南開大學
Nankai University

计算机网络实验报告

编程作业 2：Wireshark 捕获数据包

2113662 张丛

一、 实验要求

（1）搭建 Web 服务器（自由选择系统），并制作简单的 Web 页面，包含简单文本信息（至少包含专业、学号、姓名）、自己的 LOGO、自我介绍的音频信息。页面不要太复杂，包含要求的基本信息即可。

（2）通过浏览器获取自己编写的 Web 页面，使用 Wireshark 捕获浏览器与 Web 服务器的交互过程，并进行简单的分析说明。

（3）使用 HTTP，不要使用 HTTPS。

二、 Web 配置

(一) Web 服务器

实验中使用了 Apache 这个 Web 服务器。Apache 服务开启后,可在在浏览器中输入 http://127.0.0.1 或 http://localhost 来访问本地主机，且默认情况下，Apache 使用 80 端口。

(二) html 设计

编写的 html 文件放在 Apache 的"DocumentRoot" 目录下。html 的主体代码如下图:

```
38      </style>
39  </head>
40  <body>
41      <h1>计算机网络 Lab2</h1>
42      <p>学号：2113662</p>
43      <p>姓名：张丛</p>
44      <p>专业：信息安全</p>
45      <img src="千反田.jpg" alt="千反田" width="300" height="300">
46      <br>
47      <video controls width="300" height="240">
48          <source src="test.mp4" type="video/mp4">
49      </video>
50  </body>
```

图 1: html 代码

展示页面包含了个人信息，一张名为千反田的图片，和一段.mp4 格式视频。
页面效果如下:

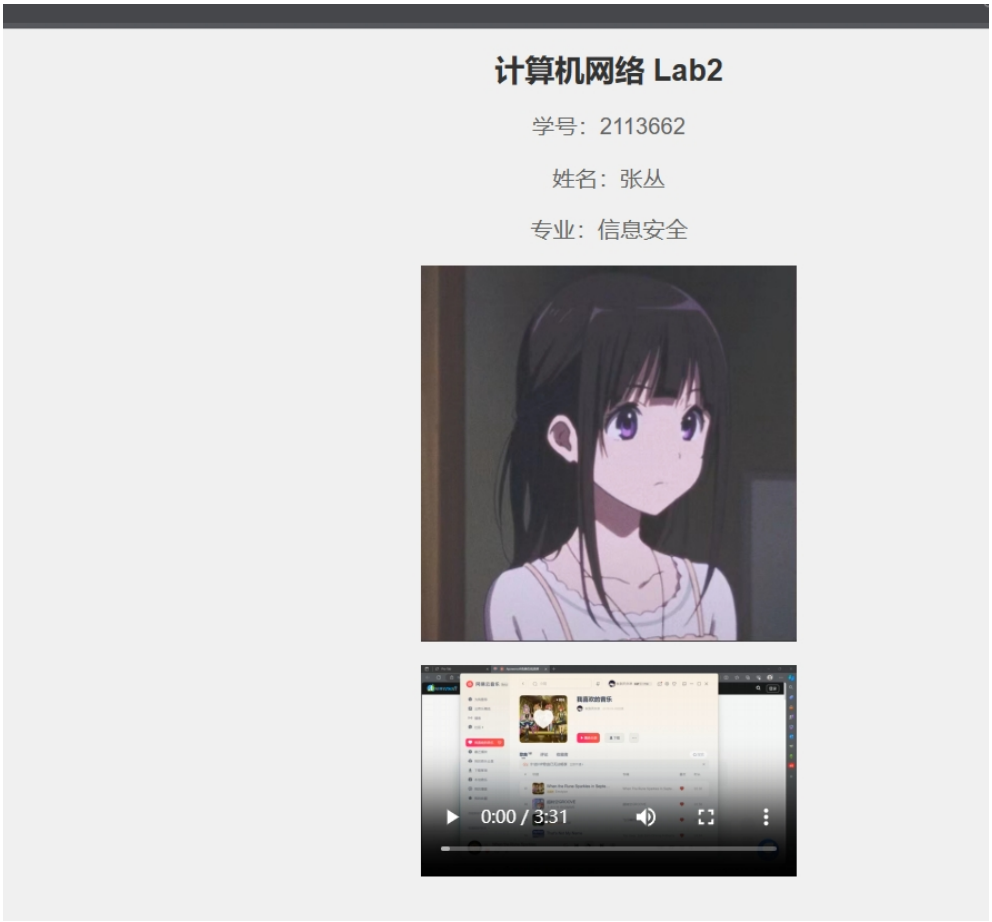

图 2: 页面效果

三、 Wireshark 捕获数据包

打开 Wireshark 后，选择捕获本地回环流量的适配器（Adapter for loopback traffic capture），并且使用过滤器仅捕获端口为 80 的数据包，如下图：

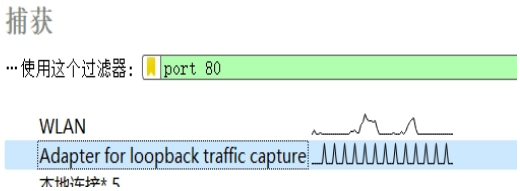

图 3: 页面效果

点击开始捕获后，打开浏览器访问 127.0.0.1，播放视频，可以返回 Wireshark 看到捕获的数据包如下：

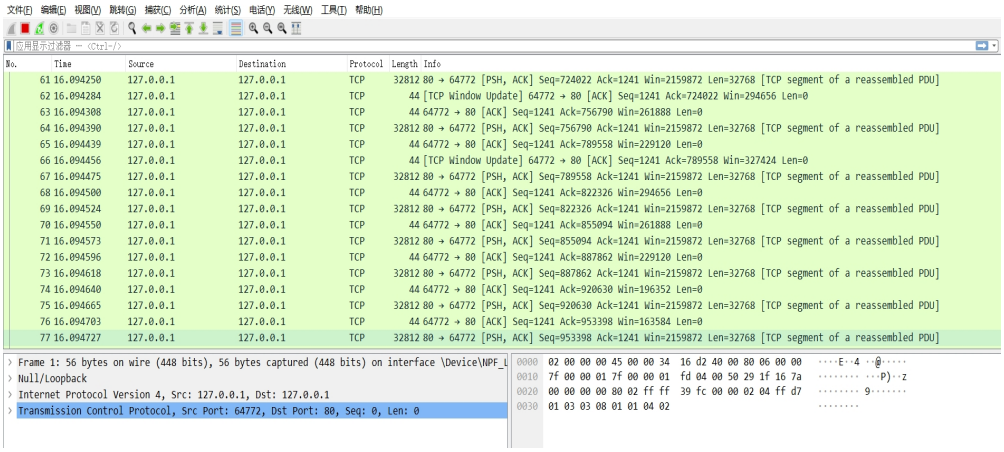

图 4: 数据包

可以关闭浏览器，断开 TCP 连接，在 Wireshark 点击停止捕获并保存为.pcapng 文件，里面包含了本次实验捕获的数据包。

(一) 三次握手

查看三次握手过程的数据包：

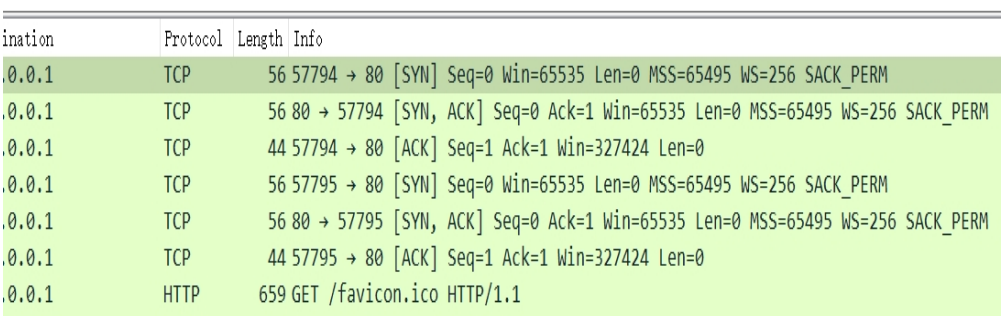

图 5: 三次握手

一个比较明显的现象是，三次握手似乎重复了两次。

再仔细观察会发现是客户端两个不同的端口（上图的 57794 和 57795）都与服务端进行了三次握手，即多个 TCP 连接。

HTTP/1.1 采用双端口连接是为了防止头阻塞的问题。

我们回过头来只看一个端口的三次握手：

1. 客户端首先发送 SYN 报文给服务端（且序号 Seq=0），表示向服务端发起连接，且此报文不包含应用数据。

2. 服务端接受到客户端的 SYN 报文后，将向客户端发送 SYN 和 ACK 标志位均置为 1 的回应报文，表示同意建立连接，这里是第二次握手。服务端此次发送的数据包同样不含应用数据，且 Seq=0 表示是服务端的第一条报文，ACK=1 表示是对上一条报文的确认。

3. 客户端接收到服务端的响应后，会发送 ACK 标志位置为 1 的数据包给服务端，这就是第三次握手，连接建立。此次的数据包可以携带客户端的数据。

可以在 Wireshark 查看数据包信息，如序号以及标志位信息等等：

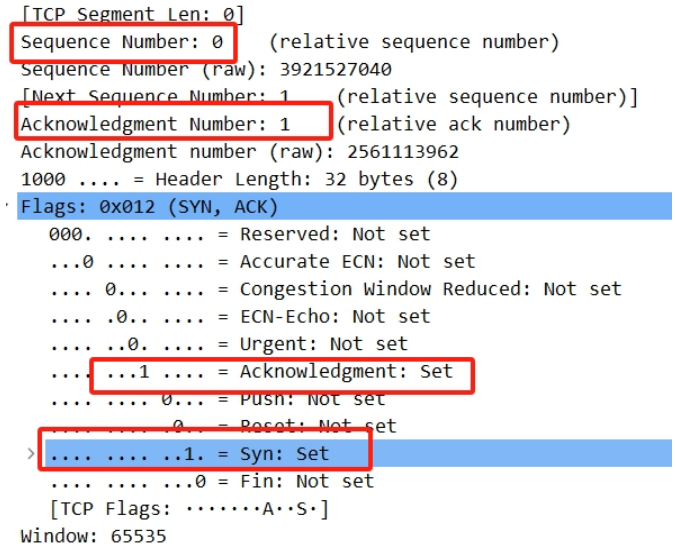

图 6: 信息

(二) 四次挥手

查看四次挥手过程的数据包：

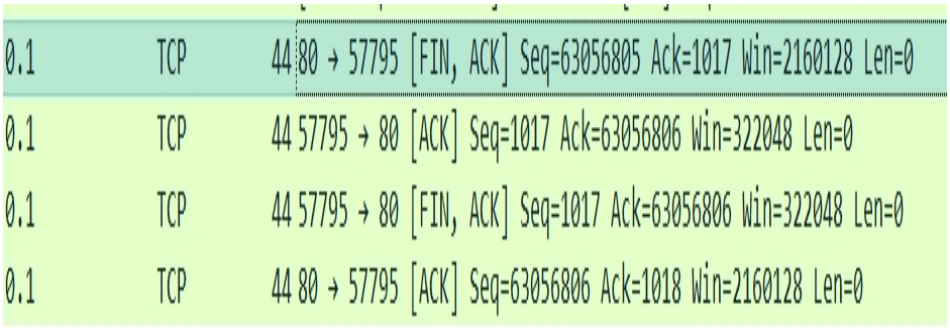

图 7: 四次挥手

四次挥手的过程：

1. 客户端如果想要关闭连接，首先向服务端发送 FIN 标志位置为 1 的报文。

2. 服务端接收到报文后，发送 ACK 报文。

3. 服务端在完成自己的数据传输后，也发送 FIN 报文给客户端。这是第三次挥手，服务端告诉客户端它不再发送数据，并请求客户端关闭连接。

4. 客户端接收到服务端的 FIN 后，发送一个 ACK 给服务端，以确认收到。

5. 客户端会等待 2MSL 时间，关闭连接。

其中:

SML 即最长报文段寿命。

客户端等待 2SML 时间是为了保证客户端发送的最后一个 ACK 报文段能够到达服务器。假设客户端不等待 2MSL 时间，而是在发送完 ACK 之后直接释放关闭，一但这个 ACK 丢失的话，服务器就无法正常的进入关闭连接状态。

同时，客户端等待 2MSL 时间，也可以使本连接持续的时间内所产生的所有报文段都从网络中消失，使下一个新的连接中不会出现这种旧的连接请求报文段。

四、 思考与总结

(一) HTTP/1.0 和 HTTP/1.1 的区别

1. 持久连接。HTTP/1.0 中一个 TCP 连接只能发送一个请求和响应，而 HTTP/1.1 的同一个 TCP 连接可以发送多次 HTTP 请求，减少了建立和关闭连接的性能开销。

2. 管道机制。第一个请求发出去了，不必等待其响应回来才能发第二个请求出去，即相当于同时发出多个请求，因而可以减少整体的响应时间。

(二) 三次挥手现象

当被动关闭方在 TCP 挥手过程中,「没有数据要发送」并且「开启了 TCP 延迟确认机制」,那么第二和第三次挥手就会合并传输，这样就出现了三次挥手。

(三) PSH 和 RST 标志

PSH 标志意味着发送方希望接收方立即将数据交付给应用层。

RST 标志通常用于表示一个错误或异常情况，以及强制关闭一个 TCP 连接。在实验中我们可能没有捕获到四次挥手的报文而是捕获到 RST 报文。

(四) 总结

本次实验编写了 html 文件，建立了简单的 Web 页面, 并通过 Wireshark 捕获数据包验证了三次握手和四次挥手，也观察到了一些特别的现象并查阅资料作出了解释。

实验过程中，复习到理论课的三次握手四次挥手的知识，复习到传输层网络层报文格式，复习到 http 协议 tcp 协议。

实验过程中，进一步熟悉了 Wireshark 的使用，也学习到了新知识。

以上。