实验2：配置Web服务器，编写简单页面，分析交互过程

# 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）和自己的LOGO。

（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）提交实验报告。

（4）功能实现：

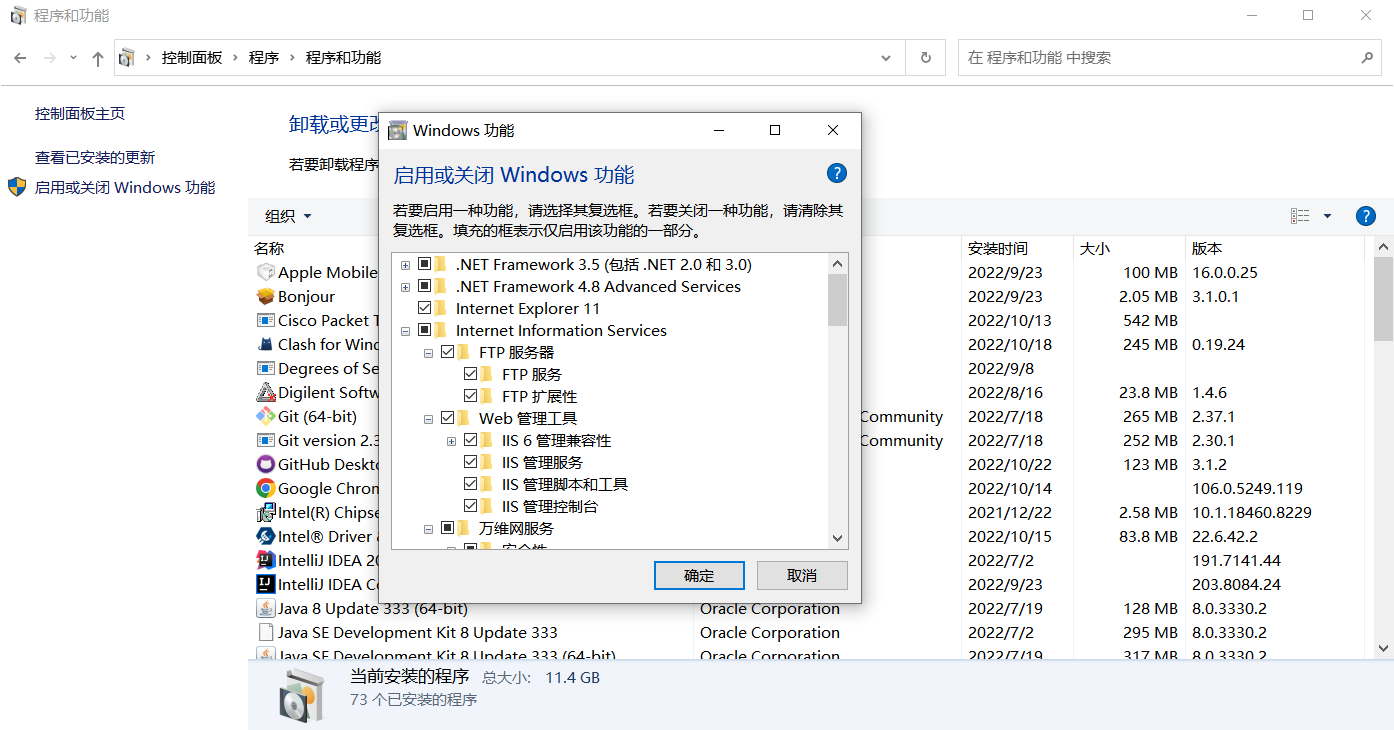
Web服务器搭建、编写Web页面（提交HTML文档）（20分）

Wireshark捕获交互过程（提交捕获文件）（20分）

# 实验准备

了解如何在win10系统下，使用IIS搭建自己的专属网站

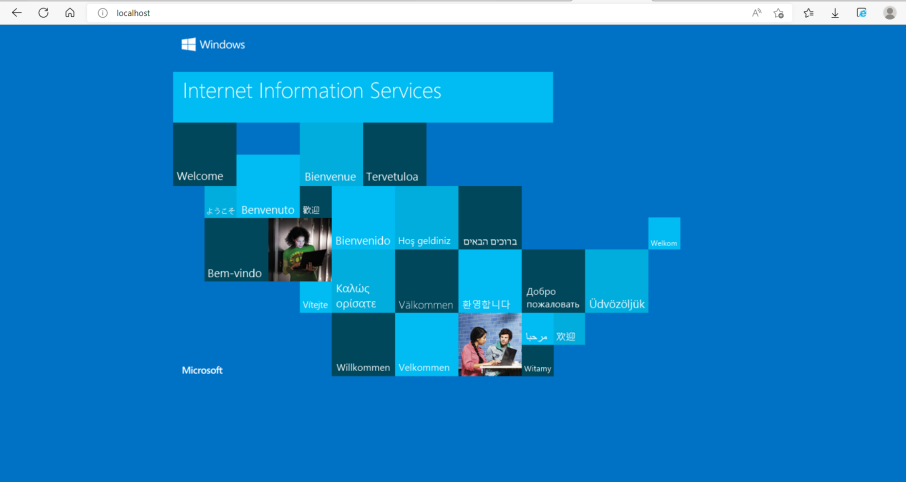
1.搜索控制面板-程序-程序和功能-启用或关闭Windows功能

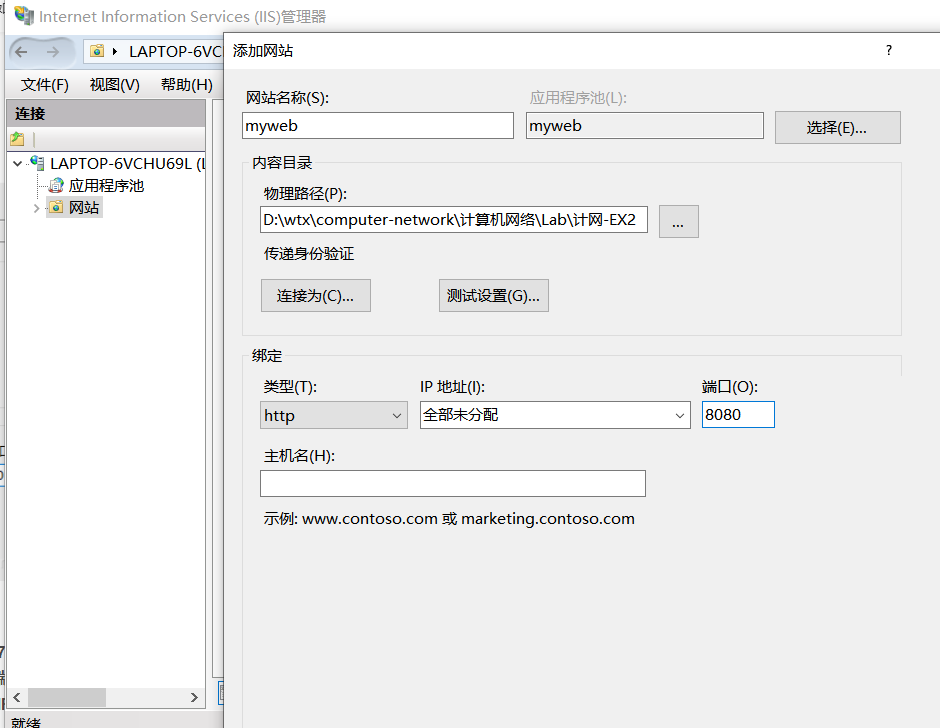


2.勾选对应选项



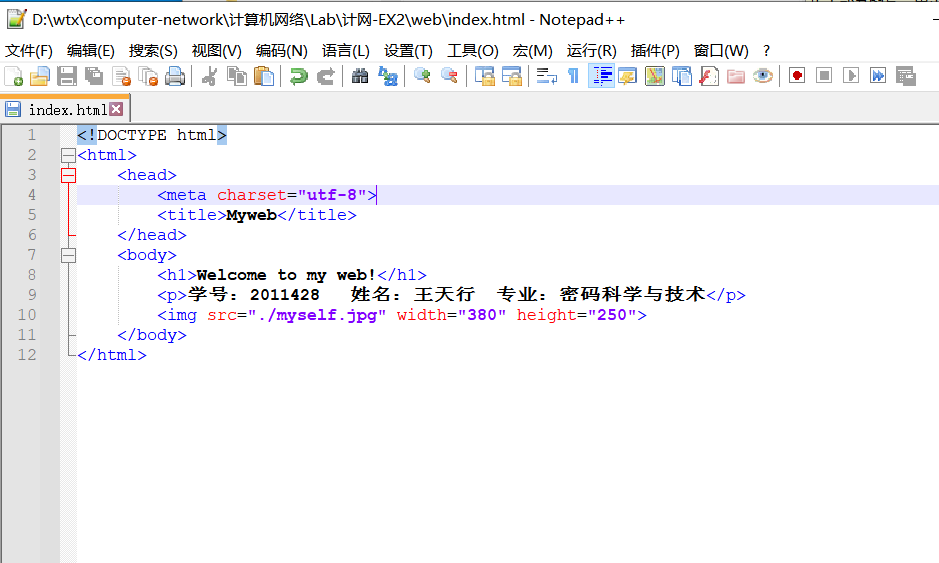
3.安装完毕后，输入网址：[http://localhost](http://localhost/)，显示如下页面即为成功

  
4.打开IIS管理器（注意不要打开为IIS 6.0管理器），右击网站-添加网站

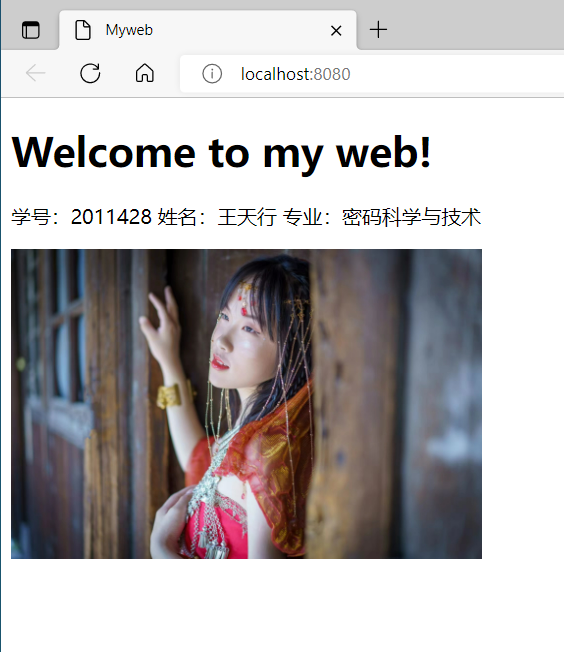


# 实验内容

## 编写html文件



页面结果如图：



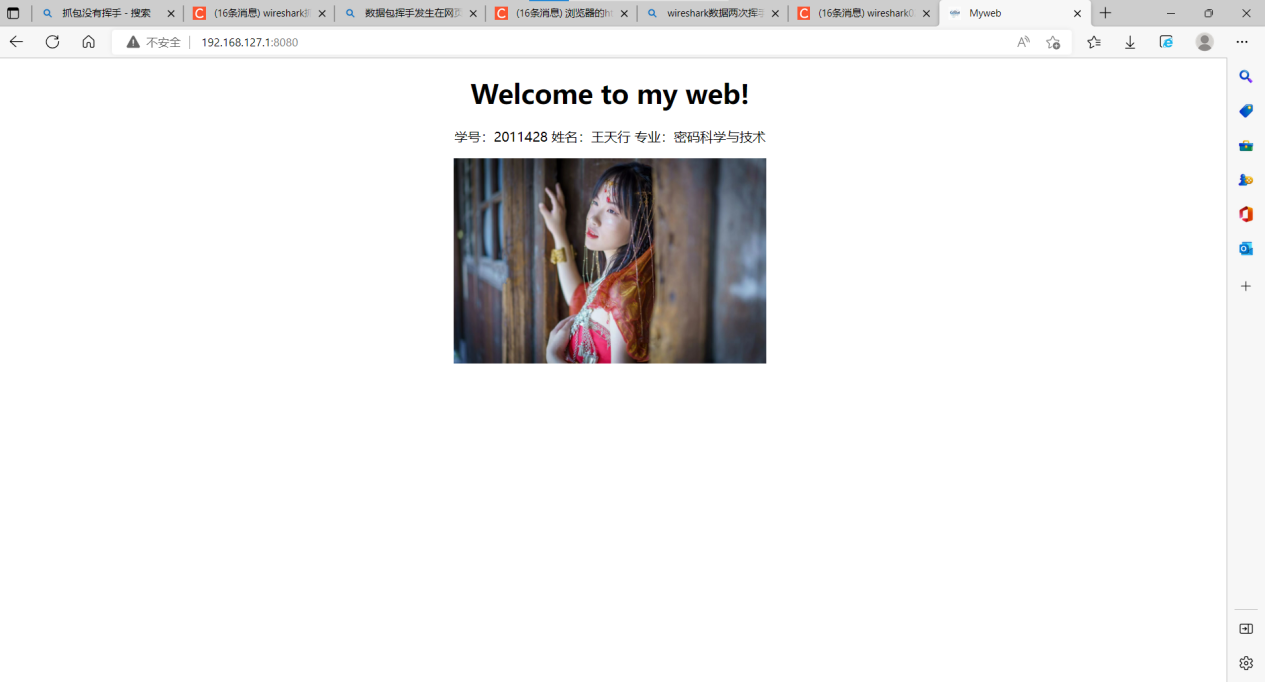
## 增加页面logo

在<head></head>之间增加代码：<link rel="shortcut icon" href="https://tse3-mm.cn.bing.net/th/id/OIP-C.jPAt6yWb93zcMPtERx6VIAHaE8?pid=ImgDet&rs=1" type="image/x-icon">

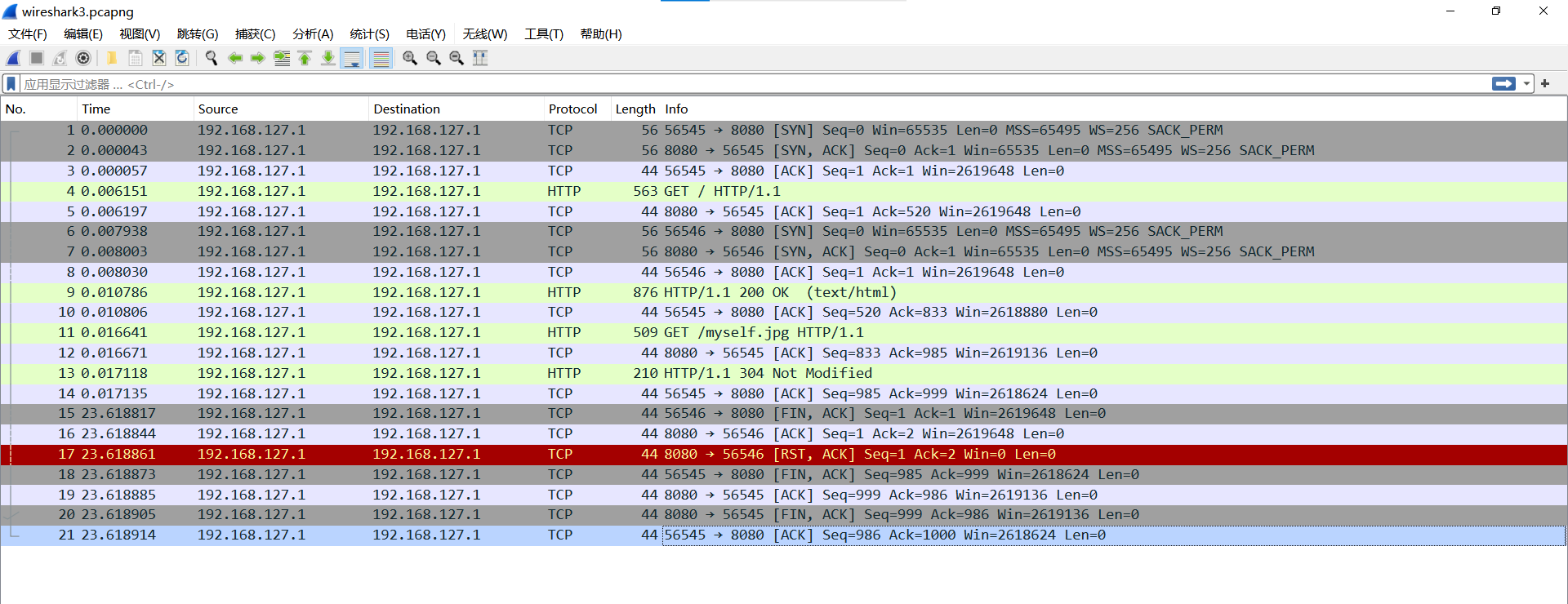
结果如图：



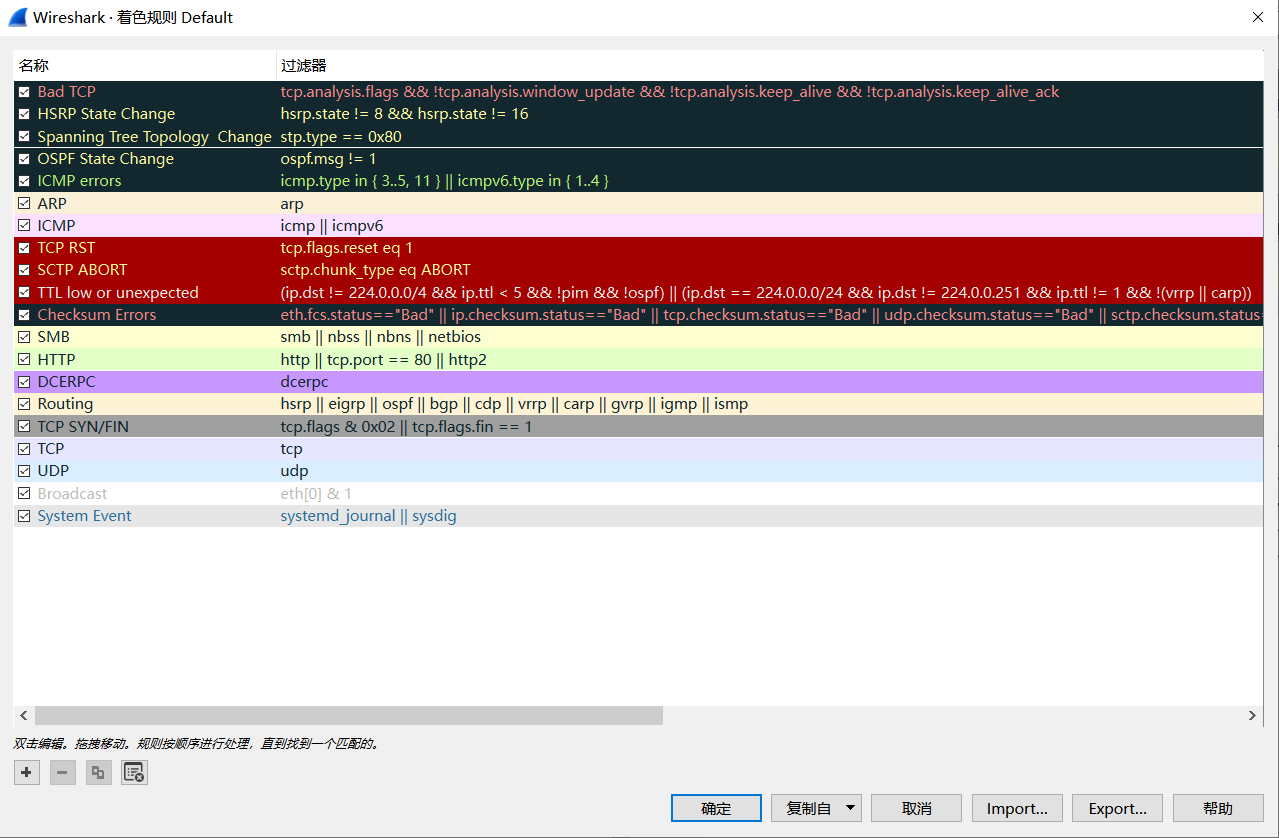
## 美化页面



## 使用wireshark捕获数据包



## 分析数据包



捕获到的数据包含有三种颜色，分别是



指捕获到的数据包为HTTP类型

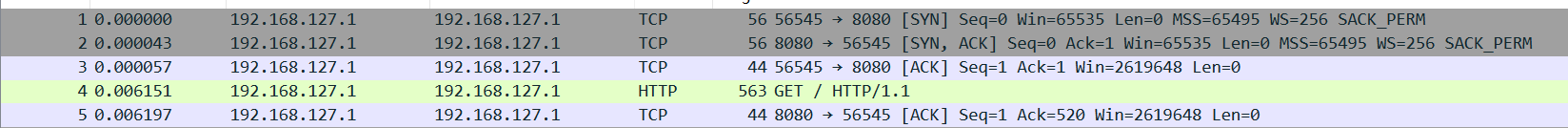


指捕获到的数据包为TCP类型



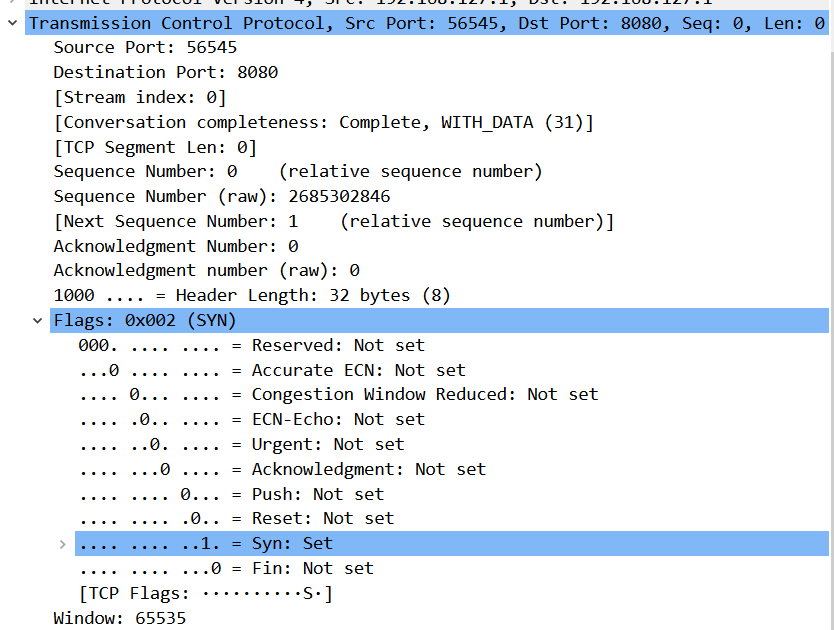
指TCP连接的起始和关闭。

### 三次握手



选择一组连接成功的数据

* 第一条：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。



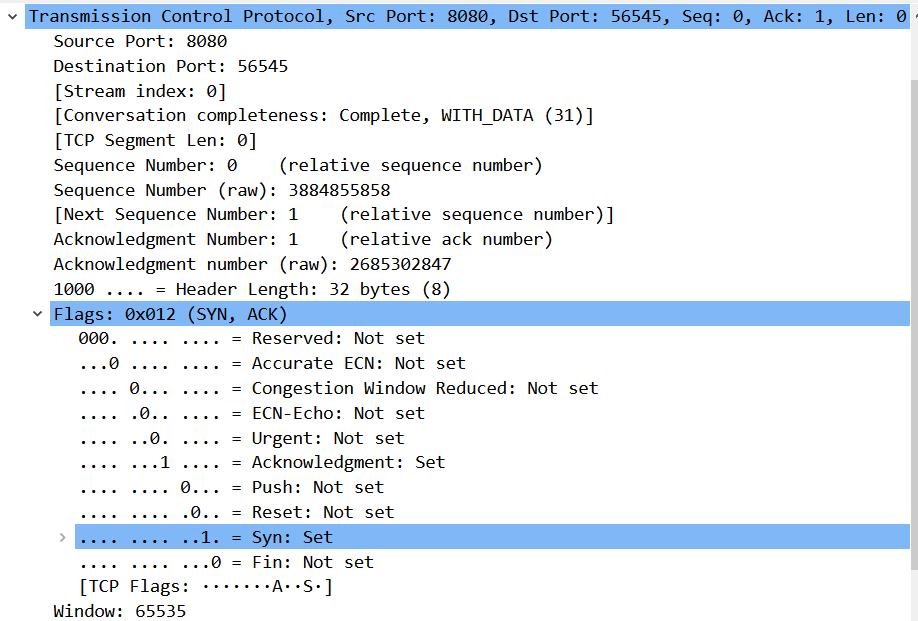
数据包的关键属性如下：

SYN ：标志位，表示请求建立连接

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

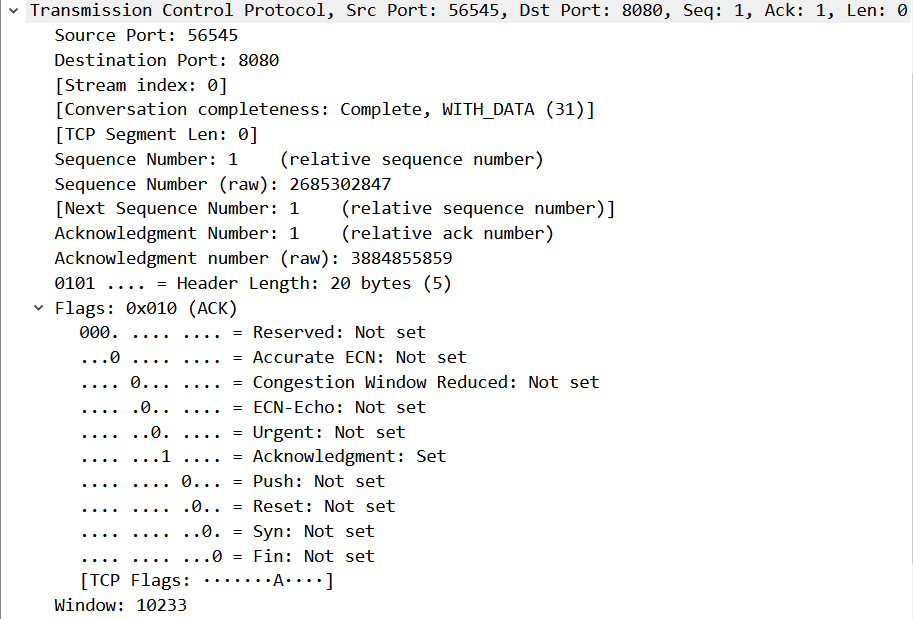
Ack =0：初始建立连接值为0，已经收到包的数量，表示当前没有接收到数据

* 第二条：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, 如下图



数据包的关键属性如下：

* [SYN + ACK]: 标志位，同意建立连接，并回送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）
* 第三条：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, 如下图：



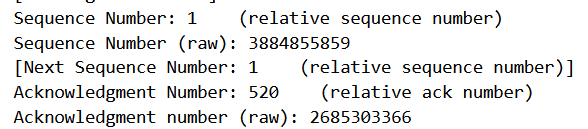
数据包的关键属性如下：

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)。

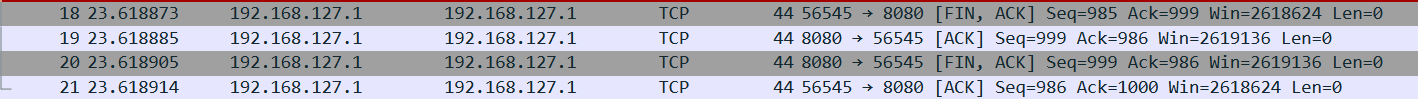
* 第五条



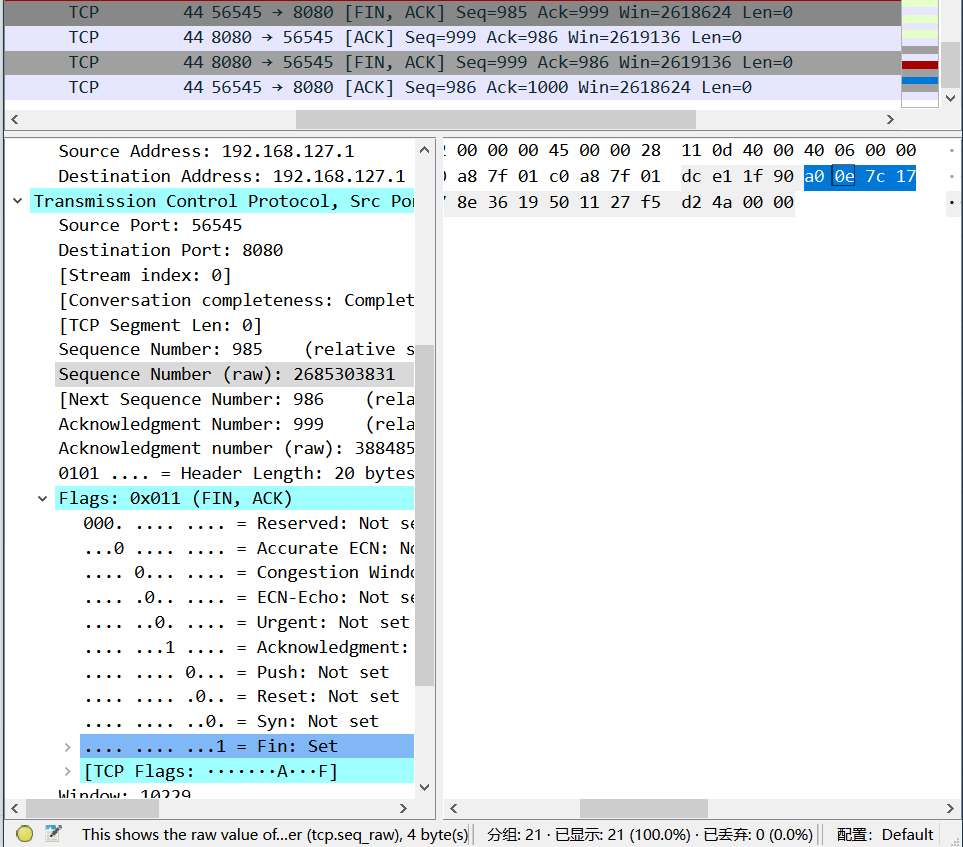
Seq: 1

Ack: 520: 说明现在服务端共收到520字节数据

### 四次挥手

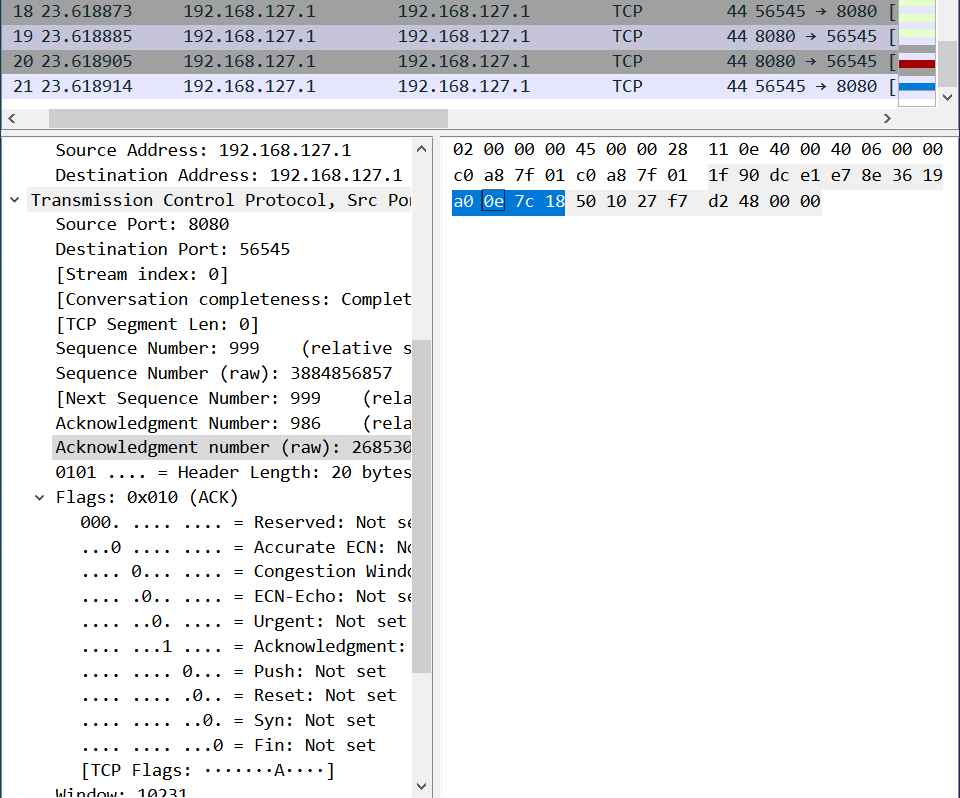


* 第一次挥手



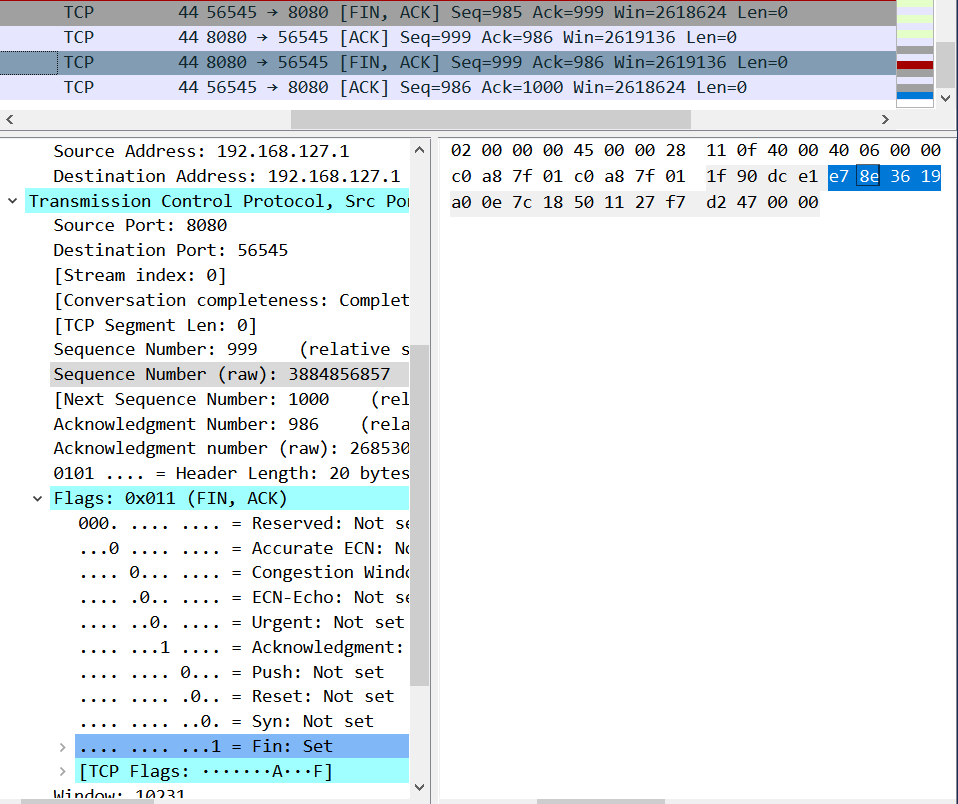
客户端发送了一个FIN，用来关闭客户端到服务器的数据传送。

* 第二次挥手



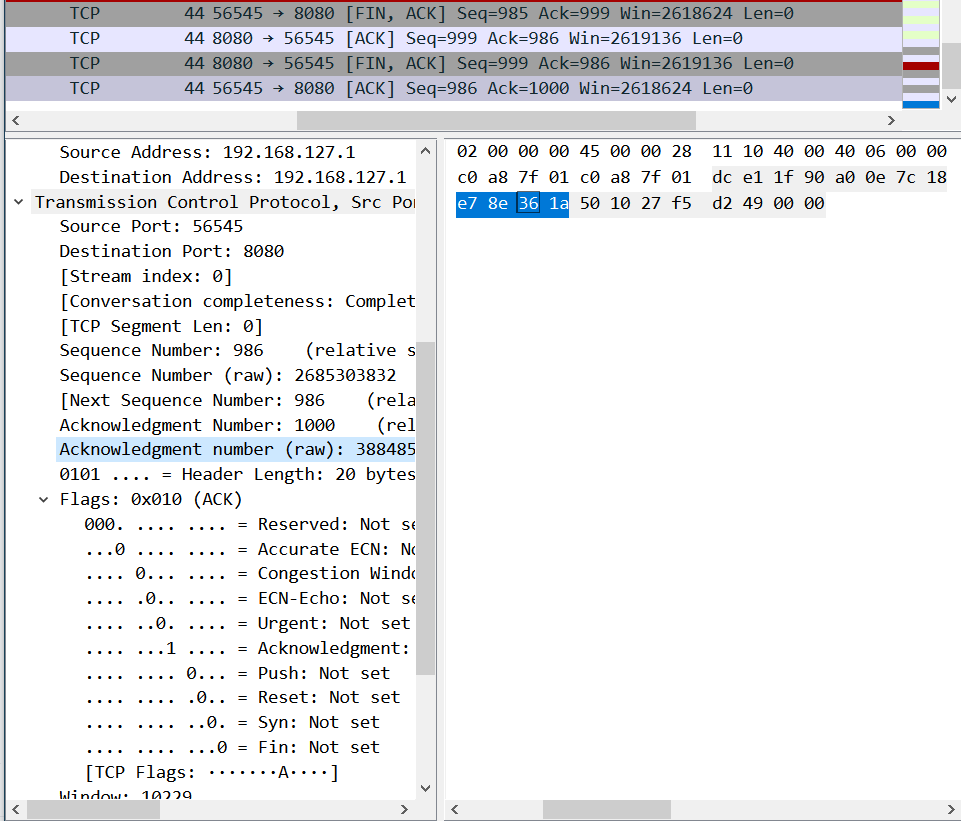
服务端收到了这个Fin，发回一个Ack，确认序号Ack=收到的Seq+1。和SYN一样， 一个FIN将占用一个序号。

* 第三次挥手



服务器关闭和客户端的连接，发送一个Fin给客户端。

* 第四次挥手



客户端发挥Ack报文确认，并将确认序号设置为序号+1，即Ack（发送）=Seq（接收）+1。

### 报错分析

有一条数据包被标记为红色，信息显示[RST,ACK]

RST（重置）：数据包表示之前尝试建立的连接已被关闭或通信应用不接受连接

原因可能是由于我的网页迟迟没有挥手数据包的捕获，于是我关闭了网页，导致连接被关闭。

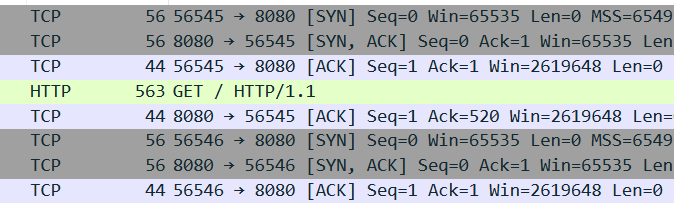
### 其它特殊数据包分析

#### HTTP/1.1 304 Not Modified

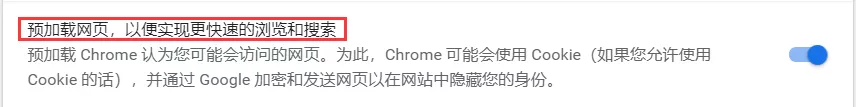
当客户端缓存了目标资源但不确定该缓存资源是否是最新版本的时候, 就会发送一个条件请求。在进行条件请求时,客户端会提供给服务器一个If-Modified-Since请求头,其值为服务器上次返回响应头中Last-Modified值,还会提供一个If-None-Match请求头,值为服务器上次返回的ETag响应头的值。

服务器会读取到这两个请求头中的值,判断出客户端缓存的资源是否是最新的,如果是的话,服务器就会返回HTTP/304 Not Modified响应头, 但没有响应体.客户端收到304响应后,就会从本地缓存中读取对应的资源。 所以：当访问资源出现304访问的情况下其实就是先在本地缓存了访问的资源。

#### 有两个端口同时建立了和网页的连接



使用的是Chrome浏览器，浏览器的默认设置导致的。



# 遇到问题

问题：网站配置好后报错



解决：开启目录浏览

问题：wireshark无法捕获到包

解决：将网站网址中的localhost改为本机ip地址，捕获选项选择下图，而不是WLAN选项



