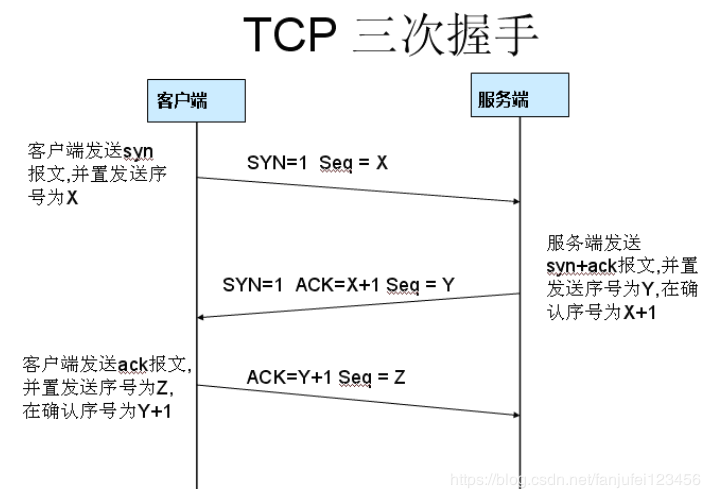
# 操作步骤

（1）打开wireshark，开始捕获界面

（2）打开一个网址（如：csdn）

（3）对捕获的数据包进行分析

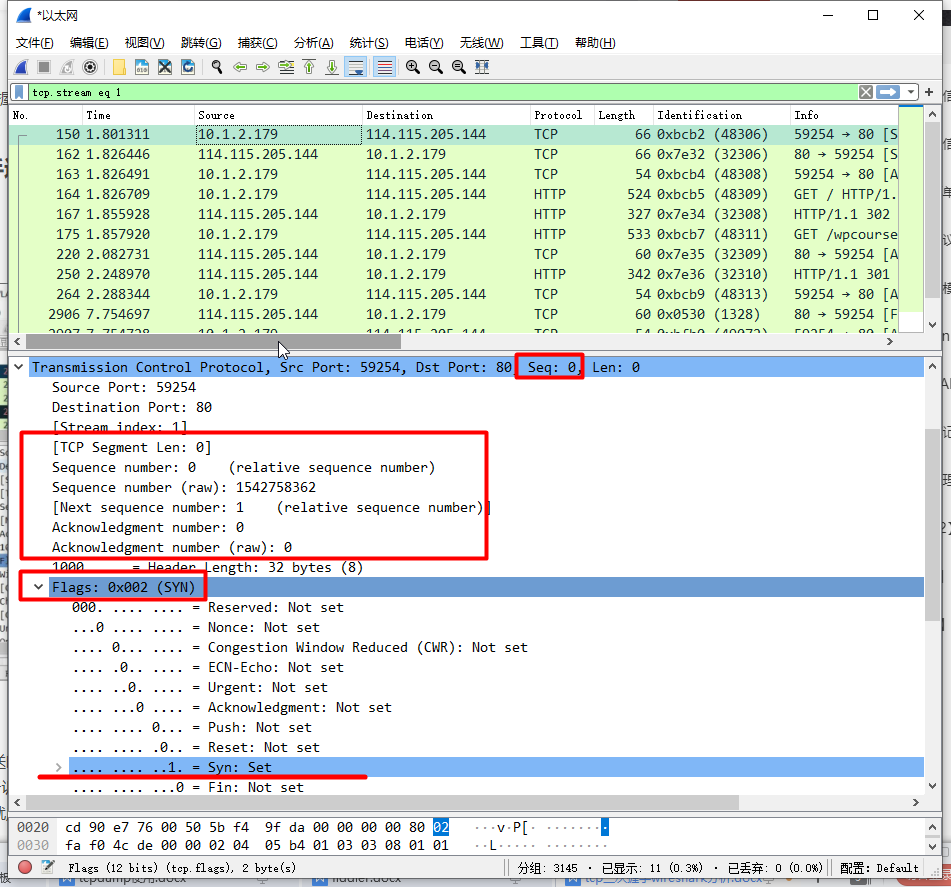


第一个包的作用是第一握手，发送连接请求；第二个包的作用是第二次握手，连接接受；第三个包的作用是第三次握手，对连接接受的确认。

# 三次握手过程分析

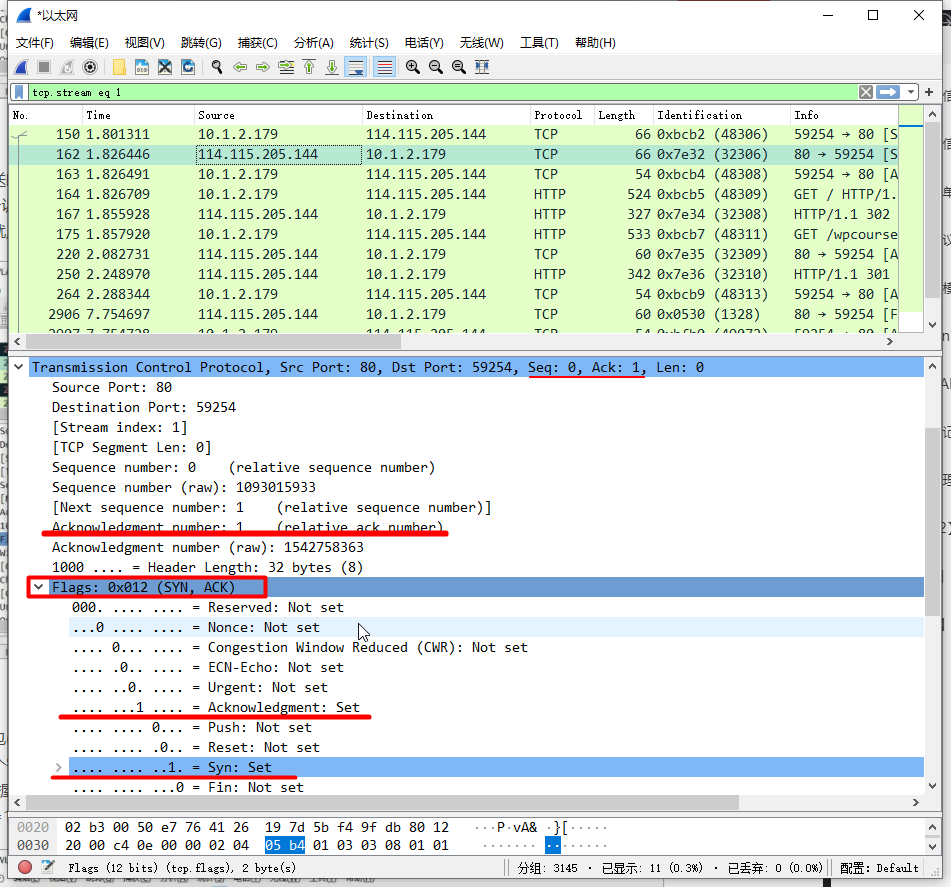
1. 第一次握手

客户端发送一个 TCP，标志位为 SYN（SYN在FLAGS的第二位，所以FLAGS=0x002），序列号seq为0，表示:客户端请求建立连接。



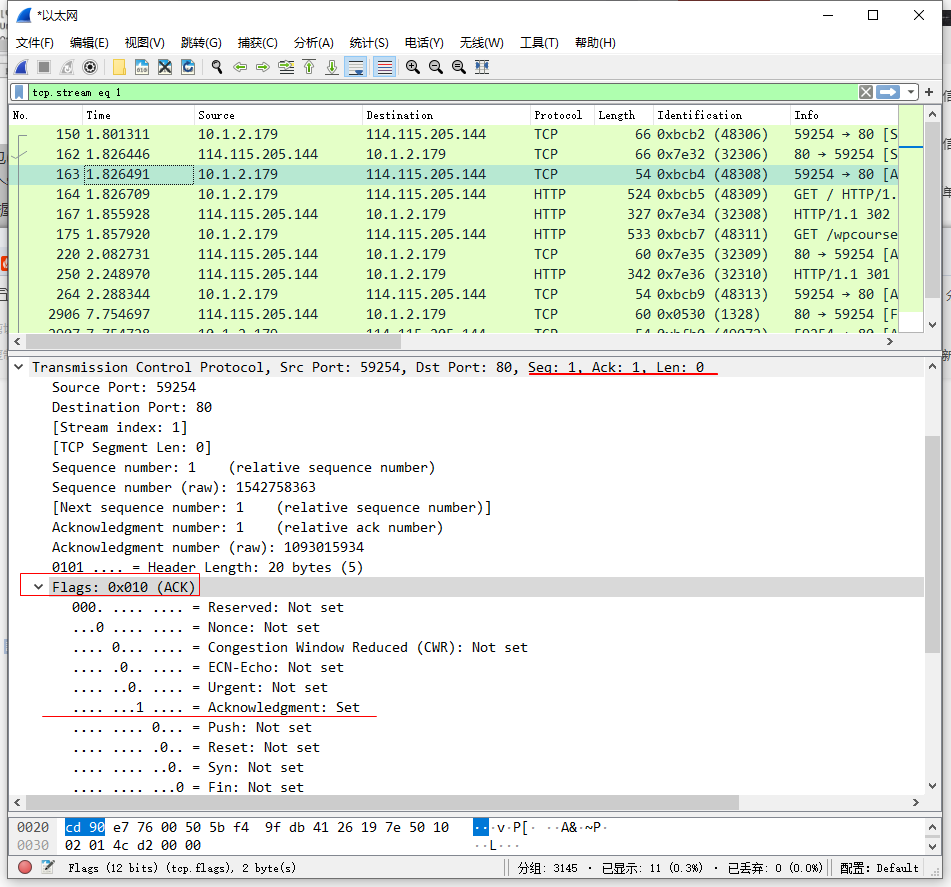
1. 第二次握手

序号说明的是自己发送的数据的编号。 由于确认包是服务器发给客户端的一个数据包，对服务器来讲，这是它的第一个数据包，因此序号 seq=0。确认号是告诉对方，下一个应该发送的数据字节的编号。由于对方（客户端）上一次（第二次握手） 发来 seq 的序号字段是0，下一个应该发送的就应该是0+1=1,因此服务器发回的确认包中的确认号是1（ACK=0+1=1）。



1. 第三次握手

客户端再次发送确认包(ACK) SYN 标志位为0,ACK 标志位为 ACK 有效.序号说明的是自己发送的数据的编号。由于客户端第一次握手的数据字段已成功发送1个字节，因此数据字段序号 seq 从0变为1。确认号是告诉对方，下一个应该发送的数据字节的编号。由于对方（服务器）上一次（第二次握手） 发来 seq 的序号字段是0，下一个应该发送的就应该是0+1=1,放在确定字段中发送给对方（ACK=0+1=1）。



# Wireshark对应网络层

