杭州电子科技大学计算机网络实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 | 郑凯心 | 学号 | 19063140 | | |
| 组别 | 4 | 时间 | 20211224 | | |
| 小组成员 | 郑凯心 张浩杨 符振皓 林伟杰 汤丰瑜 蔡思林 王常平 王浩冰 | | | | |
| 实验名称 | TCP协议 | | | 序号 | 1 |

一、实验目的：

(1)了解TCP报文段的结构。

(2)掌握TCP数据流追踪的方法。

(3)理解TCP三次握手的基本过程。

(4)理解TCP连接终止的基本过程。

(5)认识TCP重置。

(6)理解TCP可靠数据传输的基本原理。

二、实验内容及原理：

TCP可以说是Internet提供的最重要传输服务了。我们在第3部分学习了TCP协议的基本原理和Socket编程。本节将通过Wireshark软件捕获TCP客户机和服务器连接建立、数据传输、连接终止等数据包，深入学习TCP连接建立和终止的过程，了解TCP可靠传输机制的工作原理和TCP传输控制变量在这个过程中的作用。

三、实验设备及拓扑结构：

本实验可以使用WiFi接入，例如无线路由器或是无线AP，也可以使用有线局域网接

入。但都应该具有Internet 连接。另外还需要- -台安装有Wireshark软件的PC。

四、实验过程及结果

1. TCP连接的建立

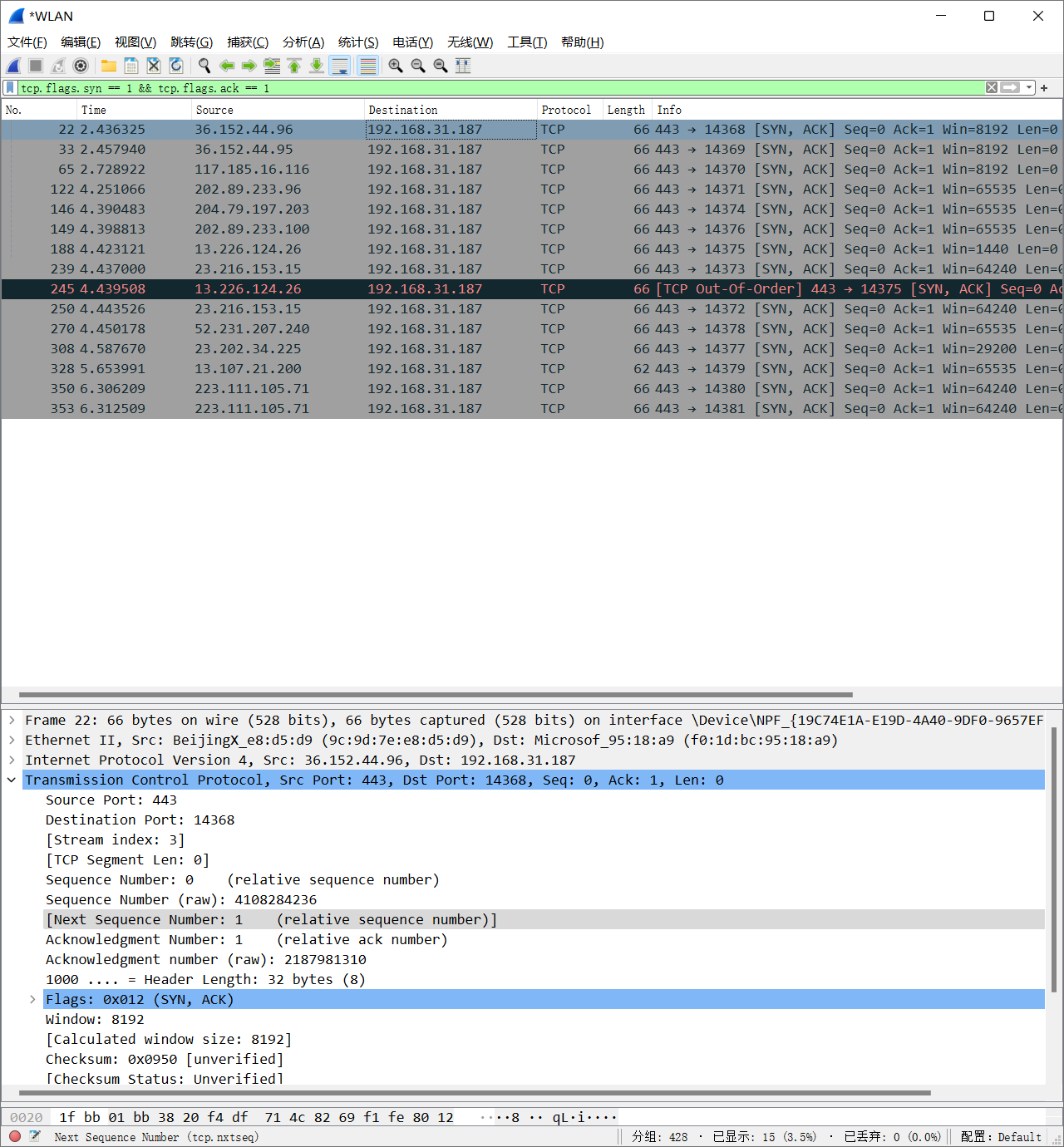
追踪任何一个TCP数据流，该数据流开始的三个数据包都是其连接建立过程的三次握

手。也可以使用FLAGS标志位进行检索，例如三次握手的第二个数据包非常特殊，SYN

ACK同时置位，可以利用这个特点发现一个三次握手的过程。

访问 baidu.com。Wireshark过滤显示SYN ACK置位数据包

tcp.flags.syn == 1 && tcp.flags.ack == 1



2. TCP连接的终止

在每个正常结束的TCP数据流中，其尾部都是TCP连接终止时在客户机和服务器间

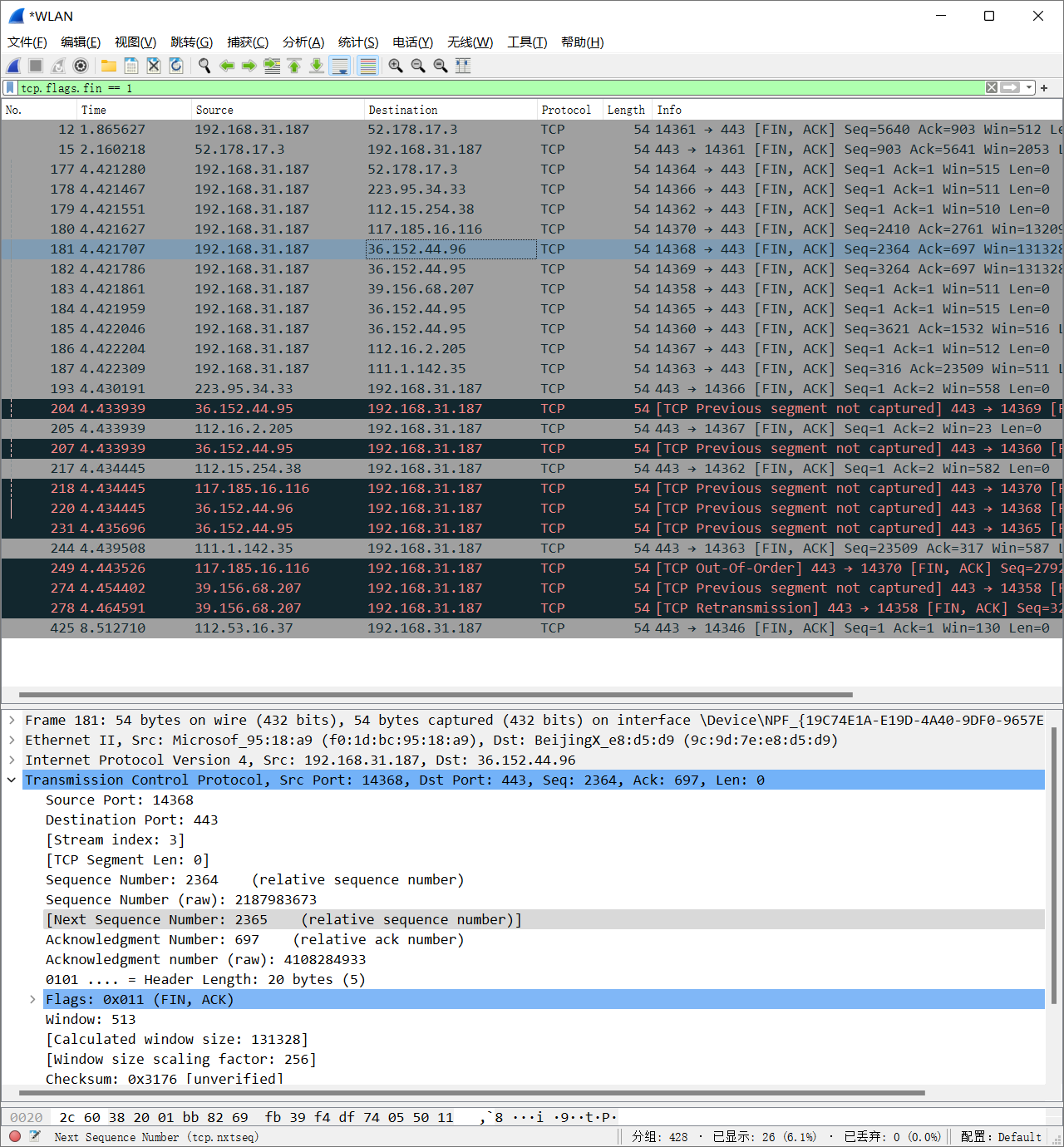
的数据包交互。TCP通信的双方都有权力发起TCP连接的终止，也可以使用FLAGS标志

位进行检索。例如发起TCP连接终止的数据包非常特殊，FIN 置位，可以利用这个特点发

现一-次终止过程。

Wireshark过滤显示FIN置位数据包

tcp.flags.fin == 1



3. TCP连接的重置

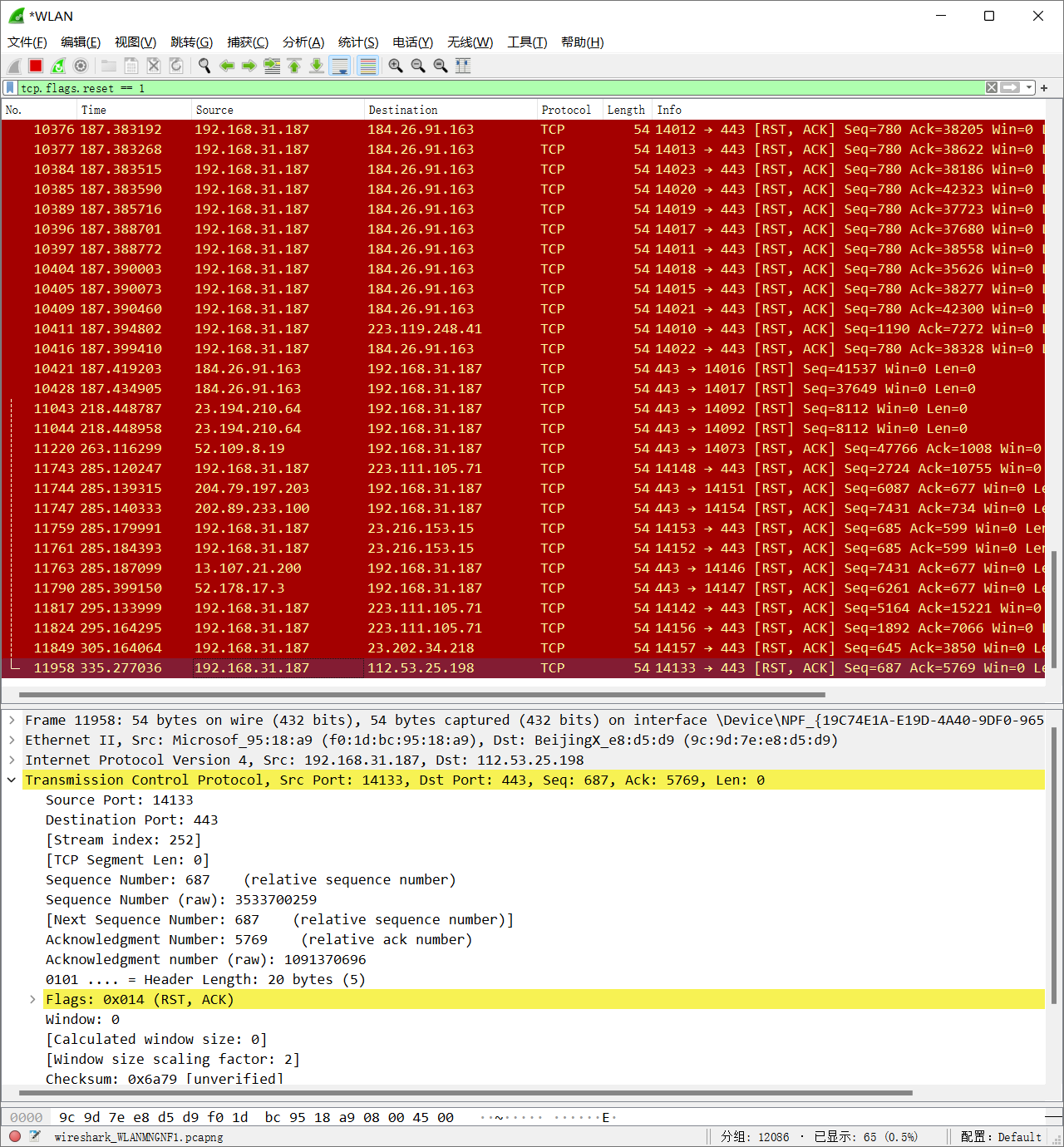
在理想的情况下，TCP连接都是正常关闭的。但在现实中的一些情况下， TCP连接会

突然断掉。例如网络的瞬时拥塞或存在潜在的攻击者等。在这些情况下，就可以使用RST

标志置位的数据包，指出连接被异常终止或拒绝连接请求。

Wireshark过滤显示RST置位数据包

tcp.flags.reset == 1



4. TCP重传

TCP重传是TCP可靠数据传输机制的核心。正是由于发送缓冲区、接收缓冲区和重传机制的使用，TCP 数据传输才变的可靠。发送端发送数据、收到接收方确认，发送指针(指下一个可以发送字节的内存地址)才会向前移动。而接收方在--段数据全部都正确接收后，才会通知发送方已经正确接收，然后把数据交付给.上层协议模块进行处理。

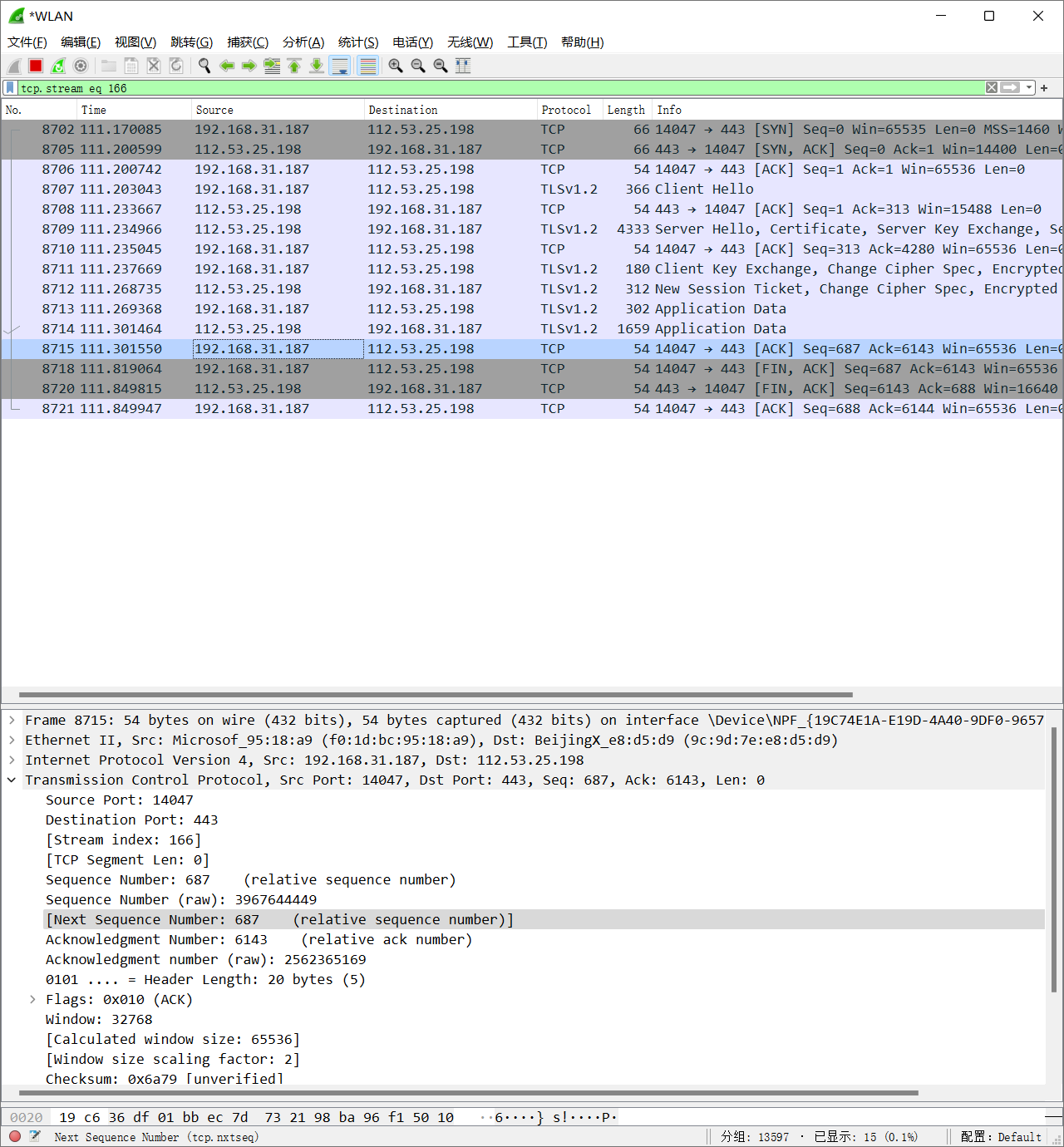
数据包的丢失有很多原因，包括网络拥塞、通信链路错误、主机错误等。但是首要的原因却是由于网络拥塞引起的超时。

操作系统的TCP模块使用估计的RTT(Round Trip Time)来确定一个 数据包是否超时。估计的RTT其实是一个变量，操作系统维护这个变量并且根据每次确认信息回来的时间不断地进行调整，以此来粗略地描述数据包在网络中传输的延时。

因为RTT的波动特别大，所以操作系统并不是直接将一个数据包真实的RTT时间和它的估计时间进行比较,而是使用另外--个值来设置超时定时器,例如使用这个估计的RTT再加上一个波动范围作为判断数据包超时的依据。若有个数据包发送了很久都没有收到接收方的确认信息，如果它的超时定时器已经触发，TCP模块就假设数据包已经丢失，然后启动重传。

Wireshark帮我们对每个数据包都进行了SEQ/ACK分析，并标注了每个数据包，特别是不正常的数据包，还会指出其可能的不正常原因。因此可以借助这个功能对重传数据包展开分析。在Wireshark数据包列表面板中，不正常的数据包通常使用黑色显示，根据这个特点可以进一步查看 Info 字段，非常容易定位重传数据包。

Wireshark 过滤显示重传数据包



Wireshark过滤显示虛假重传数据包

