山东大学 计算机 学院

计算机网络 课程实验报告

学号：202000130143	姓名： 郑凯饶	班级： 2020 级 1 班
实验题目：Wireshark HTTP		
实验学时：2	实验日期： 3.8	

实验目的：

使用 Wireshark 调查协议，探索 HTTP 协议包括基本 GET/response 通信、HTTP 报文格式、取回大型 HTML 文件、取回包含嵌入式对象的 HTML 文件以及 HTTP 认证和安全。

硬件环境：

Dell Latitude 5411

Intel(R) Core(TM) i5-10400H CPU @ 2.60GHz(8GPUs),~2.6GHz

软件环境：

Windows 10 家庭中文版 64 位（10.0，版本 18363）

Wireshark-win64-3.6.2

实验步骤与内容：

1. 问题：

1）浏览器运行的 HTTP 版本？服务器？

2）你的浏览器可以接受的语言。

3）IP 地址。

4）服务器返回的状态码。

5）取回的 HTML 文件上一次在服务器端修改的时间。

6）文件的内容占多少字节？

7）有哪些 headers 未在包列表窗口展示？

8）第一次从你的浏览器发出的 GET 请求是否包含“IF-MODIFIED-SINCE”字段？

9）第一次服务器是否返回文件内容？

10） 第二次 GET 请求是否包含“IF-MODIFIED-SINCE”字段？具体内容？

11） 第二次服务器返回文件内容？

12） 发出多少次 GET 请求？哪一个包包含 GET 请求请求 Bill or Rights？

13） 哪一个包响应了上述请求？

14） 返回的状态码。

15） 共有多少个 TCP 数据段返回 HTTP response 以及 Bill or Rights 文本？

16） 发出多少次 GET 请求？向哪些网络地址发送？

17） 你的浏览器是串行还是并行地下载两张图片？

18） 服务器对最初 HTTP 请求的响应。

19） 浏览器何时发出第二次 GET 请求，包含了哪些新字段？

2. 阐述基本方法

使用过滤器，查看指定报文信息。

3. 实验结果展示与分析

1. 浏览器运行的 HTTP 版本？服务器？

均为 HTTP 1.1；
2. 你的浏览器可以接受的语言。
zh-CN,zh;q=0.8,en;q=0.9;
3. IP 地址。
我的 IP：172.25.188.178;服务器：128.119.245.12;
4. 服务器返回的状态码。
状态码为 304;
5. 取回的 HTML 文件上一次在服务器端修改的时间。
最后一次的修改时间：Tue, 08 Mar 2022 06:59:01 GMT;
6. 文件的内容占多少字节？
293;
7. 有哪些 headers 未在包列表窗口展示？
Cache-Control，User-Agent，Accept-Encoding;
8. 第一次从你的浏览器发出的 GET 请求是否包含“IF-MODIFIED-SINCE”字段？
第一次请求不会有；
9. 第一次服务器是否返回文件内容？
第一次返回，之后没有返回，返回文件内容的话会有 File Data 字段，以及 Line-based text data 字段，下面就是文件内容；
10. 第二次 GET 请求是否包含“IF-MODIFIED-SINCE”字段？具体内容？
第二次请求有，并且显示的时间是第一次返回 Last-Modified 字段中的时间；
11. 第二次服务器返回文件内容？
第二次的状态码为 304，表示 Not Modified，即请求文件未修改。因此它也并未发送文件，而是指示浏览器加载上次返回的文件；

Destination	Protocol	Length	Info
128.119.245.12	HTTP	570	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
172.25.188.178	HTTP	728	HTTP/1.1 200 OK (text/html)
128.119.245.12	HTTP	656	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
172.25.188.178	HTTP	238	HTTP/1.1 304 Not Modified

12. 发出多少次 GET 请求？哪一个包包含 GET 请求请求 Bill or Rights?
只有 1 个，第 3 个；
13. 哪一个包响应了上述请求？
第 8 个；
14. 返回的状态码。
200，OK；
15. 共有多少个 TCP 数据段返回 HTTP response 以及 Bill or Rights 文本？
3 个 TCP 段；

128.119.245.12	172.25.188.178	TCP	56 80 → 64781 [ACK] Seq=1 Ack=517 Win=30336 Len=0
128.119.245.12	172.25.188.178	TCP	1514 80 → 64781 [ACK] Seq=1 Ack=517 Win=30336 Len=1460 [TCP
128.119.245.12	172.25.188.178	TCP	1514 80 → 64781 [ACK] Seq=1461 Ack=517 Win=30336 Len=1460 [T
128.119.245.12	172.25.188.178	TCP	1514 80 → 64781 [ACK] Seq=2921 Ack=517 Win=30336 Len=1460 [T
128.119.245.12	172.25.188.178	HTTP	479 HTTP/1.1 200 OK (text/html)
172.25.188.178	128.119.245.12	TCP	54 64781 → 80 [ACK] Seq=517 Ack=2921 Win=131328 Len=0
172.25.188.178	128.119.245.12	TCP	54 64781 → 80 [ACK] Seq=517 Ack=4806 Win=131328 Len=0

16. 发出多少次 GET 请求？向哪些网络地址发送？
3 个 http 请求，前两个请求 128.119.245.12，后面一个 178.79.137.164；
17. 你的浏览器是串行还是并行地下载两张图片？
应该是串行下载，下载完成一张图片之后再请求下一张；

Source	Destination	Protocol	Length	Info
172.25.188.178	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
128.119.245.12	172.25.188.178	HTTP	1299	HTTP/1.1 200 OK (text/html)
172.25.188.178	128.119.245.12	HTTP	490	GET /pearson.png HTTP/1.1
128.119.245.12	172.25.188.178	HTTP	690	HTTP/1.1 200 OK (PNG)
172.25.188.178	178.79.137.164	HTTP	457	GET /8E_cover_small.jpg HTTP/1.1
178.79.137.164	172.25.188.178	HTTP	225	HTTP/1.1 301 Moved Permanently

18. 服务器对最初 HTTP 请求的响应。

401（Unauthorized）；

19. 浏览器何时发出第二次 GET 请求，包含了哪些新字段？

新增 Authorization 字段，附上账号信息；

Source	Destination	Protocol	Length	Info
172.25.188.178	128.119.245.12	HTTP	588	GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.h
128.119.245.12	172.25.188.178	HTTP	715	HTTP/1.1 401 Unauthorized (text/html)
172.25.188.178	128.119.245.12	HTTP	647	GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.h
128.119.245.12	172.25.188.178	HTTP	528	HTTP/1.1 404 Not Found (text/html)

结论分析与体会：

这次实验了解了 HTTP 协议的基本内容。观察了 HTTP GET 请求及及其响应过程，还有在大型文件、网页包含嵌入式对象和安全认证的情形下数据如何传输。希望继续了解其他协议。