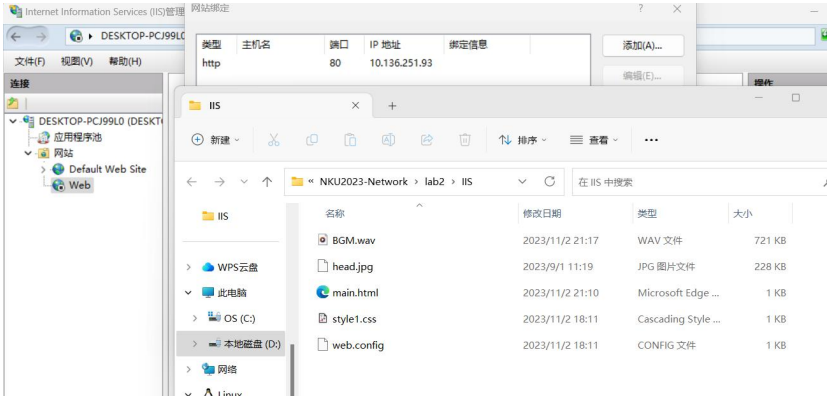
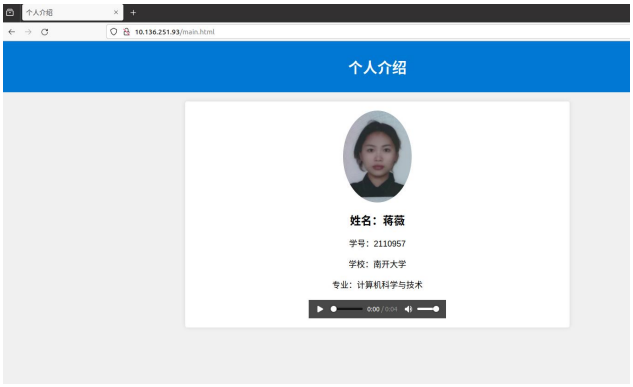
一、Web 服务器搭建（IIS）



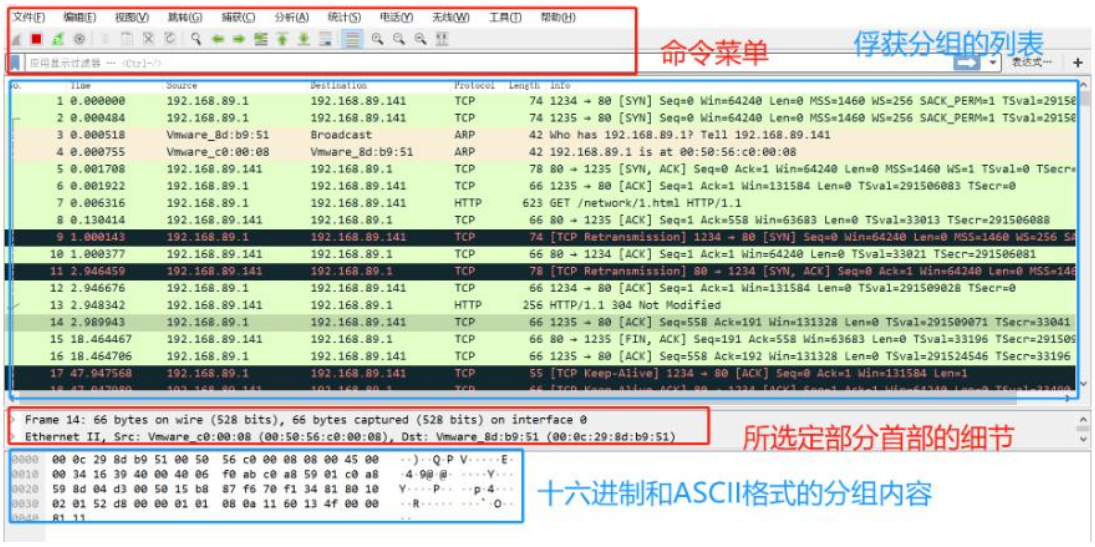
二、通过 Wireshark 捕获与 Web 服务器的交互过程

1、网页




```html
<html>
<head>
    <meta charset="UTF-8">
    <title>个人介绍</title>
    <link rel="stylesheet" href="style1.css">
</head>
<body>
    <header>
        <h1>个人介绍</h1>
    </header>
    <div class="container">
        <div class="profile">
            <img src="head.jpg" alt="个人照片">
            <h2>姓名：蒋薇</h2>
            <p>学号：2110957</p>
            <p>学校：南开大学</p>
            <p>专业：计算机科学与技术</p>
        </div>
        <div class="audio">
            <audio controls>
                <source src="BGM.wav" type="audio/mpeg">
            </audio>
        </div>
    </div>
</body>
</html>
```

2.wireshark



界面大致分为四个区：命令菜单区、俘获分组列表区、选定分组首部细节区、十六进制和 ASCII 格式分组内容区。

其中，命令菜单区的**应用显示过滤器**部分可以筛选显示的分组，例如：

服务器 IP 地址 . . . . . : 10.136.251.93，端口号 port = 80
浏览器访问，ip 地址：192.168.182.128,端口号 port=57422

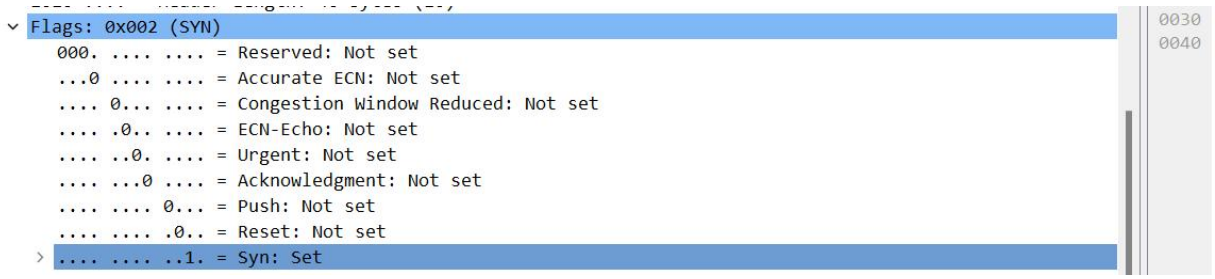
过滤器条件：
ip.addr == 192.168.182.128 && ip.addr == 10.136.251.93 && tcp.port == 80

3.针对数据交互过程的数据包的关键属性说明

消息（4 个部分）

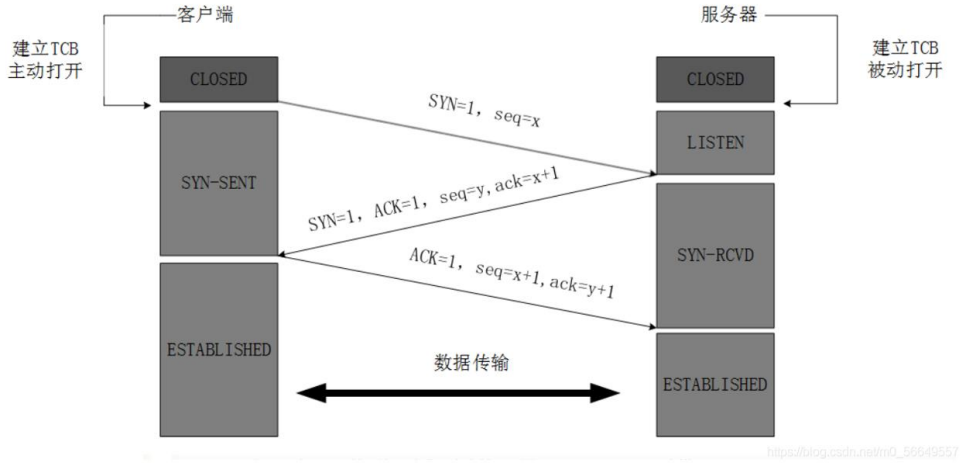
1. **Frame**，指的是==物理层的数据帧概况；
2. **Ethernet II**，**第 0-13 个字节**，表示数据层以太网帧头部信息，包含**目的地址**、**源地址**和**协议类型**
3. **Internet Protocol Version 4**，**第 14-33 个字节**，互联网层 IP 包头部信息
4. **Transmission Control Protocol**，**第 34 个字节开始**，传输层的数据段头部信息

在 TCP 层，有个 FLAGS 字段，这个字段有以下几个标识：SYN, FIN, ACK, PSH, RST, URG。
其中，对于我们日常的分析有用的就是前面的五个字段。它们的含义是：SYN 表示建立连接，FIN 表示关闭连接，ACK 表示响应，PSH 表示有 DATA 数据传输，RST 表示连接重置。



HTTP，选取一条 HTTP 消息，消息格式为**在原有 TCP 格式的基础上**，增加超文本传输协议部分。

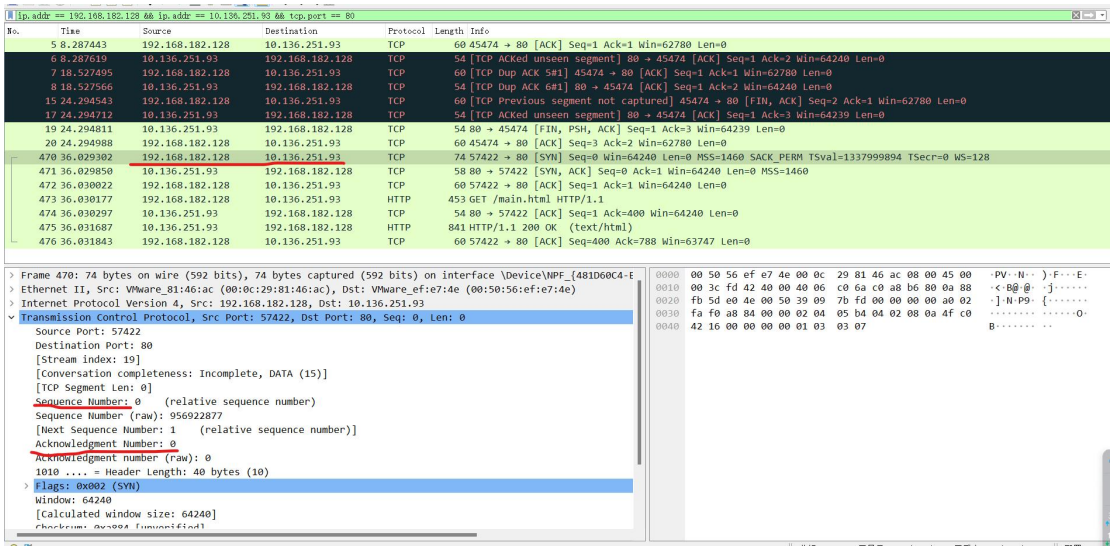
4.Tcp 三次握手：



SYN 表示建立连接，FIN 表示关闭连接，ACK 表示响应，PSH 表示有 DATA 数据传输，RST 表示连接重置。

1.第一次握手数据包

客户端发送一个 TCP，标志位为 SYN，序列号为 0， 代表客户端请求建立连接。如下图。



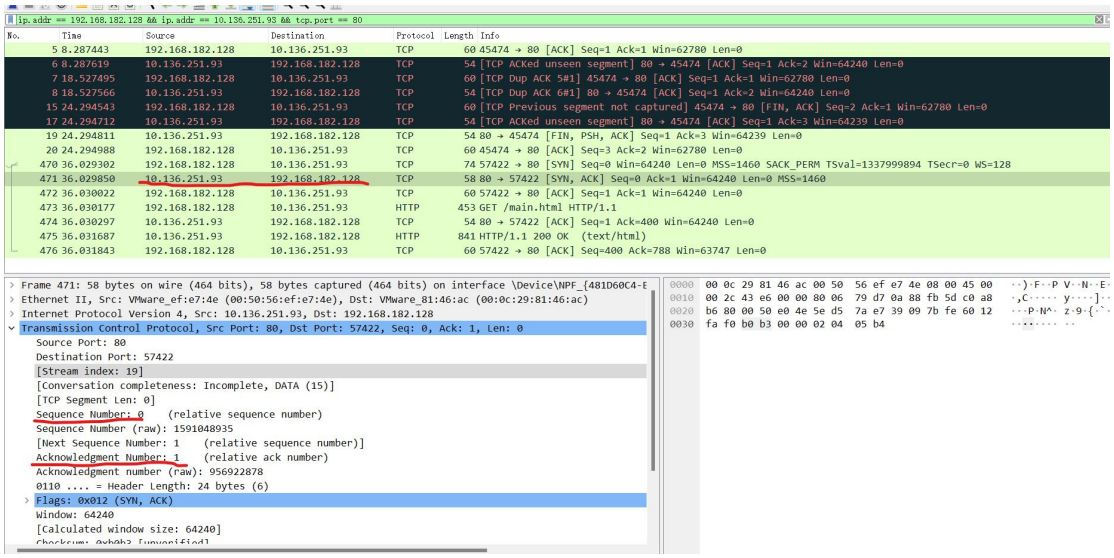
SYN ：标志位，表示请求建立连接，SYN

Seq = 0 ：初始建立连接值为 0，数据包的相对序列号从 0 开始，表示当前还没有发送数据

Ack =0：初始建立连接值为 0，已经收到包的数量，表示当前没有接收到数据

2.第二次握手的数据包

服务器发回确认包，标志位为 SYN,ACK. 将确认序号(Acknowledgement Number)设置为客户的 I S N 加 1 以.即 0+1=1



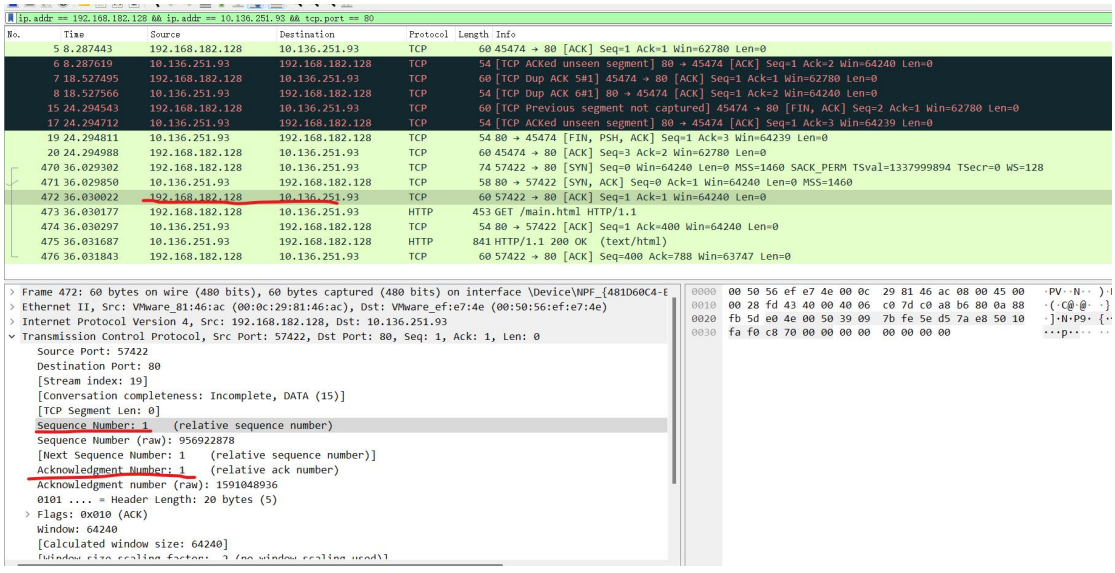
Flag = SYN,ACK

Seq = 0 ： 初始建立值为 0，表示当前还没有发送数据

Ack = 1：表示当前端成功接收的数据位数，虽然客户端没有发送任何有效数据，确认号还是被加 1，因为包含 SYN 或 FIN 标志位。（并不会对有效数据的计数产生影响，因为含有 SYN 或 FIN 标志位的包并不携带有效数据）

3.第三次握手的数据包

客户端再次发送确认包(ACK) SYN 标志位为 0,ACK 标志位为 1.并且把服务器发来 ACK 的序号字段+1,放在确定字段中发送给对方.并且在数据段放写 ISN 的+1,

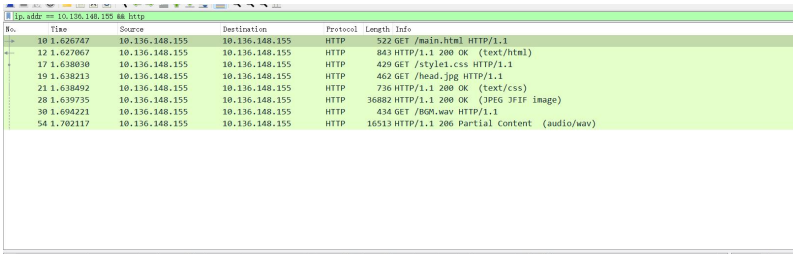


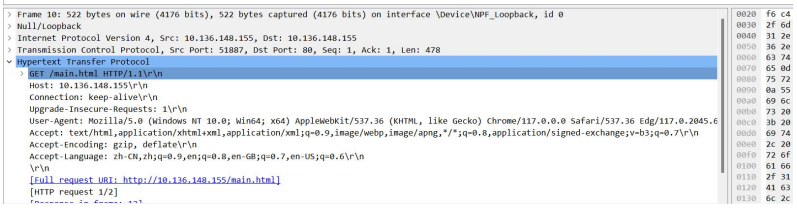
Flag = ACK ： 标志位，表示已经收到记录

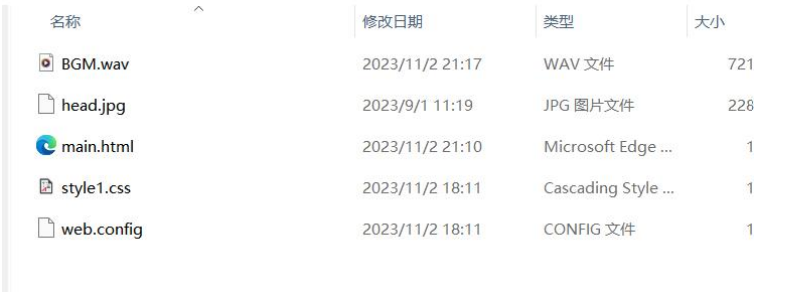
Seq = 1 ： 表示当前已经发送 1 个数据

Ack = 1：表示当前端成功接收的数据位数，虽然服务端没有发送任何有效数据，确认号还是被加 1，因为包含 SYN 或 FIN 标志位（并不会对有效数据的计数产生影响，因为含有 SYN 或 FIN 标志位的包并不携带有效数据)。

6.http







报文传输各层简要介绍

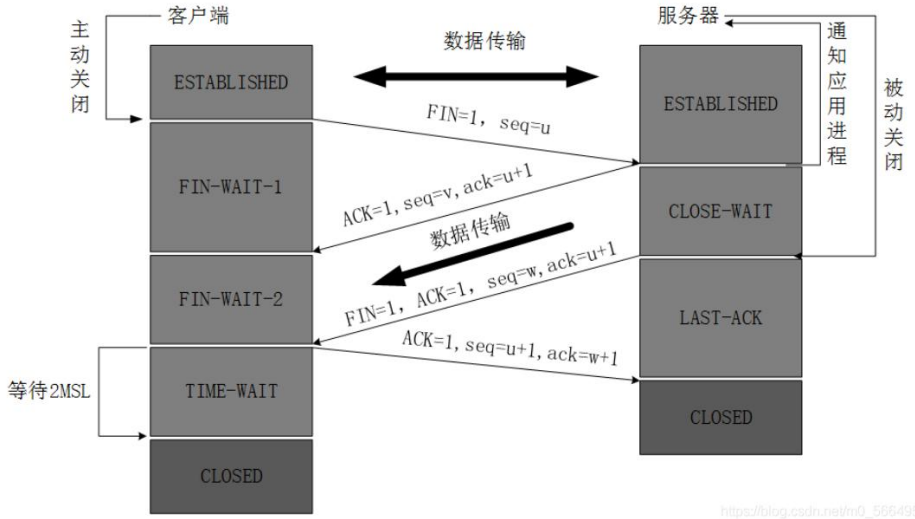
- Frame：物理层的数据帧概况
- Ethernet II：数据链路层以太网帧头部信息
- Internet Protocol Version 4：互联网层 IP 包头部信息
- Transmission Control Protocol：传输层 T 的数据段头部信息，此处是 TCP
- Hypertext Transfer Protocol：应用层的信息，此处是 HTTP 协议

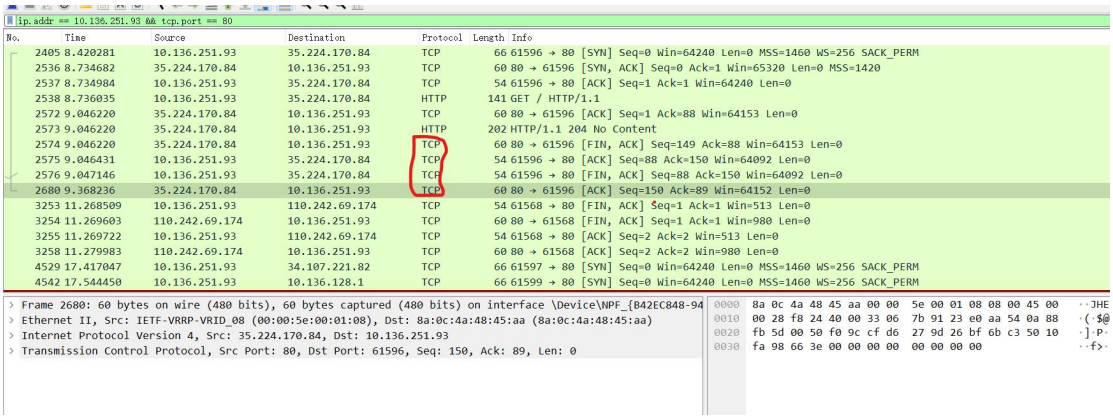
Get 请求，返回协议码 200 表示请求成功；若出现协议码 304 为有缓存且未修改。
Style.css 文件美化页面，head.jpg 为图片文件，BGM.wav 为音频文件

音频文件，响应码 206 表示 Partial Content，表示服务器成功处理了部分 GET 请求。这通常用于断点续传或者分块下载时，客户端只请求资源的一部分。服务器会在应头中包含 Content-Range 字段，指示返回的是资源的哪一部分。

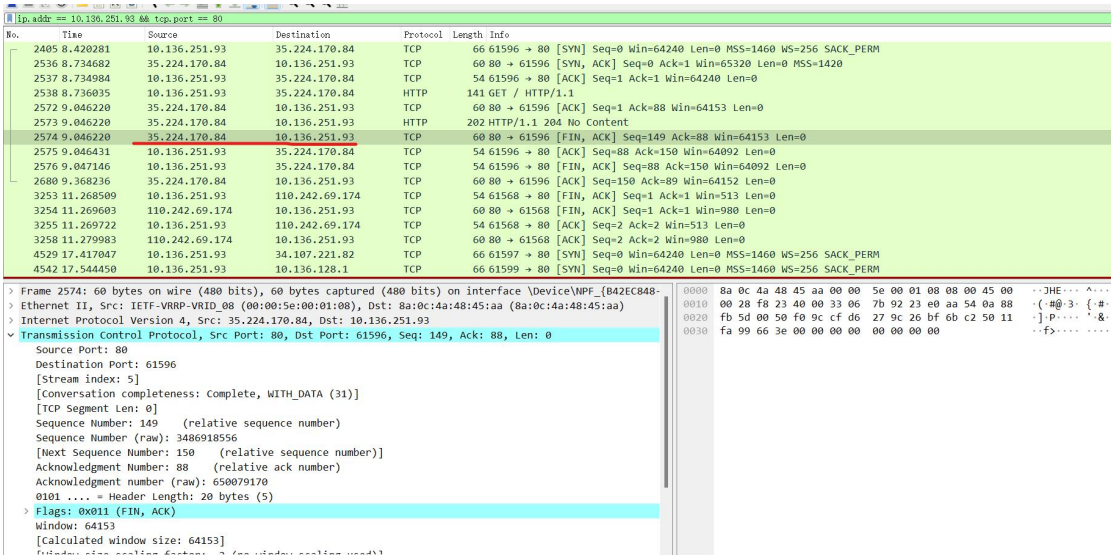
TCP 三次握手，建立了连接，发起 http 的一个连接，开始进行数据交互，中间发的都是正常的数据包，直到客户端发完数据包了，客户端发起一个 fin，ack 包开始四次挥手

5、Tcp 四次挥手



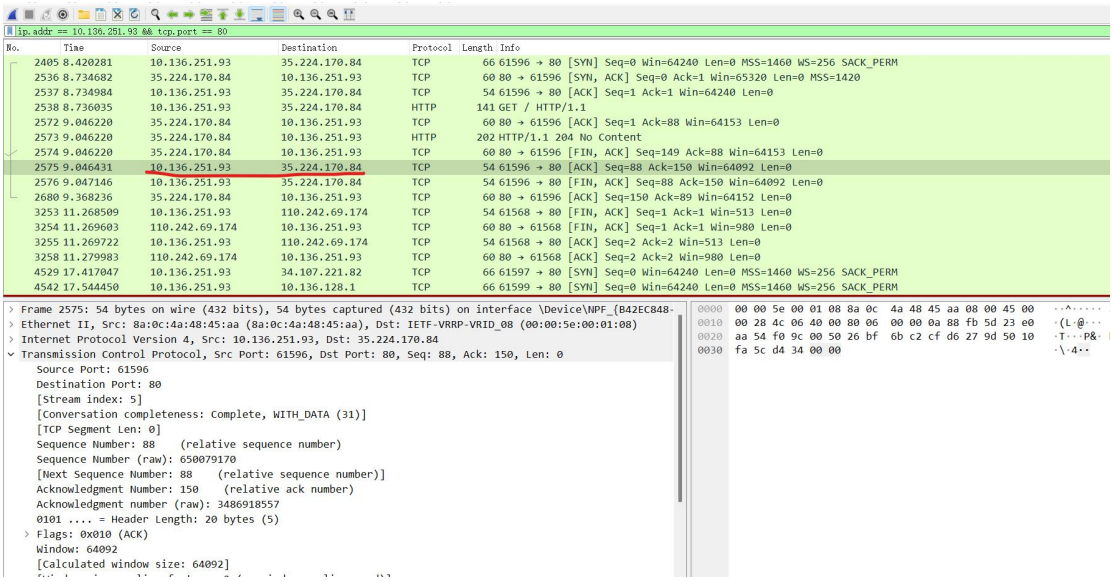


1.客户端发的第一个释放连接的请求



tcp 报文是一个可靠的协议，它的每一个数据包都要进行确认，每发一个数据包都有一个 ack 包。表示每发一个包，都要确认。Sequence Number,序号；Acknowledgment Number,确认号；Acknowledgment：Set，对上一个报文的确认包；Fin:Set,fin 位被标记，为释放连接的请求报文。

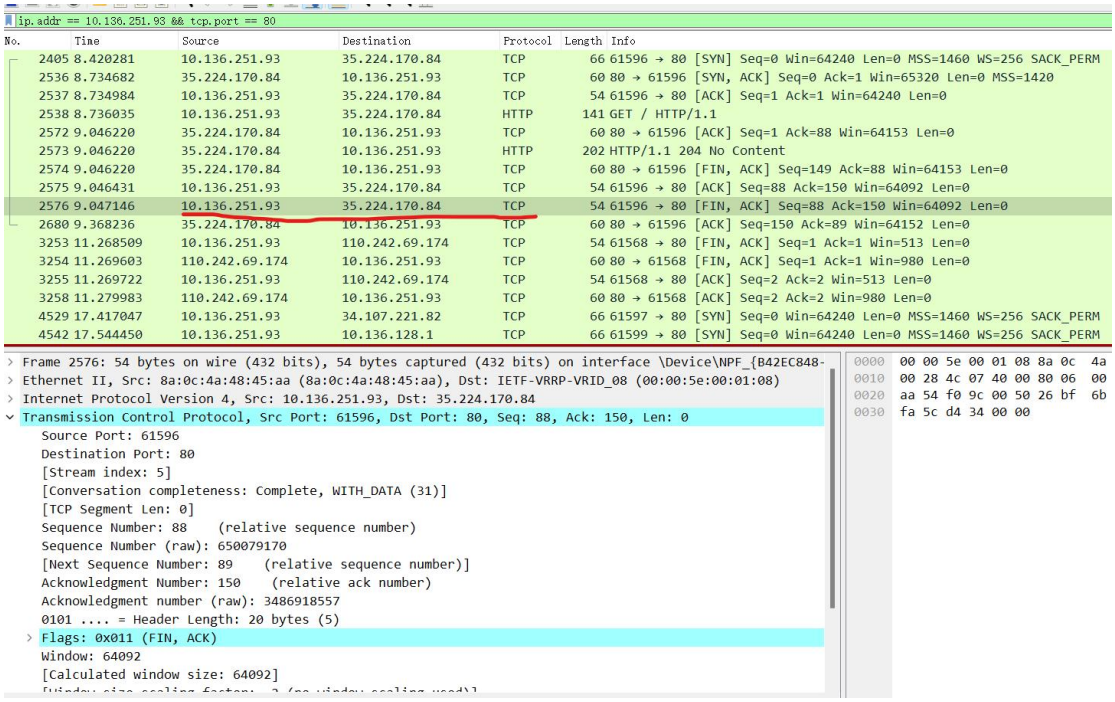
2.服务器给客户端回应确认消息



只有 ack 位被标记了，其它位没有被标记，因为这就是一个确认消息。

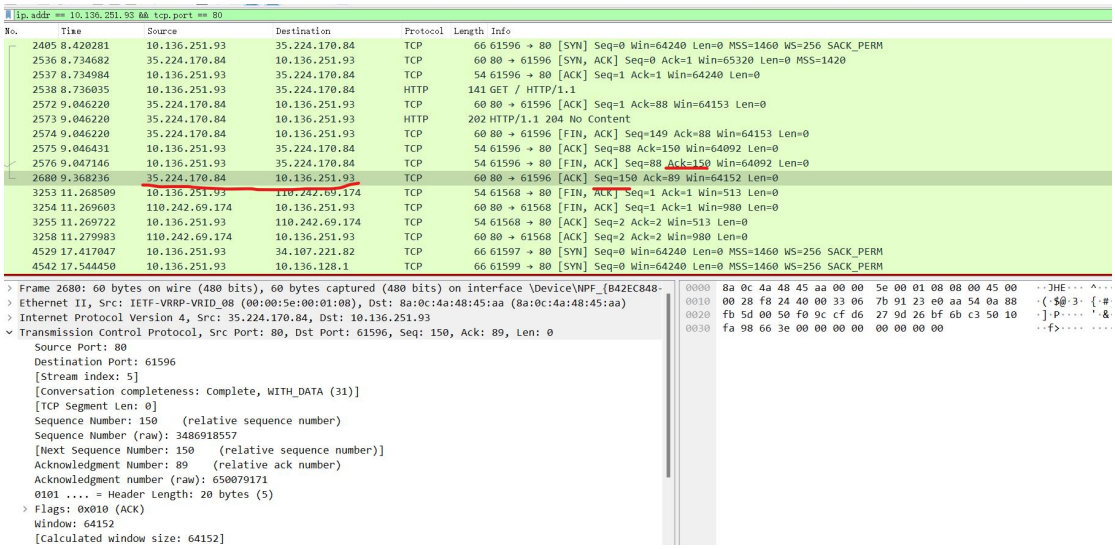
ack 包的序号是 150，是因为客户端发的 fin，ack 包希望下一个包的序号是 150（确认号是 150）

3.服务器发给客户端释放连接的请求



再次发送一个 fin，ack 包，表示我也要释放连接；fin，ack 和 ack 包的序号、确认号是一样的；因为是一个服务器发的，所以确认号和序号是一样的；fin 位被置位，也是要释放连接到。

4.客户端发送确认消息



客户端也发了一个 ack 包。这个包的 ack 号等于上一个包的序列号加 1。

三、总结

1.当第一次请求页面并请求成功时，页面会返回状态码 200 表示请求成功，并同时返回页面的 html 内容；当再次请求且页面没有修改时会返回 304 表示页面未修改可以直接使用浏览器缓存的内容

2.传输流程整体:

客户端发出请求，服务器在局域网内（因为使用的是本地的虚拟机）发送查找网卡请求并找到 ip 对应的物理地址;

三次握手建立连接;

进行页面请求，服务器返回 html 内容;
请求并返回文字、图片、音频等内容；
四次挥手断开连接。

HTTP 1.1 与 HTTP 1.0 是两个不同版本的 HTTP 协议,

持久连接为其重要特性，HTTP 1.1 引入了持久连接（Persistent Connections）的概念，允许多个请求和响应在同一个 TCP 连接上进行，减少了连接的建立和关闭的开销；

2.虚拟主机支持：HTTP 1.1 支持虚拟主机（Virtual Hosting），允许在同一个服务器上运行多个网站，通过 Host 头字段来区分不同的网站；

3..缓存控制：HTTP 1.1 引入了更强大的缓存控制机制，包括 Cache-Control 头字段和 ETag 头字段；