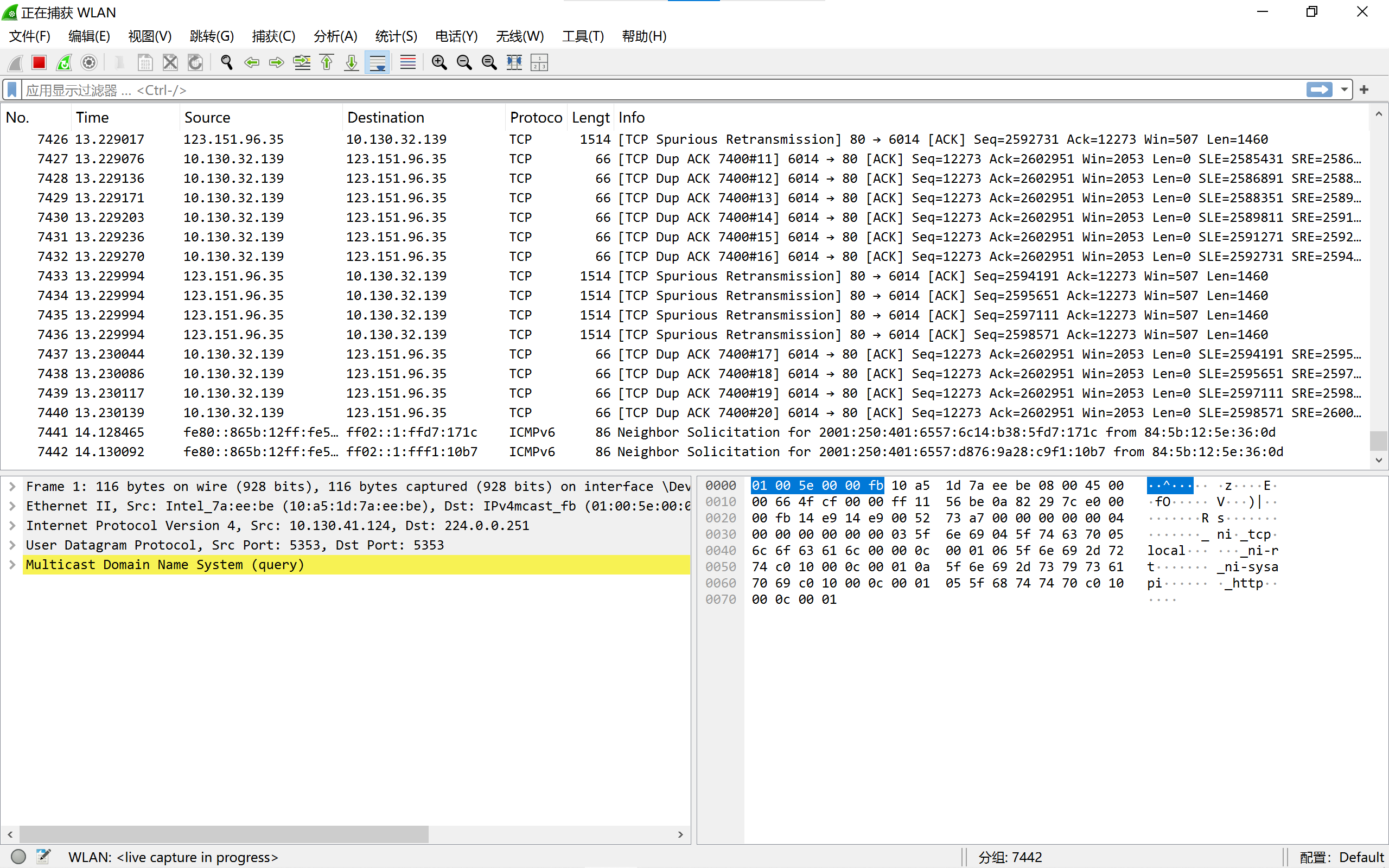
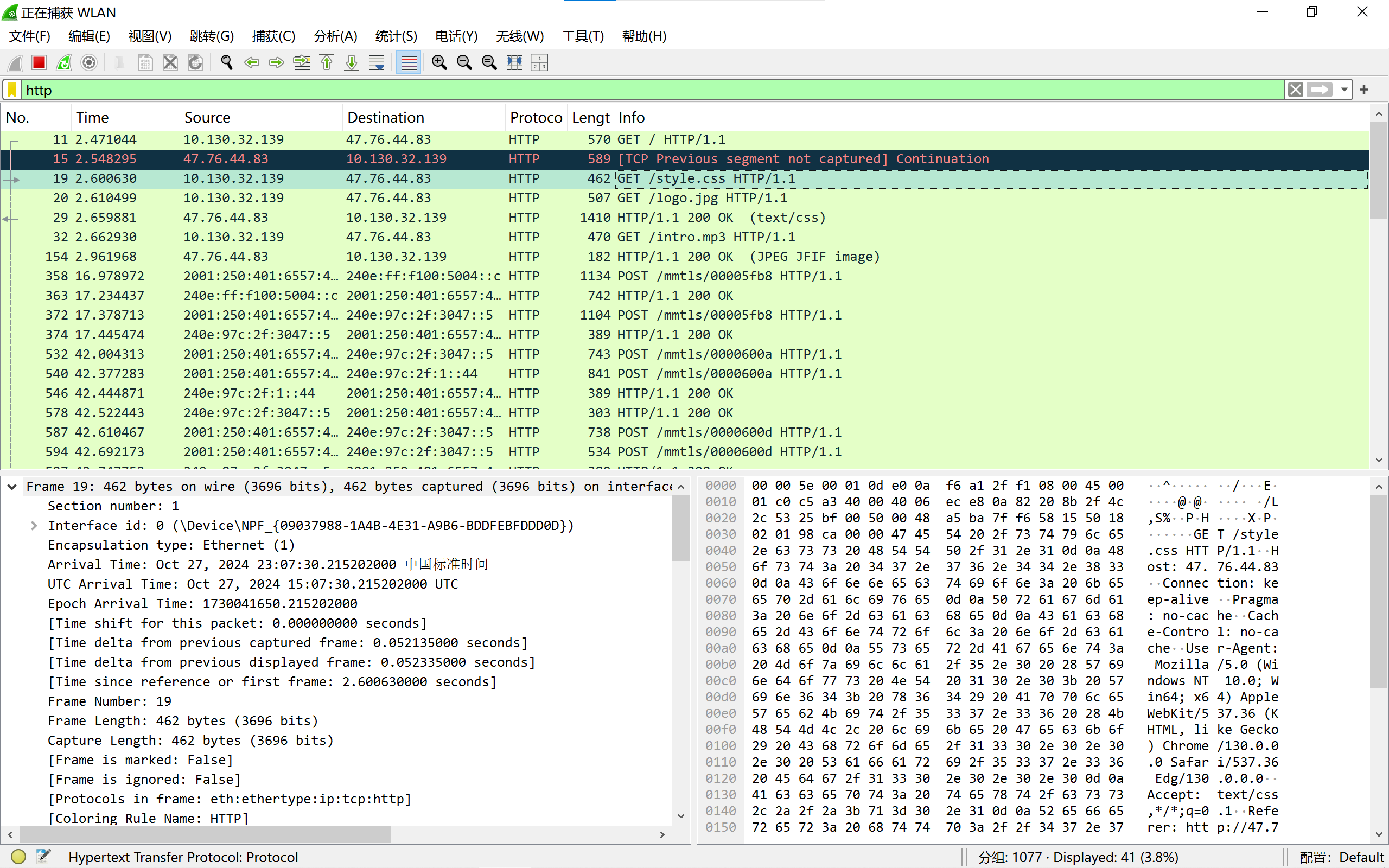
打开wireshark,选择WLAN接口并开始捕获：  


这时浏览器访问我的web网站：emolorry.xyz，浏览器加载并显示界面：



进入wireshark并添加筛选条件：http，从而筛出 http 协议的数据包：



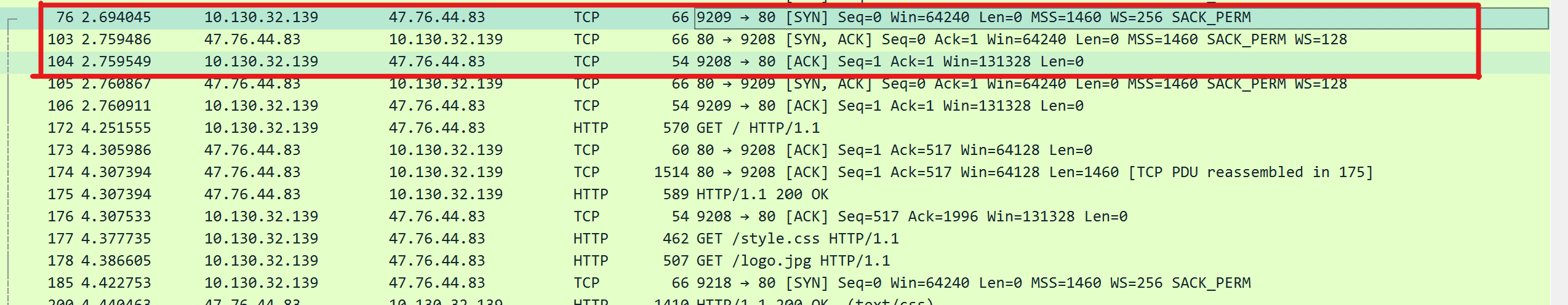
可以看到wireshark显示出来从开始捕获时起到现在所有的HTTP协议的包，注意到与我的主页网址IP <47.76.44.83>有关的几个捕获的包中，有GET请求HTTP、logo.jpg、intro.mp3等内容，对应主机向服务器获取web项目不同类型的资源文件。

连接建立过程与断开连接过程的具体分析：

TCP负责在网络中可靠地传输数据，而HTTP则使用TCP作为底层传输协议，在应用层上实现网页浏览和数据通信。在wireshark的protoco（规则）选择中，TCP对应着传输层，而传输层的作用是建立端口到端口之间的通信，因此在wireshark中想要观测三次握手与四次挥手的过程，就不能再筛选http,否则不能显示有关tcp协议的过程。

我因此此时筛选：ip.addr == 47.76.44.83来观测与该网址的连接的建立和断开的过程：

三次握手：（红框标识的为三次握手的过程）



第一次握手

      客户端向服务器发出连接请求报文，这时报文首部中的同部位SYN=1，同时随机生成初始序列号 seq=x，此时，TCP客户端进程进入了 SYN-SENT（同步已发送状态）状态。TCP规定，SYN报文段（SYN=1的报文段）不能携带数据，但需要消耗掉一个序号。这个三次握手中的开始。表示客户端想要和服务端建立连接。

图中第一条报文：

76 2.694045 10.130.32.139 47.76.44.83 TCP 66 9209 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM

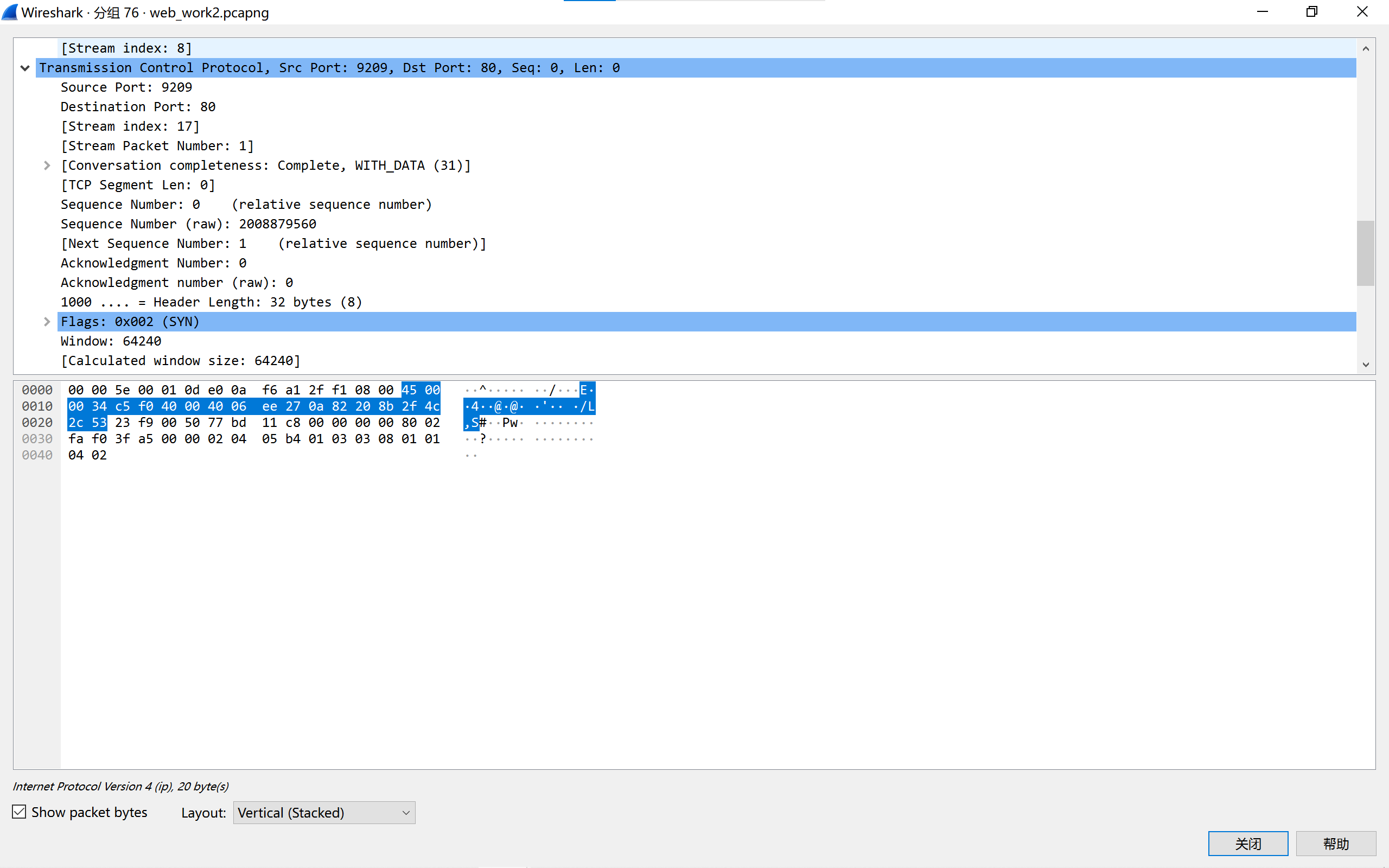
 10.130.32.139 是客户端的IP地址，47.76.44.83 是服务器的IP地址。

 9209 → 80 表示客户端从本地端口 9209 向服务器的端口 80（HTTP端口）发送请求。

 [SYN] 表示这是一个SYN请求，Seq=0 代表初始序列号为0。

 MSS=1460 表示最大分段大小，WS=256 表示窗口大小的缩放因子，SACK\_PERM 表示支持选择性确认（SACK）。

这里查看其具体数据（十六进制类型）及其对应的格式化信息，显示如下：



第二次握手

      TCP服务器收到请求报文后，如果同意连接，则发出确认报文。确认报文中应该 ACK=1，SYN=1，确认号是ack=x+1，同时也要为自己随机初始化一个序列号 seq=y，此时，TCP服务器进程进入了SYN-RCVD（同步收到）状态。这个报文也不能携带数据，但是同样要消耗一个序号。这个报文带有SYN(建立连接)和ACK(确认)标志，询问客户端是否准备好。

图中第二条报文：

103 2.759486 47.76.44.83 10.130.32.139 TCP 66 80 → 9208 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK\_PERM WS=128

 47.76.44.83 是服务器的IP地址，10.130.32.139 是客户端的IP地址。

 80 → 9208 表示服务器从端口 80 向客户端的端口 9208 发送响应。

 [SYN, ACK] 表示此报文带有SYN和ACK标志，用于确认并建立连接。

 Seq=0 表示服务器的初始序列号为0，Ack=1 表示确认号为 x+1。

 Win=64240 表示窗口大小为64240，MSS=1460 表示最大分段大小，SACK\_PERM 表示支持选择性确认。

第三次握手

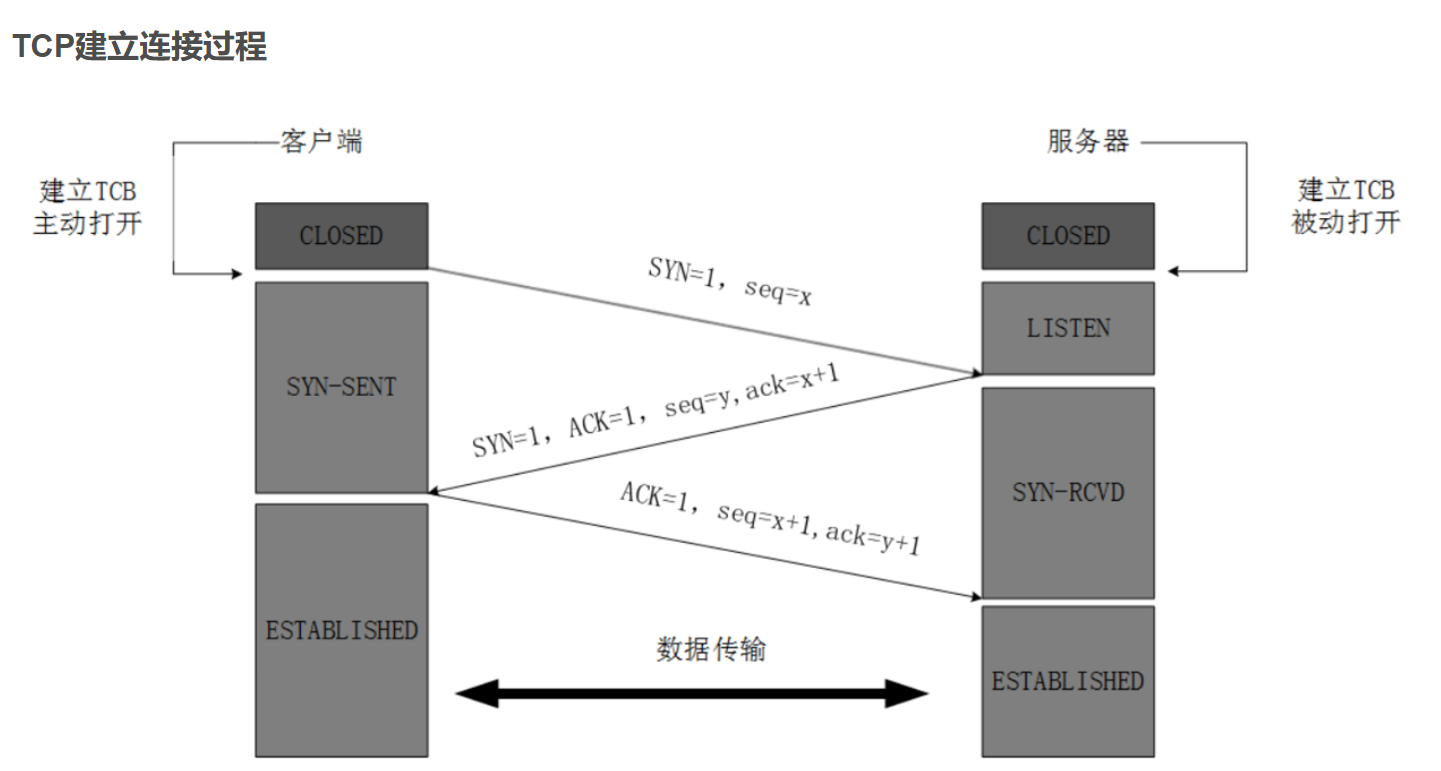
　　 TCP客户进程收到确认后，还要向服务器给出确认。确认报文的ACK=1，ack=y+1，此时，TCP连接建立，客户端进入ESTABLISHED（已建立连接）状态。TCP规定，ACK报文段可以携带数据，但是如果不携带数据则不消耗序号。这里客户端表示我已经准备好。

图中第三条报文：

104 2.759549 10.130.32.139 47.76.44.83 TCP 54 9208 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0

* 10.130.32.139 是客户端的IP地址，47.76.44.83 是服务器的IP地址。
* 9208 → 80 表示客户端从端口 9208 向服务器的端口 80 发送ACK确认。
* [ACK] 表示这是一个确认报文。
* Seq=1 表示客户端的序列号为1，Ack=1 表示确认号为 y+1。
* Win=131328 表示窗口大小为131328。

通过这三次握手，客户端和服务器建立了一个可靠的TCP连接。



四次挥手：

第一次挥手：

第二次挥手：

第三次挥手：

第四次挥手：

