Week 11: TCP协议分析

一、实验目的

- 了解 TCP 协议的工作原理
  - 学习TCP建立连接三次握手的过程
  - 学习TCP断开连接四次挥手的过程

二、实验任务

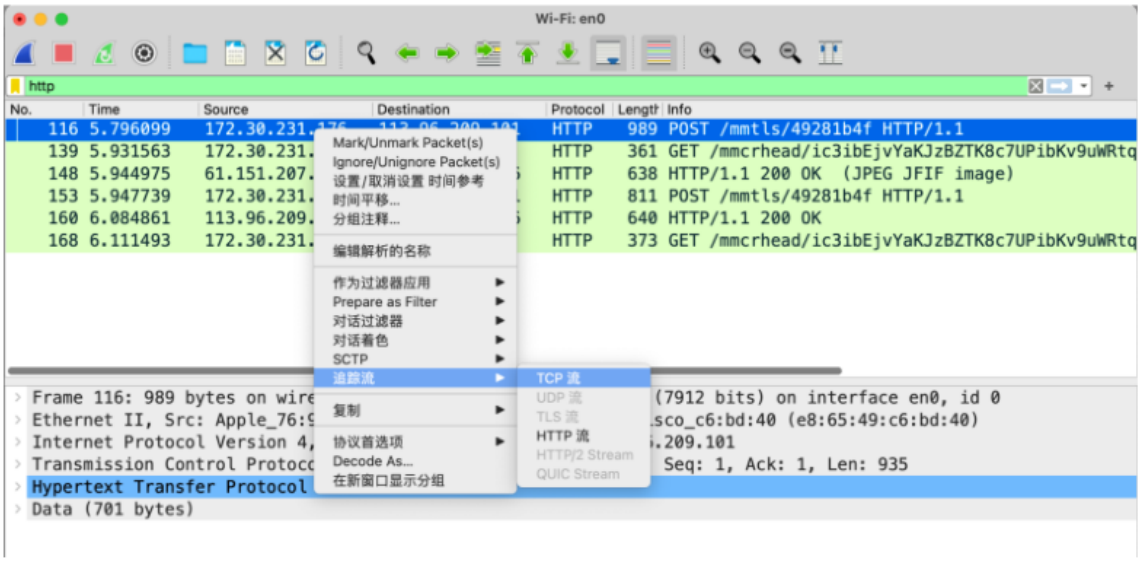
- 使用Wireshark快速了解TCP协议

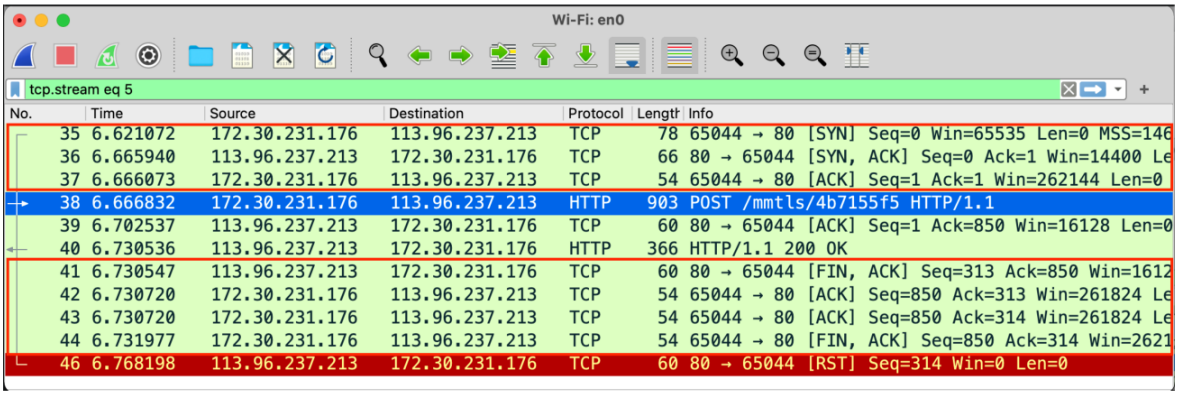
三、实验过程

3.1 TCP协议

TCP是因特网运输层的**面向连接的可靠的运输协议。**TCP被称为是面向连接的（connection.oriented），这是因为在一个应用进程可以开始 向另一个应用进程发送数据之前，这两个进程必须先**相互"握手"**，即它们必须相互发送某些预备报文段，以建立确保数据传输的参数。作为TCP连接建立的一部分，连接的双方都将初始化与TCP连接相关的许多TCP状态变量。

图 3-29　TCP 报文段结构

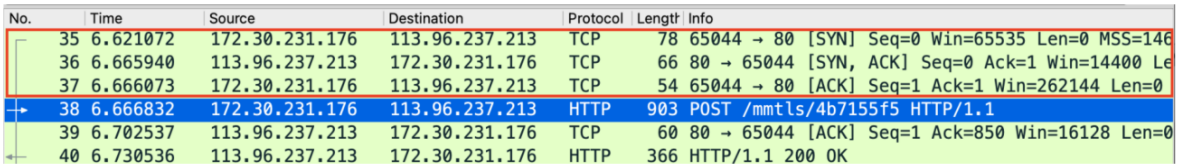


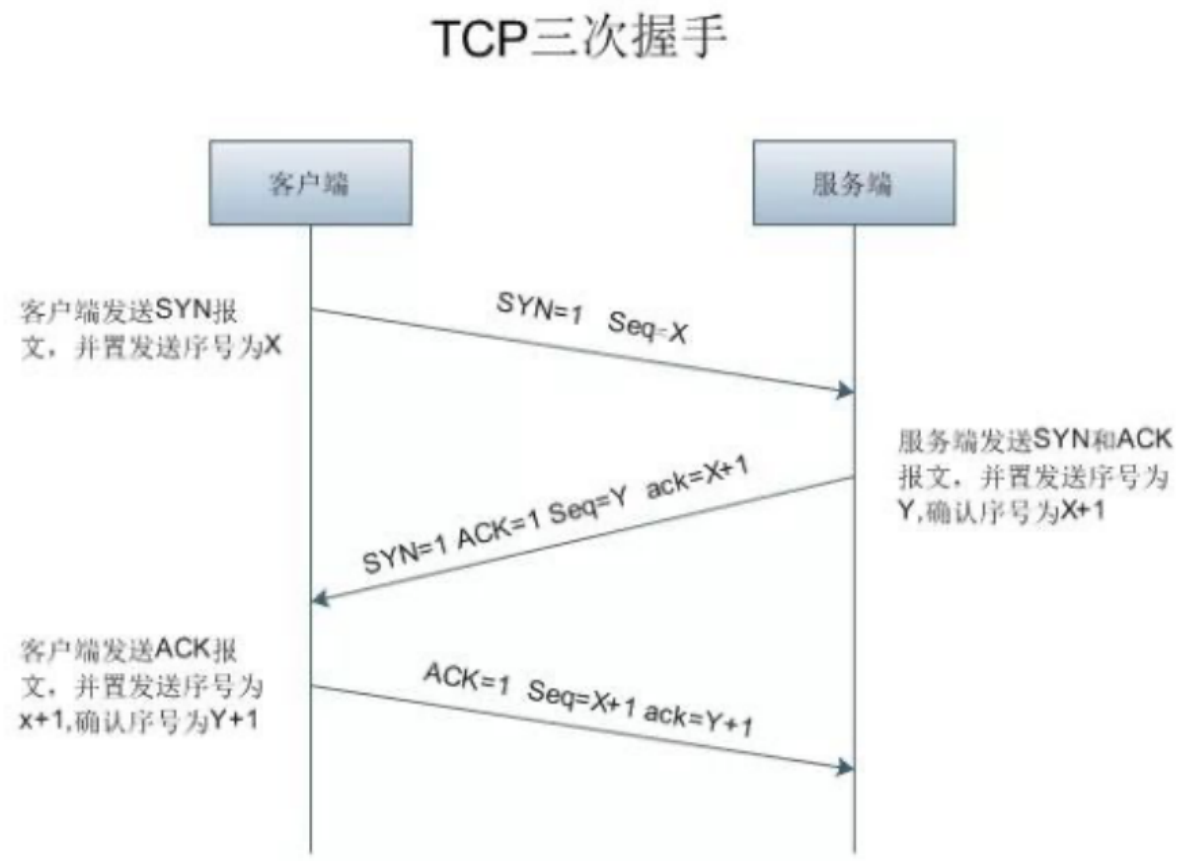


task1: 利用Wireshark抓取一个TCP数据包，查看其具体数据结构和实际的数据（要求根据报文结构正确标识每个部分），请将实验结果附在实验报告中。

3.2 TCP三次握手

- TCP建立连接时，会有三次握手过程，如下图所示，Wireshark截获到了三次握手的三个数据包。第四个包才是http的，说明http的确是使用TCP建立连接的。

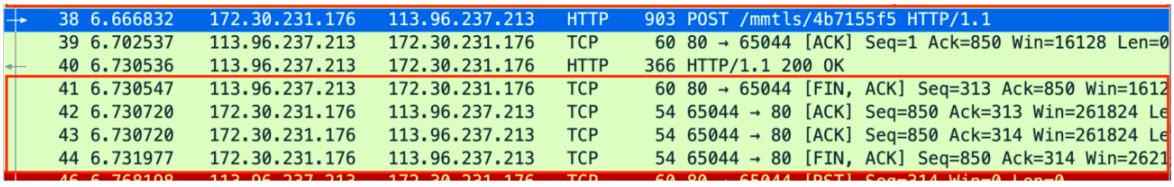


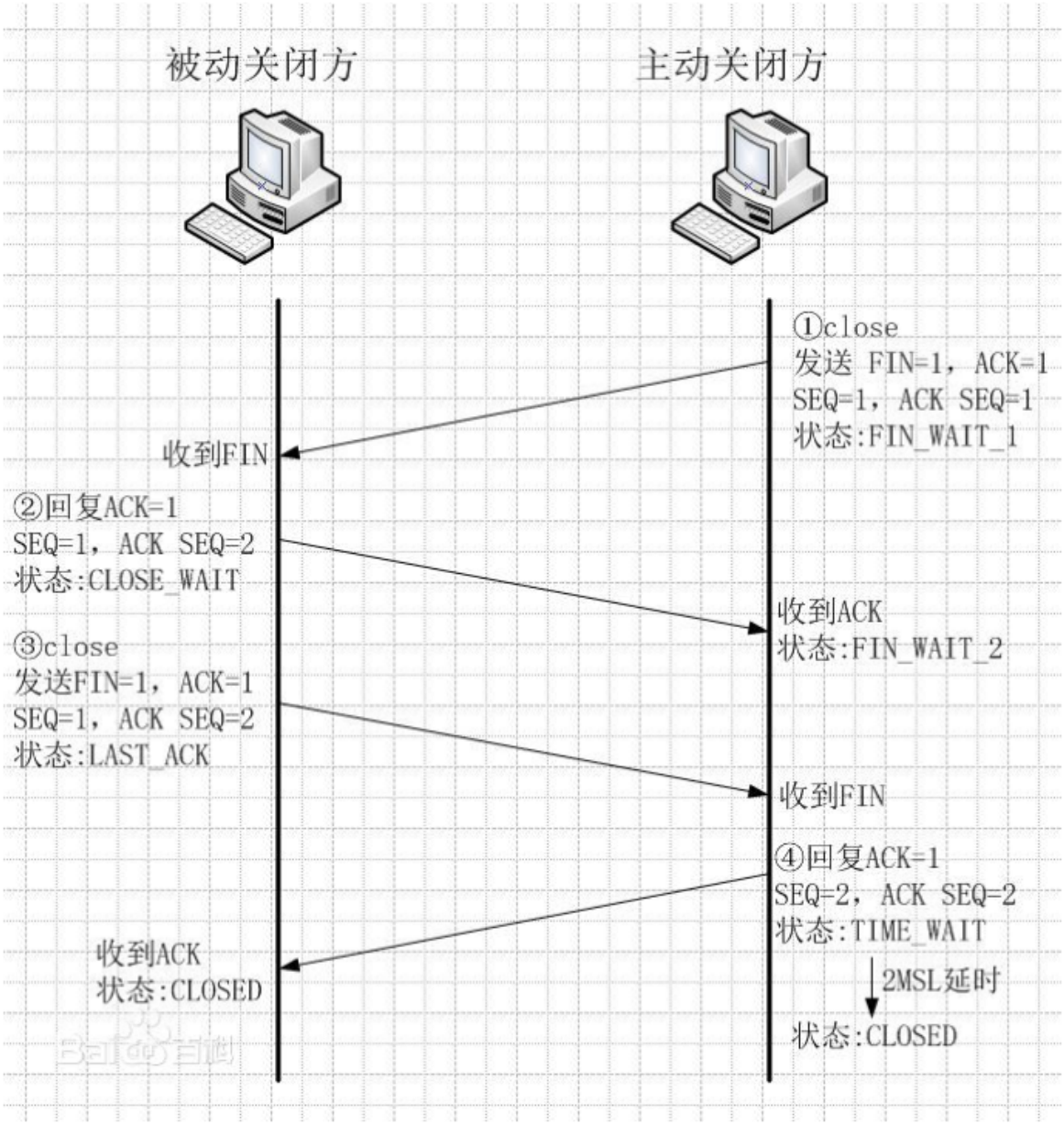


task2: 根据TCP三次握手的交互图和抓到的TCP报文详细分析三次握手过程，请将实验结果附在实验报告中。

3.3 TCP四次挥手

- 当通信双方完成数据传输，需要进行TCP连接的释放，由于TCP连接是全双工的，因此每个方向都必须单独进行关闭。这个原则是当一方完成它的数据发送任务后就能发送一个FIN来终止这个方向的连接。收到一个 FIN只意味着这一方向上没有数据流动，一个TCP连接在收到一个FIN后仍能发送数据。首先进行关闭的一方将执行主动关闭，而另一方执行被动关闭。因为正常关闭过程需要发送4个TCP帧，因此这个过程也叫作4次挥手。如下图所示，Wireshark截获到了四次挥手的四个数据包。





task3: 根据TCP四次挥手的交互图和抓到的TCP报文详细分析四次挥手过程，请将实验结果附在实验报告中。