# 计算机学院 计算机网络 课程实验报告

| 实验题目：实验二 ： 探讨 HTTP 协议 | | 学号：202200400053 |
|---|---|---|
| 日期：2024-03-15 | 班级： 2 班 | 姓名： 王宇涵 |
| Email：1941497679@qq.com | | |

**实验方法介绍：**

1. 通过清空浏览器缓存，打开给定网址进行抓包
2. 分析数据包信息，从而深入了解 HTTP 协议

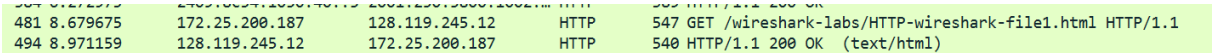
**实验过程描述：**

**一 ：基本 HTTP GET/响应交互**

1. 启动网络浏览器 google，WireShark，过滤 http 信息，开启抓包
2. 打开 fire1 网址，显示信息

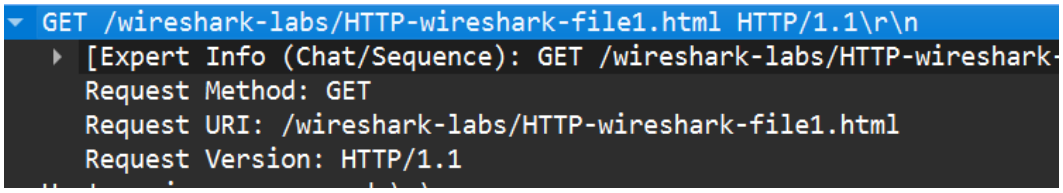
Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!

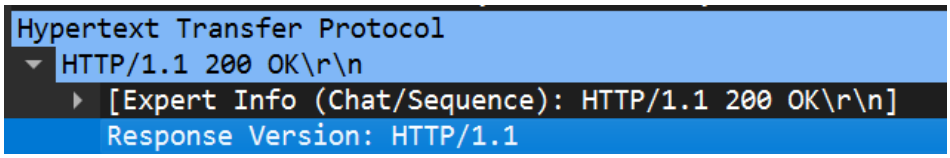
捕获 Get 数据包和 OK 数据包




回答问题 ：

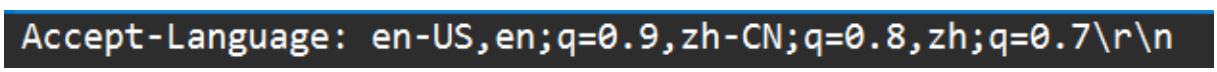
1. 您的浏览器运行的是 HTTP 版本 1.0、1.1 还是 2？服务器运行什么版本的 HTTP？




答： 浏览器运行版本 1.1，服务器运行版本为 1.1

2. 您的浏览器表明服务器可以接受哪些语言（如果有）？




答：首选的语言是英语（美国），其次是任何英语版本（en），然后是简体中文（zh-CN），最后是任何中文版本（zh）。

3. 您电脑的 IP 地址是多少？gaia.cs.umass.edu 服务器的 IP 地址是多 少？

答 ： 分别为 Src: 172.25.200.187, Dst: 128.119.245.12

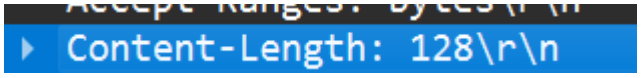
4. 服务器返回给浏览器的状态码是什么？


答 ：200 OK

5. 您正在检索的 HTML 文件最后一次在服务器上修改是什么时候？


答 ：Thu, 14 Mar 2024 05:59:01

6. 有多少字节的内容返回到您的浏览器？



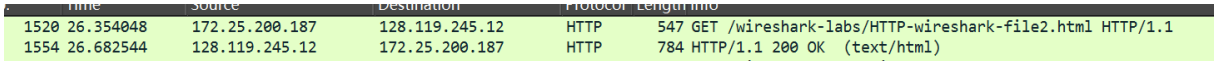

答: 128 字节

7. 通过检查数据包内容窗口中的原始数据，您是否看到数据中未显示在数据包列表窗口中的任何标头？如果有，请说出一个。

答：没有看到数据未显示标头的

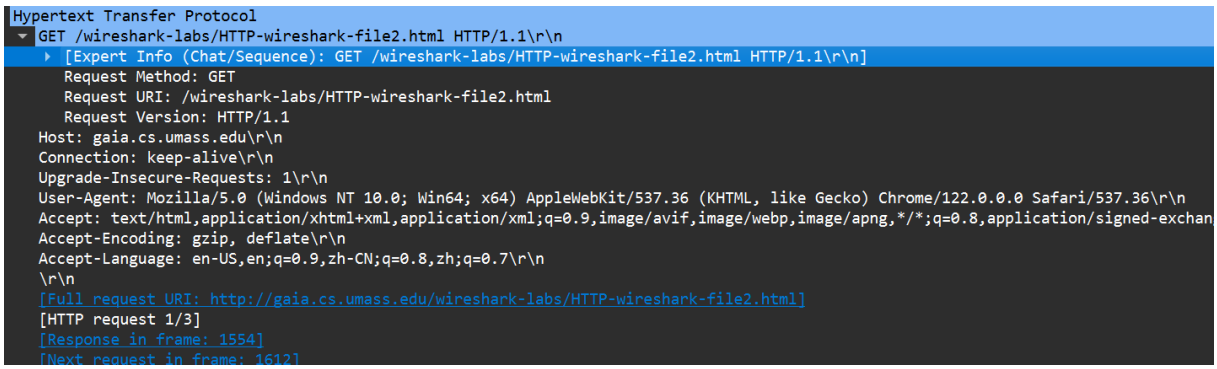
**二 ： HTTP 有条件交互**

1. 清除浏览器缓存，打开 fire2 文件，进行抓包
2. 得到结果




回答问题：

8. 检查从浏览器到服务器的第一个 HTTP GET 请求的内容。您是否在 HTTP GET 中看到“IF-MODIFIED-SINCE”行？




答 ： 没看到

9. 检查服务器响应的内容。服务器是否显式返回了文件的内容？你怎么知道？

```
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>\r
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

答 ：确实显示返回了文件的内容，可以在 line-based text data 中找到

10. 现在检查从浏览器到服务器的第二个 HTTP GET 请求的内容。您是否在 HTTP

GET 中看到“IF-MODIFIED-SINCE:”行6？如果是这样，“IF-MODIFIEDSINCE:”标头后面有哪些信息？

```
195 3.046274    172.25.200.187    128.119.245.12    HTTP    659 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
223 3.499032    128.119.245.12    172.25.200.187    HTTP    294 HTTP/1.1 304 Not Modified
```

答 ： 看到了该行， 信息为 `If-Modified-Since: Fri, 15 Mar 2024 05:59:02 GMT\r\n`

11. 服务器响应第二次 HTTP GET 返回的 HTTP 状态代码和短语是什么？服务器

是否显式返回了文件的内容？解释。

答 ： 返回的 HTTP 状态代码和短语为 `HTTP/1.1 304 Not Modified\r\n`，服务器没有显式返回文件的内容，可能是由于从 cache 中直接获取数据，文件没有被修改.

**三 ： 检索长文档**

1. 清除浏览器缓存，打开 fire3 网址进行抓包
2. 抓包失败，直接使用官方提供的文件

回答问题

```
26 3.813230    10.0.0.44         128.119.245.12    HTTP    547 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
27 3.841397    128.119.245.12    10.0.0.44         TCP      68 80 → 54985 [ACK] Seq=1 Ack=482 Win=30080 Len=0 TSval=3636786978 TSecr=492255584
28 3.841957    128.119.245.12    10.0.0.44         TCP    1514 80 → 54985 [ACK] Seq=1 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU]
29 3.841961    128.119.245.12    10.0.0.44         TCP    1514 80 → 54985 [ACK] Seq=1449 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU]
30 3.842054    10.0.0.44         128.119.245.12    TCP      66 54985 → 80 [ACK] Seq=482 Ack=2897 Win=128832 Len=0 TSval=492255612 TSecr=3636786980
31 3.842198    128.119.245.12    10.0.0.44         TCP    1514 80 → 54985 [ACK] Seq=2897 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU]
32 3.842202    128.119.245.12    10.0.0.44         HTTP    583 HTTP/1.1 200 OK  (text/html)
```

12. 您的浏览器发送了多少条 HTTP GET 请求消息？跟踪中的哪个数据包编号包含法案或权利的 GET 消息？

答 ：浏览器发送了一条 HTTP GET 请求数据，第 26 号编号包含了 get 信息

13. 跟踪中的哪个数据包编号包含与 HTTP GET 请求的响应相关的状态代码和短语？

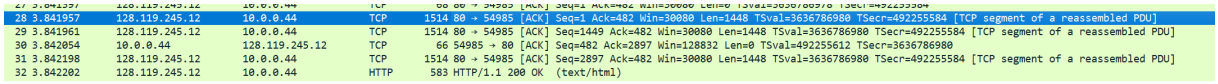
```
28 3.841957    128.119.245.12    10.0.0.44         TCP    1514 80 → 54985 [ACK] Seq=1 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU]
29 3.841961    128.119.245.12    10.0.0.44         TCP    1514 80 → 54985 [ACK] Seq=1449 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU]
30 3.842054    10.0.0.44         128.119.245.12    TCP      66 54985 → 80 [ACK] Seq=482 Ack=2897 Win=128832 Len=0 TSval=492255612 TSecr=3636786980
31 3.842198    128.119.245.12    10.0.0.44         TCP    1514 80 → 54985 [ACK] Seq=2897 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU]
32 3.842202    128.119.245.12    10.0.0.44         HTTP    583 HTTP/1.1 200 OK  (text/html)
```

答 ： 28：返回的第一个数据包

14. 响应中的状态代码和短语是什么？

答： 200 OK

15. 需要多少个包含数据的 TCP 段来承载单个 HTTP 响应和权利法案文本？



| | | | | | |
|---|---|---|---|---|---|
| 28 | 3.841957 | 128.119.245.12 | 10.0.0.44 | TCP | 1514 80 → 54985 [ACK] Seq=1 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU] |
| 29 | 3.841961 | 128.119.245.12 | 10.0.0.44 | TCP | 1514 80 → 54985 [ACK] Seq=1449 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU] |
| 30 | 3.842054 | 10.0.0.44 | 128.119.245.12 | TCP | 66 54985 → 80 [ACK] Seq=482 Ack=2897 Win=128832 Len=0 TSval=492255612 TSecr=3636786980 |
| 31 | 3.842198 | 128.119.245.12 | 10.0.0.44 | TCP | 1514 80 → 54985 [ACK] Seq=2897 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP segment of a reassembled PDU] |
| 32 | 3.842202 | 128.119.245.12 | 10.0.0.44 | HTTP | 583 HTTP/1.1 200 OK (text/html) |

答 ： 3，可以看到有三个 TCP segment 段

**四：带入嵌入对象的 HTML 文档**

1. 清除缓存，输入网站，得到结果
2. 抓包失败，直接使用官方提供的文件

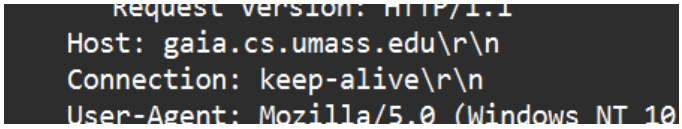
回答问题:

16. 您的浏览器发送了多少条 HTTP GET 请求消息？这些 GET 请求发送到哪些 Internet 地址？

| No. | Time | Source | Destination | Protocol | Length Info |
|---|---|---|---|---|---|
| 12 | 1.222524 | 192.168.1.187 | 128.119.245.12 | HTTP | 1507 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 17 | 1.255989 | 128.119.245.12 | 192.168.1.187 | HTTP | 1355 HTTP/1.1 200 OK (text/html) |
| 19 | 1.293632 | 192.168.1.187 | 128.119.245.12 | HTTP | 1427 GET /pearson.png HTTP/1.1 |
| 25 | 1.321639 | 128.119.245.12 | 192.168.1.187 | HTTP | 745 HTTP/1.1 200 OK (PNG) |
| 29 | 1.387687 | 192.168.1.187 | 178.79.137.164 | HTTP | 443 GET /8E_cover_small.jpg HTTP/1.1 |
| 31 | 1.478827 | 178.79.137.164 | 192.168.1.187 | HTTP | 225 HTTP/1.1 301 Moved Permanently |

答: 发送了 3 条 HTTP GET 请求信息，这些 GET 请求分别被发送到 128.119.245.12，128.119.245.12，178.79.137.164

17. 您能否判断您的浏览器是串行下载这两个图像，还是从两个网站并行下载它们？解释。

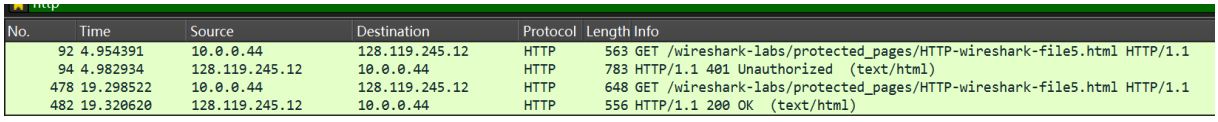


```
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10
```

答: 串行连接，因为连接是始终打开的，其次可以通过发现 get 顺序和相应顺序一致.

**五 HTTP 认证**

1. 清除缓存，输入网址，开始抓包
2. 发现抓不到 Unauthorized 信息，因此使用官网自带包



| No. | Time | Source | Destination | Protocol | Length Info |
|---|---|---|---|---|---|
| 92 | 4.954391 | 10.0.0.44 | 128.119.245.12 | HTTP | 563 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 94 | 4.982934 | 128.119.245.12 | 10.0.0.44 | HTTP | 783 HTTP/1.1 401 Unauthorized (text/html) |
| 478 | 19.298522 | 10.0.0.44 | 128.119.245.12 | HTTP | 648 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 482 | 19.320620 | 128.119.245.12 | 10.0.0.44 | HTTP | 556 HTTP/1.1 200 OK (text/html) |

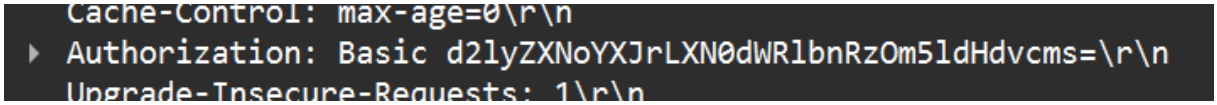
**回答问题:**

18. 服务器对来自浏览器的初始 HTTP GET 消息的响应（状态代码和短语）是什么？

答 : 401 Unauthorized

19. 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？

答 ： 对比两次消息可以发现多包含字段



```
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Upgrade-Insecure-Requests: 1\r\n
```

**结论分析：**

本次实验更加深入地了解了 HTTP 协议的几个方面 ：包括基础部分, 有条件响应, 长文档 TCP 划分, 带入嵌入多对象的 HTML 文档, 含有加密的 HTTP 认证等, 丰富了我对于 HTTP 协议的认识和理解, 加深和巩固了我的理论课知识.

**结论：**

基础部分：我学会了如何捕获和分析网络数据包。我了解了网络协议的基本结构，包括以太网、IP、TCP 和 HTTP 等.

有条件响应：我能够观察到不同条件下服务器和客户端之间的通信行为.

长文档 TCP 划分：我观察到 TCP 是如何将长文档分割成更小的数据包进行传输，并在目的地重新组装这些数据包以恢复原始文档.

带入嵌入多对象的 HTML 文档：我研究了在网络通信中传输包含多个对象（如图像、脚本等）的 HTML 页面的过程.

加密的 HTTP 认证: 我了解到加密和授权的方式, 可以增强安全性.