



**计算机网络实验报告**

**姓名：**

**学号：**

**专业：**

**使用Wireshark操作TCP的三次握手**

一、实验目的

1. 了解Tcp的数据组成部分

2. 理解Tcp三次握手的基本原理

3. 用Wireshark抓包来进一步理解Tcp的三次握手原理

二、实验环境

Windows wireshark

三、具体做法

1. Tcp的数据组成部分，并结合抓包数据进行分析对应。

源端口和目的端口字段——各占2字节。端口是传输层与应用层的服务接口。传输层的复用和分用功能都要通过端口才能实现。

　　序号字段——占4字节。TCP连接中传送的数据流中的每一个字节都编上一个序号。序号字段的值则指的是本报文段所发送的数据的第一个字节的序号。

　　确认号字段——占4字节，是期望收到对方的下一个报文段的数据的第一个字节的序号。它和IP数据包头部一样，也有个Options字段，长度是不固定的，而为了要确认整个TCP封包大小，就需要这个标志来说明整个封包区段的起始位置。

　　数据偏移——占4bit，它指出TCP报文段的数据起始处距离 CP报文段的起始处有多远。“数据偏移”的单位不是字节而是32bit字（4字节为计算单位）。

　　保留字段——占6bit，保留为今后使用，但目前应置为0。

　　紧急比特URG——当URG＝1时，表明紧急指针字段有效。它告诉系统此报文段中有紧急数据，应尽快传送(相当于高优先级的数据)。

　　确认比特ACK——只有当ACK＝1时确认号字段才有效。当ACK＝0时，确认号无效。

　　复位比特RST(Reset) —— 当RST＝1时，表明TCP连接中出现严重差错（如由于主机崩溃或其他原因），必须释放连接，然后再重新建立运输连接。

　　同步比特SYN——同步比特SYN置为1，就表示这是一个连接请求或连接接受报文。

　　终止比特FIN(FINal)——用来释放一个连接。当FIN＝1时，表明此报文段的发送端的数据已发送完毕，并要求释放运输连接。

　　窗口字段——占2字节。窗口字段用来控制对方发送的数据量，单位为字节。TCP连接的一端根据设置的缓存空间大小确定自己的接收窗口大小，然后通知对方以确定对方的发送窗口的上限。

　　TCP检验和——占2字节。当数据要由发送端送出前，会进行一个检验的动作，并将该动作的检验值标注在这个字段上； 而接收者收到这个封包之后，会再次的对封包进行验证，并且比对原发送的 Checksum 值是否相符，如果相符就接受，若不符就会假设该封包已经损毁，进而要求对方重新发送此封包！在计算检验和时，要在TCP报文段的前面加上12字节的伪首部。

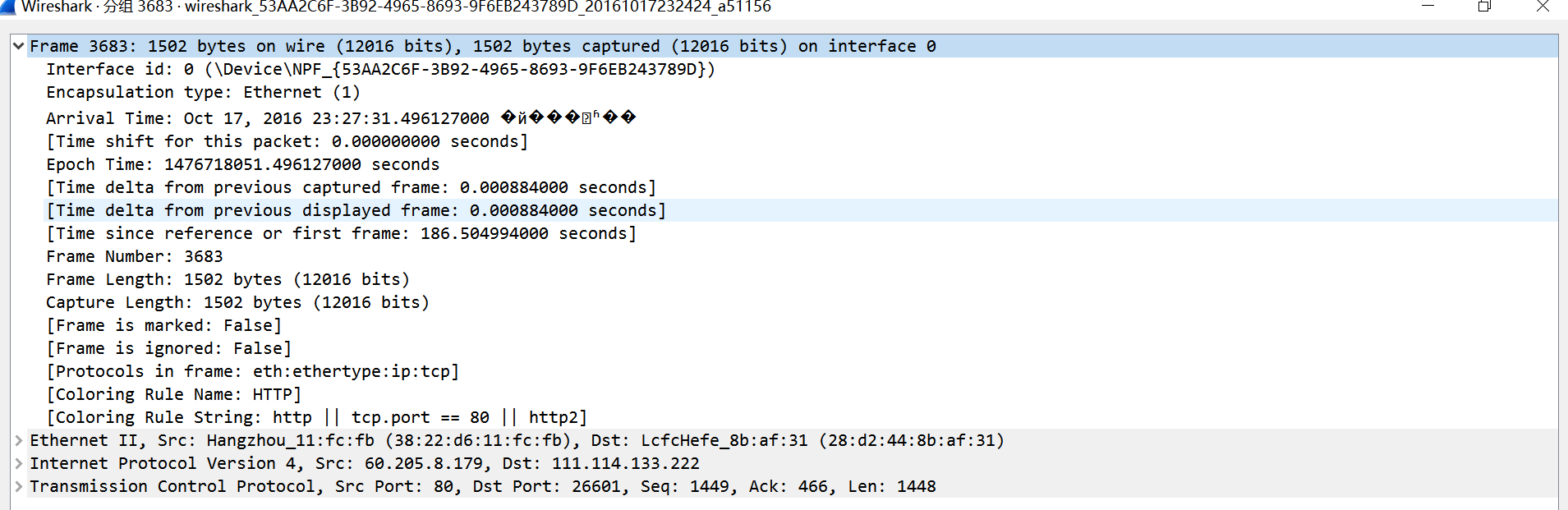
　　紧急指针字段——占16bit。这个字段是在 Code 字段内的 URG = 1 时才会产生作用。可以告知紧急数据所在的位置。紧急指针指出在本报文段中的紧急数据的最后一个字节的序号。

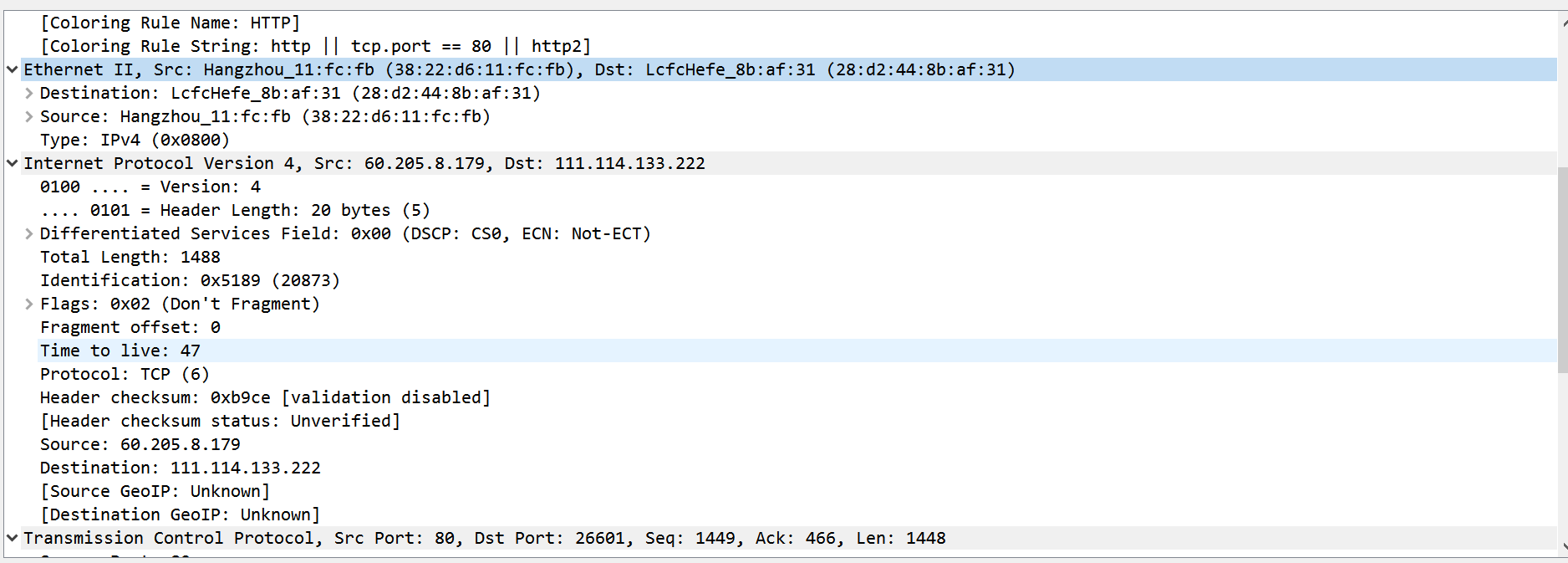
　　选项字段——长度可变。TCP首部可以有多达40字节的可选信息，用于把附加信息传递给终点，或用来对齐其它选项。目前此字段仅应用于表示接收端可以接收的最大数据区段容量，若此字段不使用， 表示可以使用任意数据区段的大小。 这个字段较少使用。

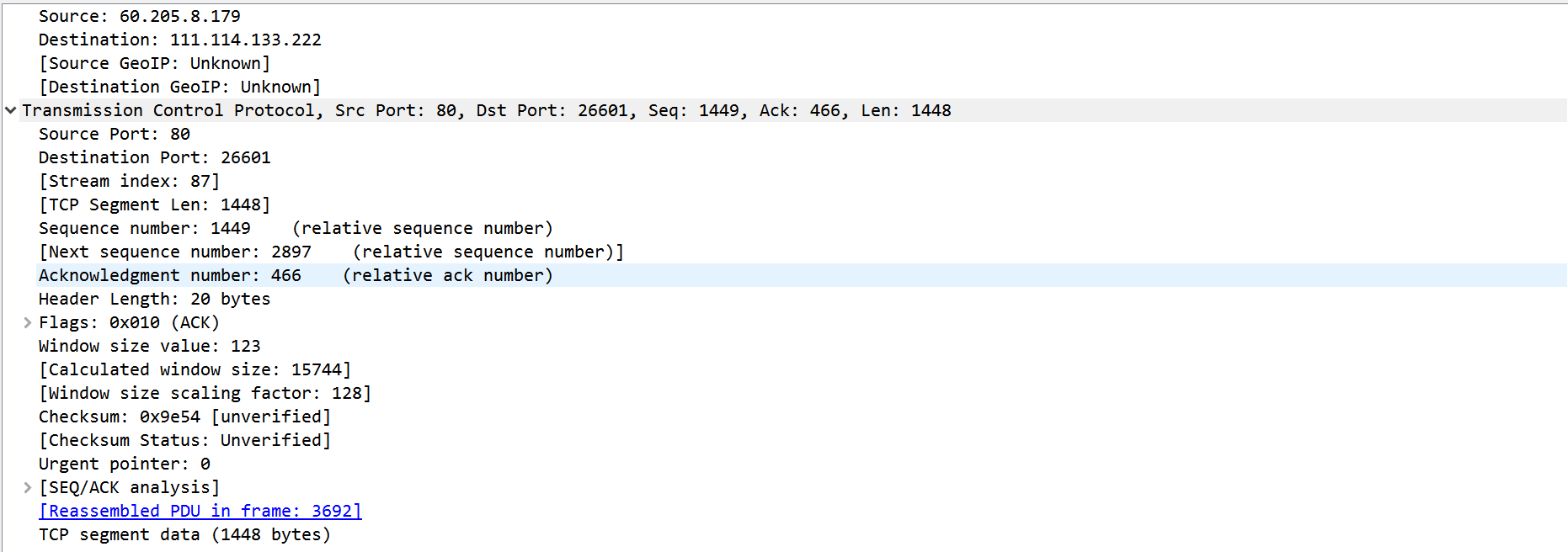
TCP首部的主要选项：

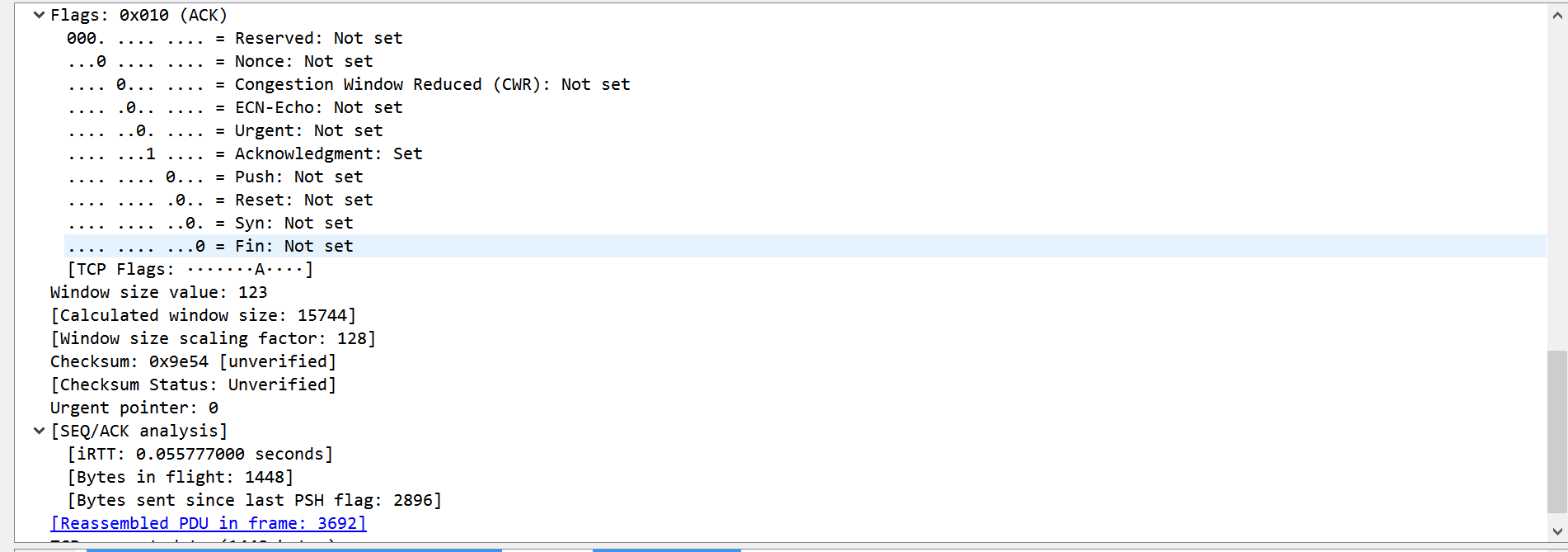
最大报文段长度MSS(Maximum Segment Size)是TCP报文段中的数据字段的最大长度。MSS告诉对方TCP：“我的缓存所能接收的报文段的数据字段的最大长度是MSS个字节。”

填充字段——如同 IP 封包需要有固定的 32bits 表头一样， Options 由于字段为非固定， 所以也需要 Padding 字段来加以补齐才行。同样也是 32 bits 的整数。这是为了使整个首部长度是4字节的整数倍。

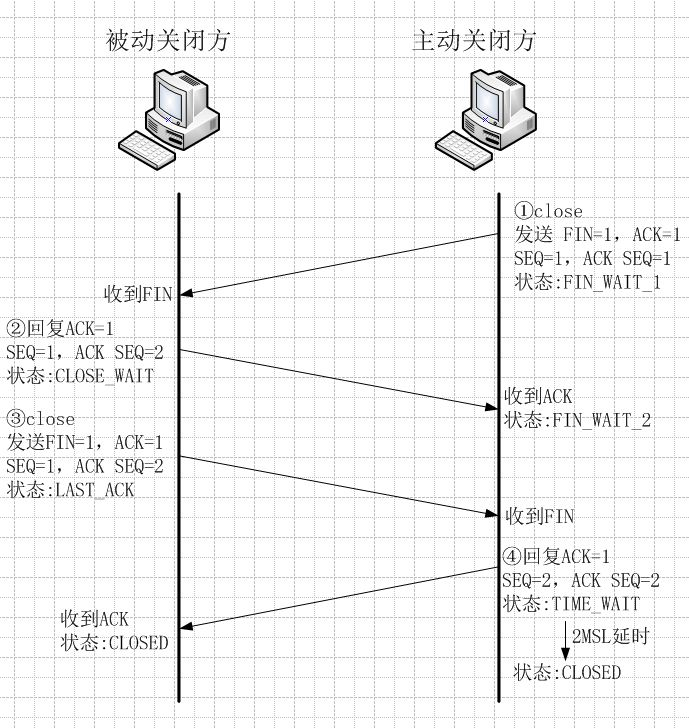






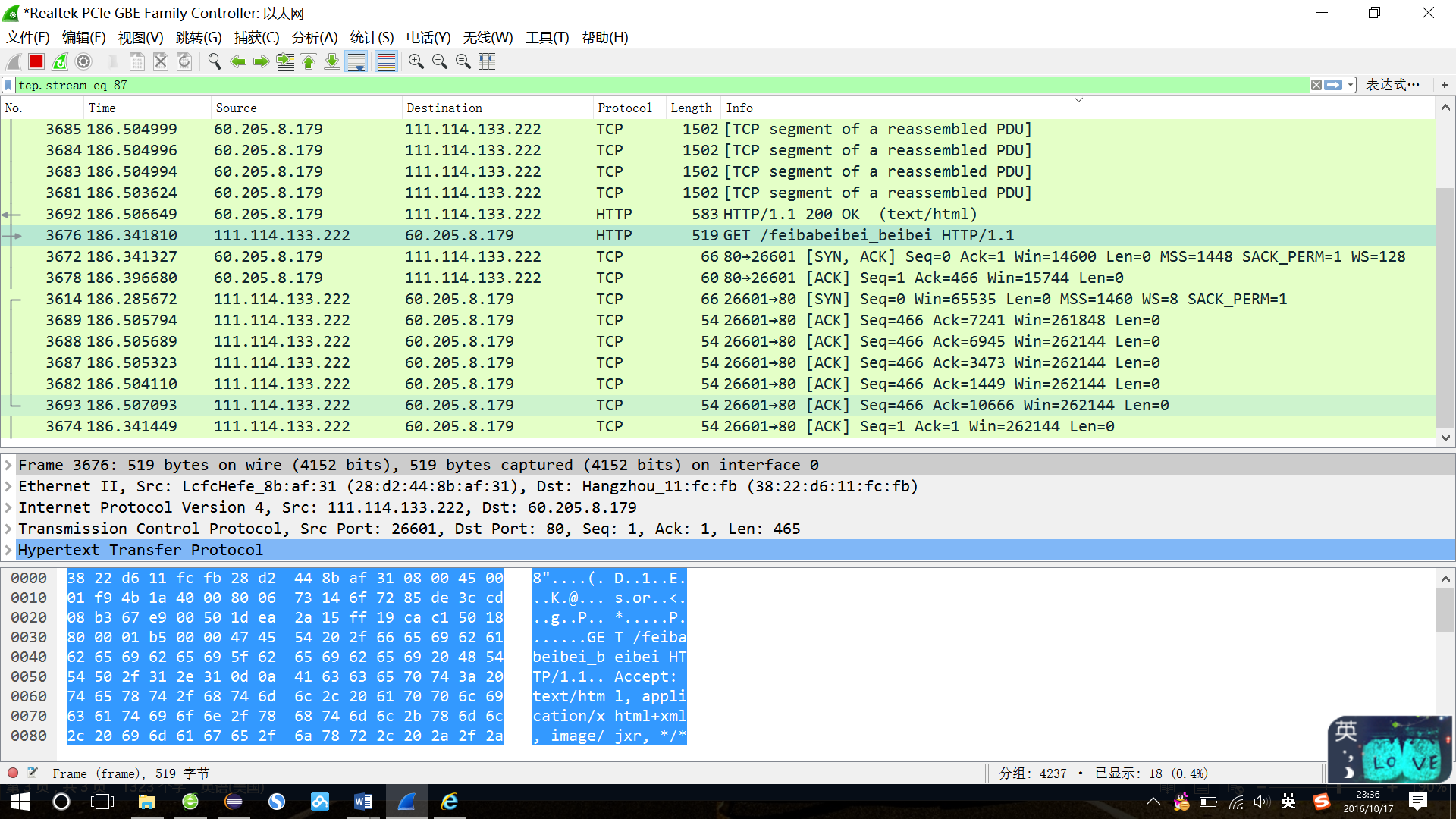


2.三次握手的过程



在TCP/IP协议中，TCP协议提供可靠的连接服务，采用三次握手建立一个连接。   
 第一次握手：建立连接时，客户端发送syn包(syn=j)到服务器，并进入SYN\_SEND状态，等待服务器确认；   
 第二次握手：服务器收到syn包，必须确认客户的SYN（ack=j+1），同时自己也发送一个SYN包（syn=k），即SYN+ACK包，此时服务器进入SYN\_RECV状态；   
 第三次握手：客户端收到服务器的SYN＋ACK包，向服务器发送确认包ACK(ack=k+1)，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。   
 完成三次握手，客户端与服务器开始传送数据。

3. 分析每一次的握手过程：



由图可知：

在第一次握手中：Seq=0， Ack=1，Win=14600 Len=0 MSS=1488 SACK\_PERM=1;

在第二次握手中：Seq=1，ACK=466,Win=15744,Len=0;

在第三次握手中：Seq=466，ACK=7241,Win=261848,Len=0;

四、心得体会

本次上机主要学到了TCP的三次握手，包括TCP的数据组成部分分析，以及其基本原理，首先进行抓包，其次对抓包数据进行分析整理，并与理论知识相对应，对三次握手过程也进行了详细分析，不足之处在于对基础知识的理解不到位，对抓到的包中的数据辨识度不高，不会具体进行分类，对三次握手中Seq和Ack的变化不太理解，但是随后通过查资料以及上网查询得到了较为详细的解释。所以今后应加强预习，同时课后要及时复习，使得知识掌握的更加牢固。