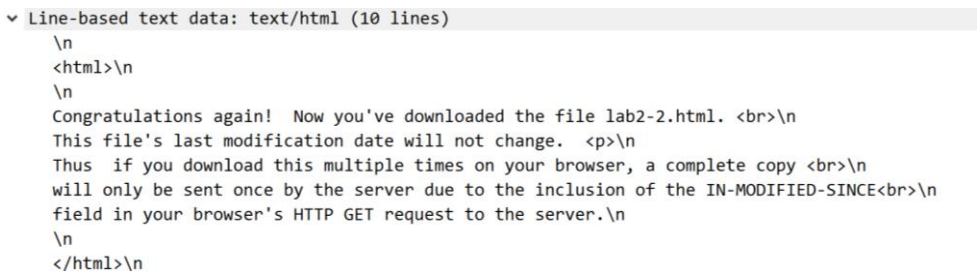
4. 服务器返回到浏览器的状态代码：200

5. 服务器上 HTML 文件最近一次修改时间：27 Feb 2023 06:59:01（观察到最近一次修改时间并不是一分钟以前，猜想可能是修改未被检测到）

6. 服务器返回多少字节的内容到您的浏览器：128 字节

7. 检查第一个从您浏览器到服务器的 HTTP GET 请求的内容，在 HTTP GET 中看到了"IF-MODIFIED-SINCE"行吗？
   没有

8. 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？



是。上图中的文本就是服务器显式返回的文件内容。

9. 检查第二个 HTTP GET 请求的内容。您在 HTTP GET 中看到了"IF-MODIFIED-SINCE:"行吗？如果是，"IF-MODIFIED-SINCE:"头后面包含哪些信息？

```
If-Modified-Since: Mon, 27 Feb 2023 06:59:01 GMT\r\n
```

是。如上图，"IF-MODIFIED-SINCE:"头后面包含了时间信息，可以发现之前的最近一次修改时间相同。查阅资料知：IF-MODIFIED-SINCE 是标准的 HTTP 请求头标签，在发送 HTTP 请求时，把浏览器端缓存页面的最后修改时间一起发到服务器去，服务器会把这个时间与服务器上实际文件的最后修改时间进行比较。如果时间一致，那么返回 HTTP 状态码 304（不返回文件内容），客户端接到之后直接把本地缓存文件显示到浏览器中。

10. 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。

```
> [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
  Response Version: HTTP/1.1
  Status Code: 304
  [Status Code Description: Not Modified]
  Response Phrase: Not Modified
```

从服务器响应的 HTTP 状态码：304　短语：Not Modified
并没有找到服务器明确返回的文件内容。因为在第一次发送请求时网页内容被保存到缓存。如上所述，客户端收到返回的 304 状态码之后直接把本地缓存文件显示到浏览器中。

11. 您的浏览器发送了几个 HTTP GET 请求消息？这些 GET 请求发送到哪个 IP 地址？

http3	22878	192.168.1.104	128.119.245.12	HTTP	578 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
4585	5.395946	128.119.245.12	192.168.1.104	HTTP	1367 HTTP/1.1 200 OK (text/html)
4597	5.426324	192.168.1.104	128.119.245.12	HTTP	524 GET /pearson.png HTTP/1.1
4640	5.679255	128.119.245.12	192.168.1.104	HTTP	781 [TCP Previous segment not captured] Continuation
4649	5.842774	192.168.1.104	178.79.137.164	HTTP	491 GET /8E_cover_small.jpg HTTP/1.1
4680	6.196469	178.79.137.164	192.168.1.104	HTTP	237 HTTP/1.1 301 Moved Permanently

如图，浏览器发送了三个 HTTP GET 请求消息。前两个 GET 请求发送到 128.119.245.12 第三个 GET 请求发送到 178.79.137.164

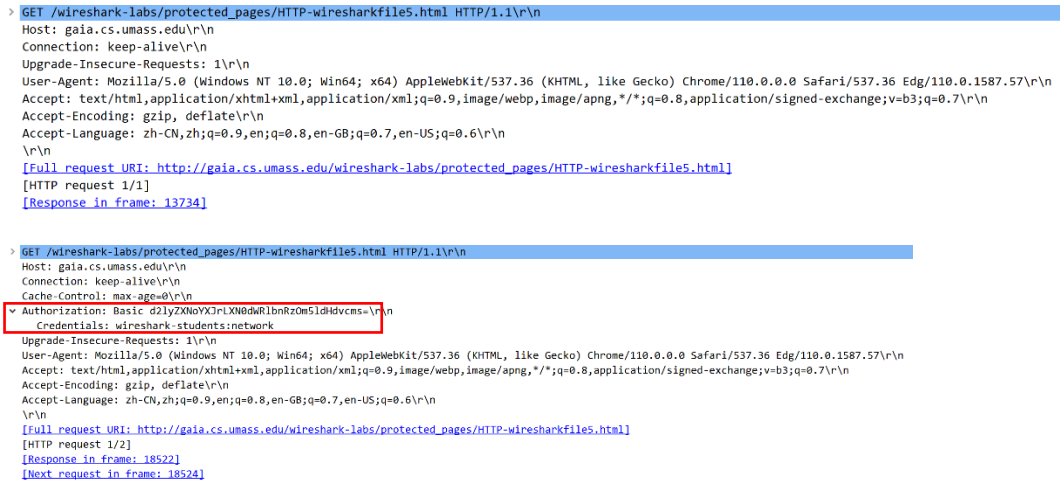
12. 浏览器从两个网站串行还是并行下载了两张图片？请说明
串行。根据后两个 HTTP GET 请求距离捕获开始的时间来看，当前一个请求收到回复之后，第二个请求才发出。因此推测浏览器从两个网站并行下载了两张图片

13. 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？

```
> [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
  Response Version: HTTP/1.1
  Status Code: 401
  [Status Code Description: Unauthorized]
  Response Phrase: Unauthorized
```

如上图，服务器响应是 401 Authorization Required，表示用户没有访问权限，需要进行身份认证。而相关信息尚未被提供，或已提供但没有通过授权测试。

14. 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？



```
> GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.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/110.0.0.0 Safari/537.36 Edg/110.0.1587.57\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  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/protected_pages/HTTP-wiresharkfile5.html]
  [HTTP request 1/1]
  [Response in frame: 13734]

> GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
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/110.0.0.0 Safari/537.36 Edg/110.0.1587.57\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  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/protected_pages/HTTP-wiresharkfile5.html]
  [HTTP request 1/2]
  [Response in frame: 18522]
  [Next request in frame: 18524]
```

如图，增加了 Authorization 字段和 Credentials 字段