

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验四 观察TCP报文段并侦听分析FTP协议**

**班　　级 软件工程2018级2班**

**姓　　名 张莹玥**

**学　　号 30320172200094**

**实验时间 2020年3月25日**

**2020 年 3 月 30 日**

# 实验目的

用Wireshark侦听并观察TCP数据段。观察其建立和撤除连接的过程，观察段ID、窗口机制和拥塞控制机制等。将该过程截图在报告中。

用Wireshark侦听并观察FTP数据，分析其用户名密码所在报文的上下文特征，再总结出提取用户名密码的有效方法。基于WinPCAP工具包制作程序，实现监听网络上的FTP数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

最终在文件上输出形如下列CSV格式的日志：

时间、源MAC、源IP、目标MAC、目标IP、登录名、口令、成功与否

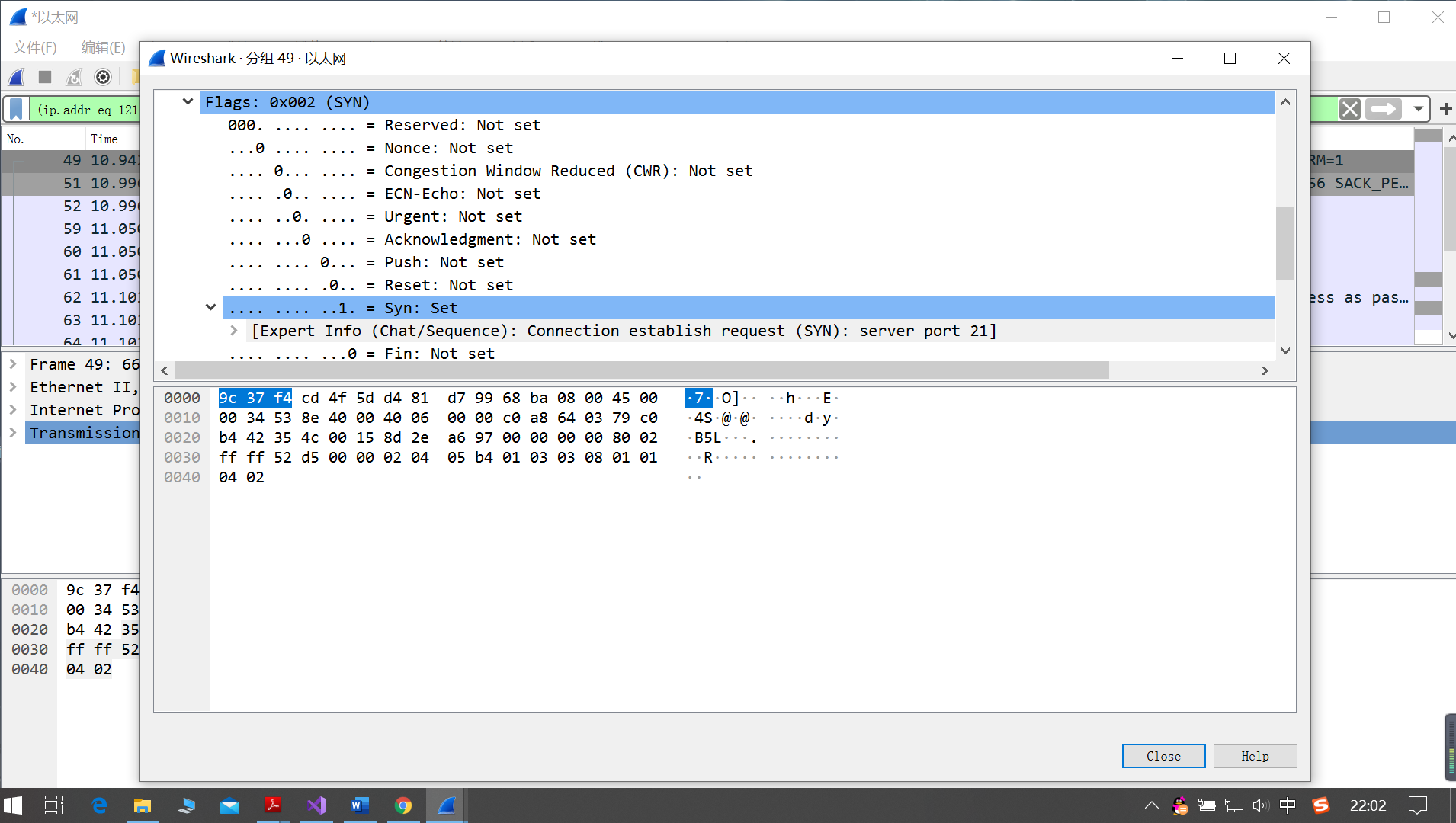
# 实验环境

Win10操作系统，C++编程

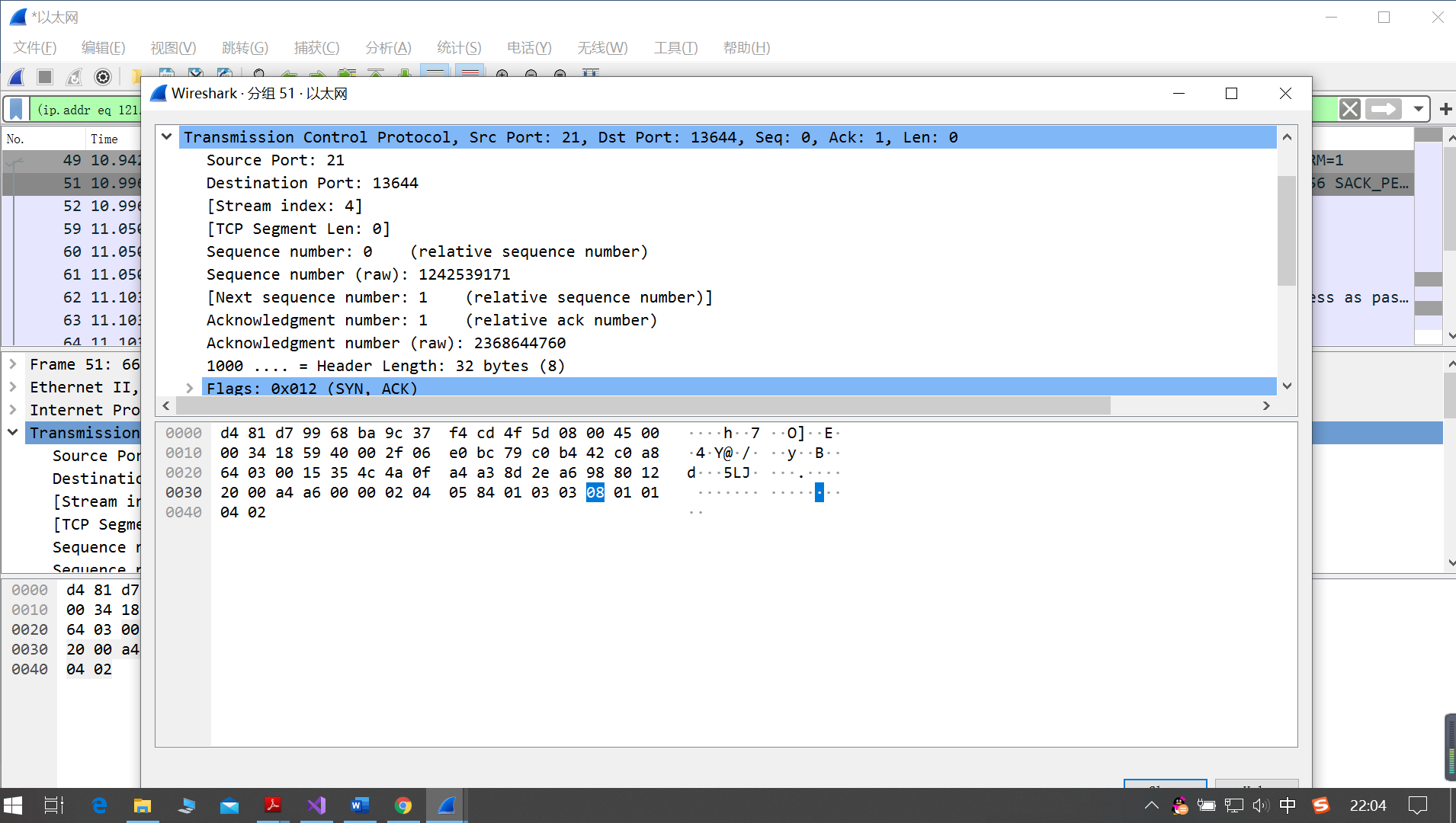
# 实验结果

1.

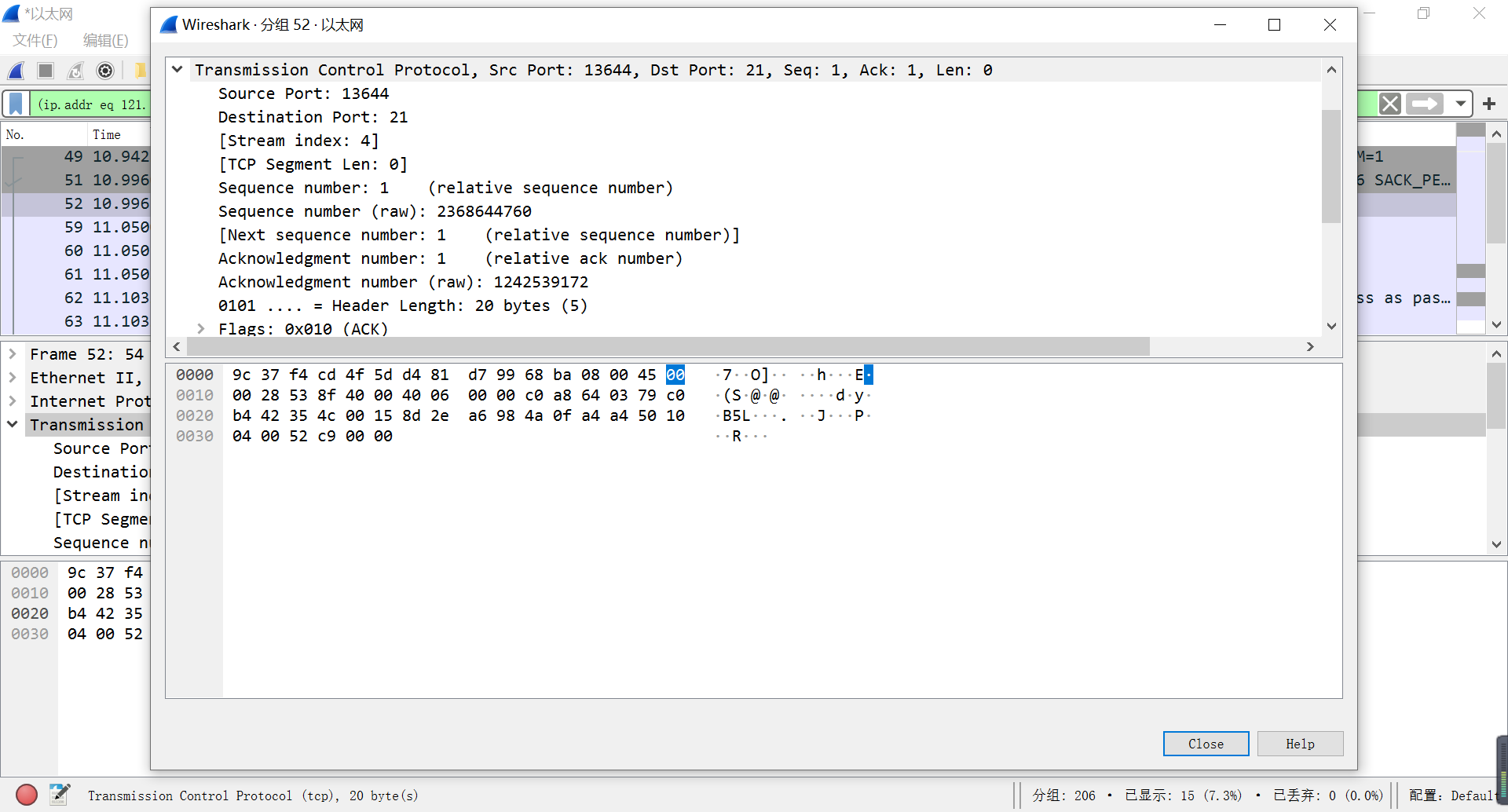
(1) 第一次握手，本机发送SYN标志，并生成随机的Seq。经观察可发现，对应的端口为Port 21



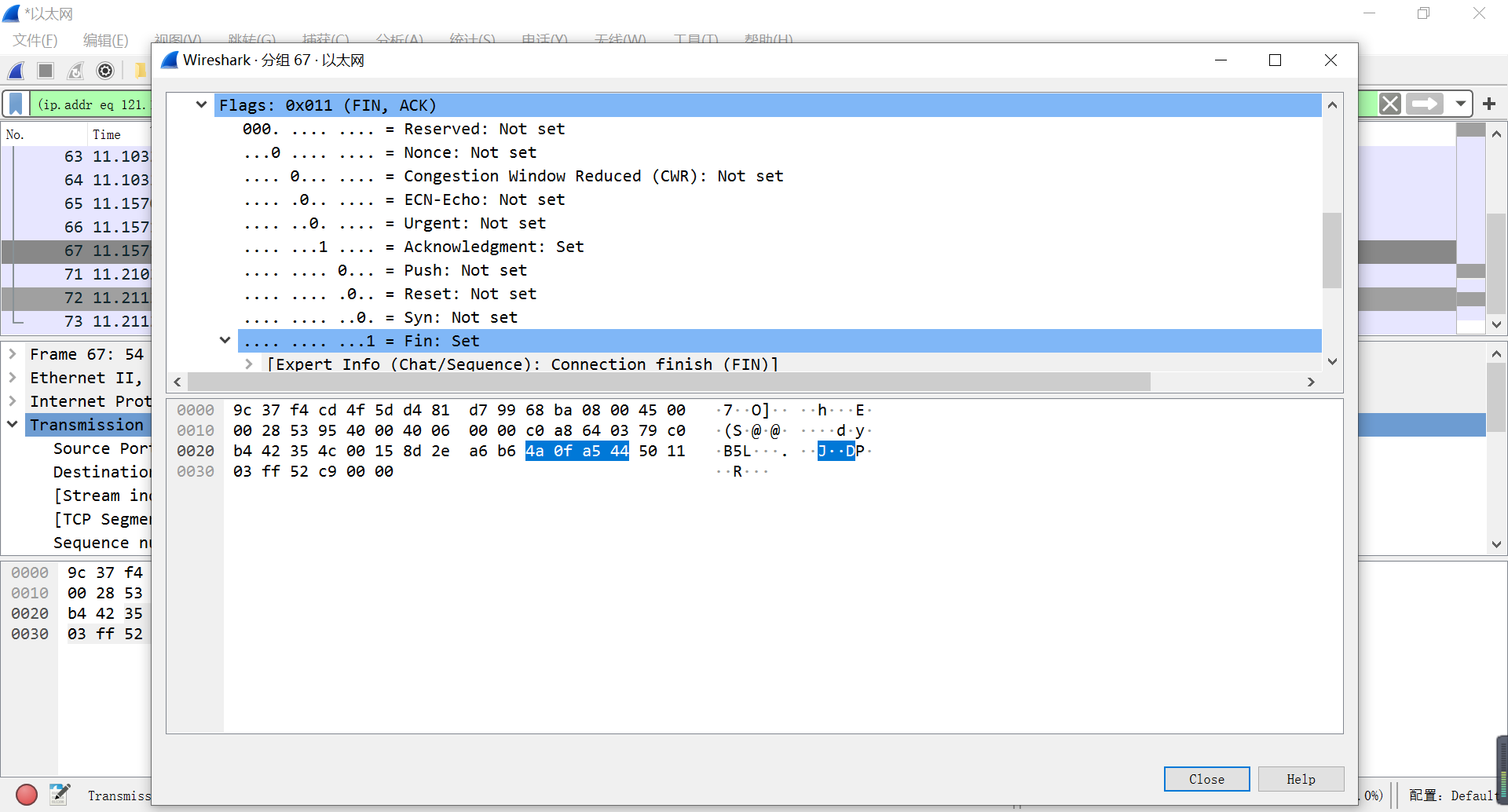
(2) 第二次握手，FTP回包，增加标志位ACK



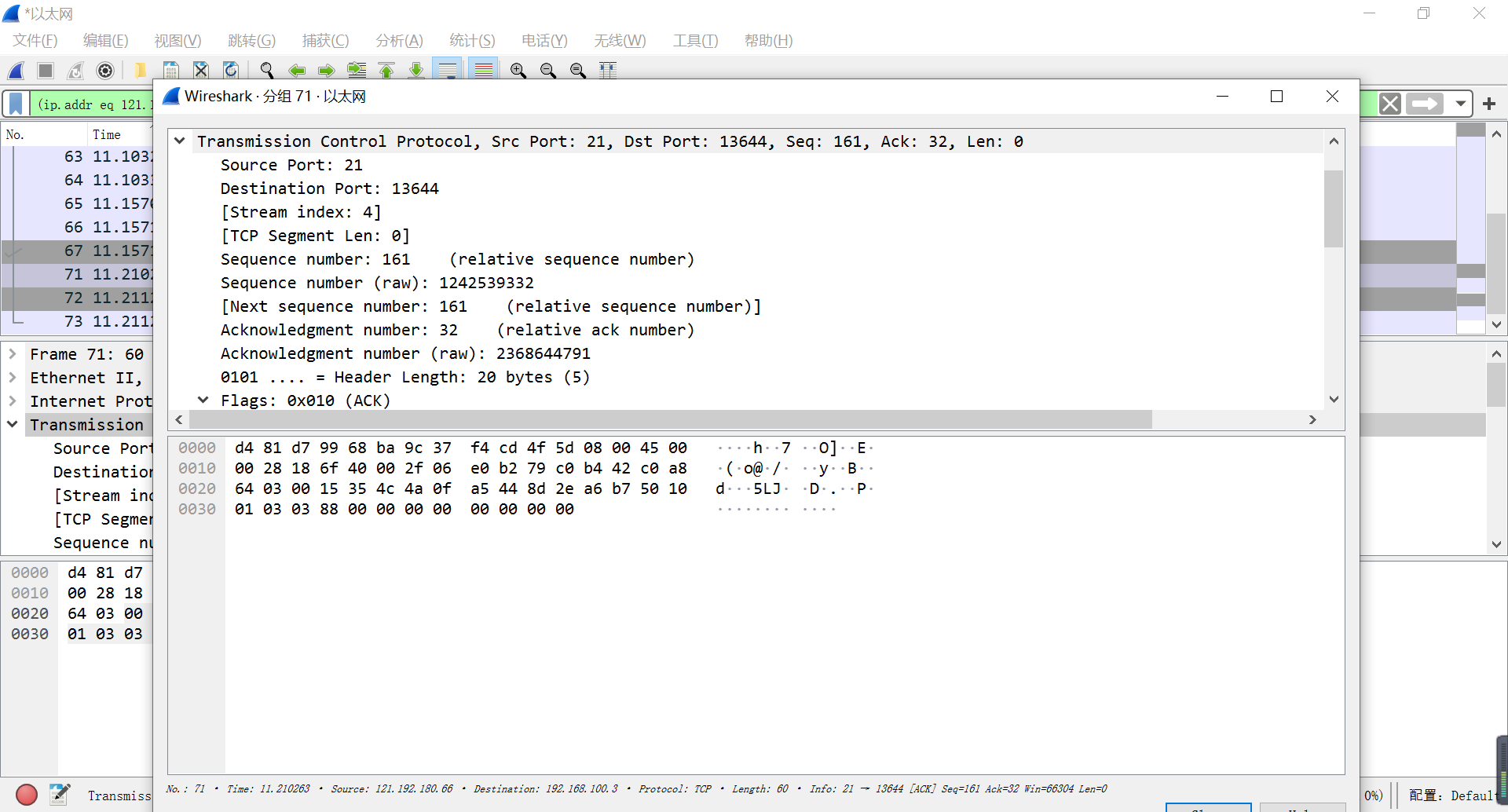
(3) 第三次握手，本机检测数据包是否正确，建立连接



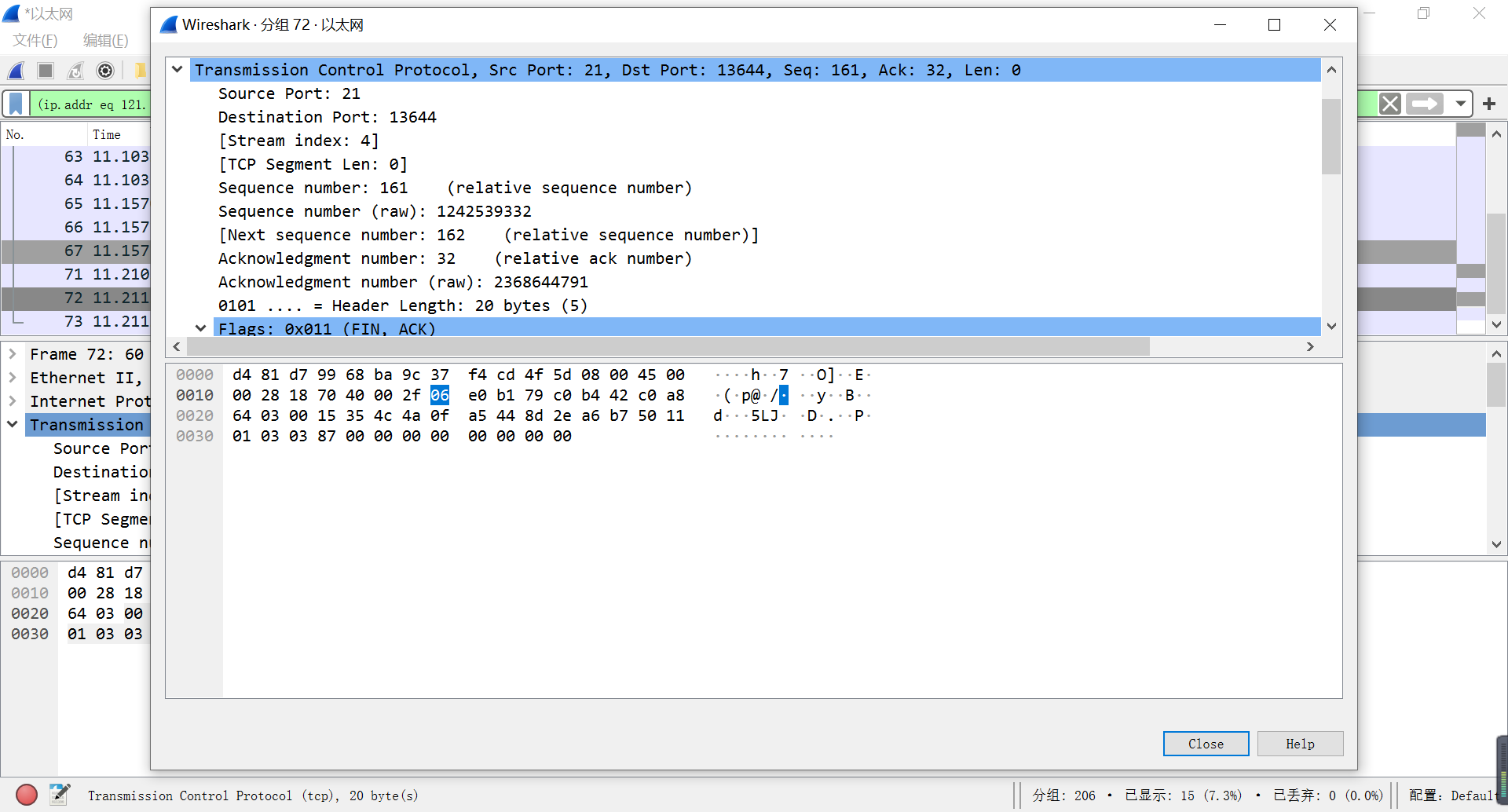
(4) 第一次挥手，本机向FTP发送信息，ACK为1，FIN置1，关闭数据传送



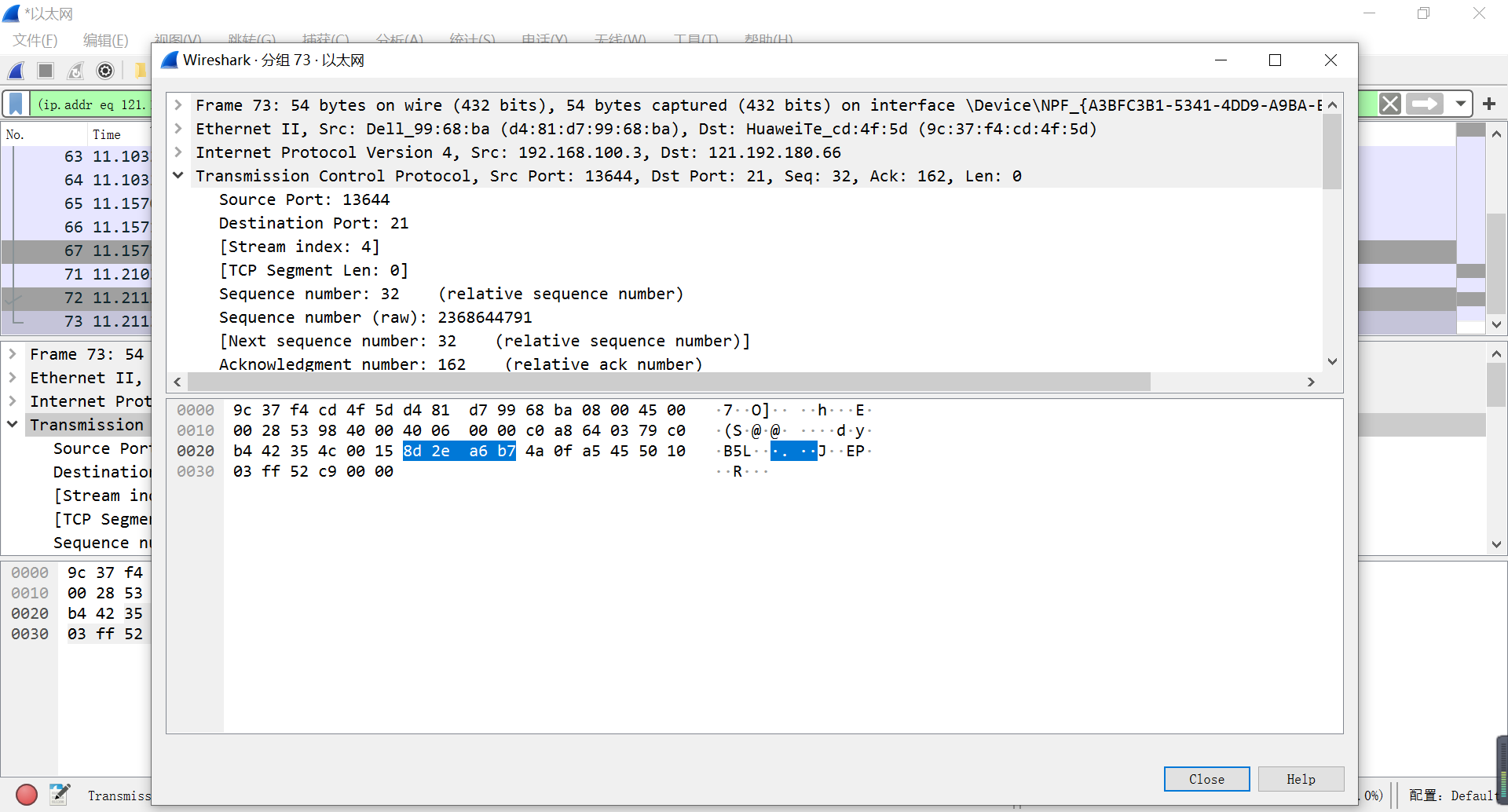
(5)第二次挥手，FTP确认信息



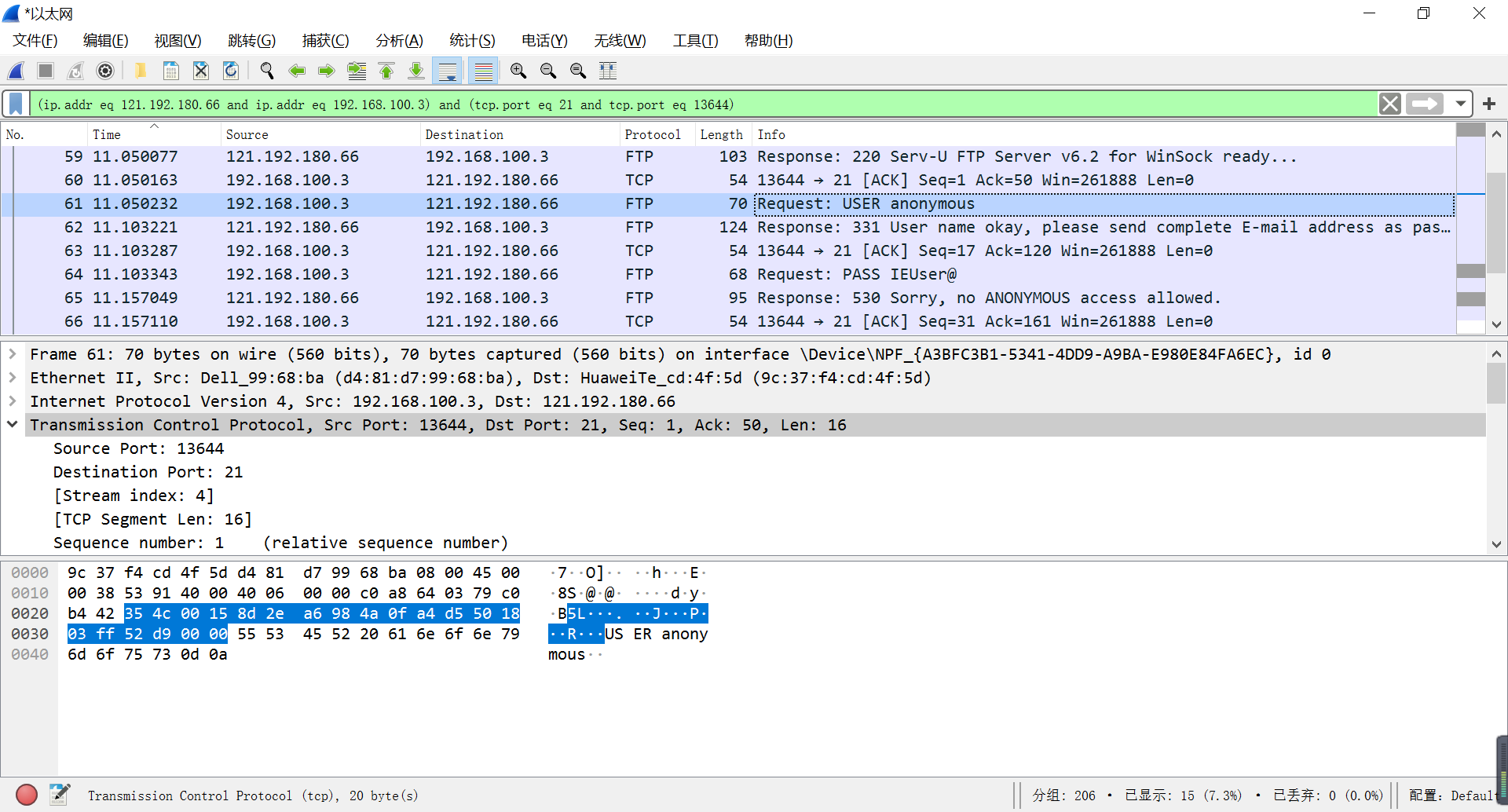
(6)第三次挥手，本机向FTP发送信息，关闭连接



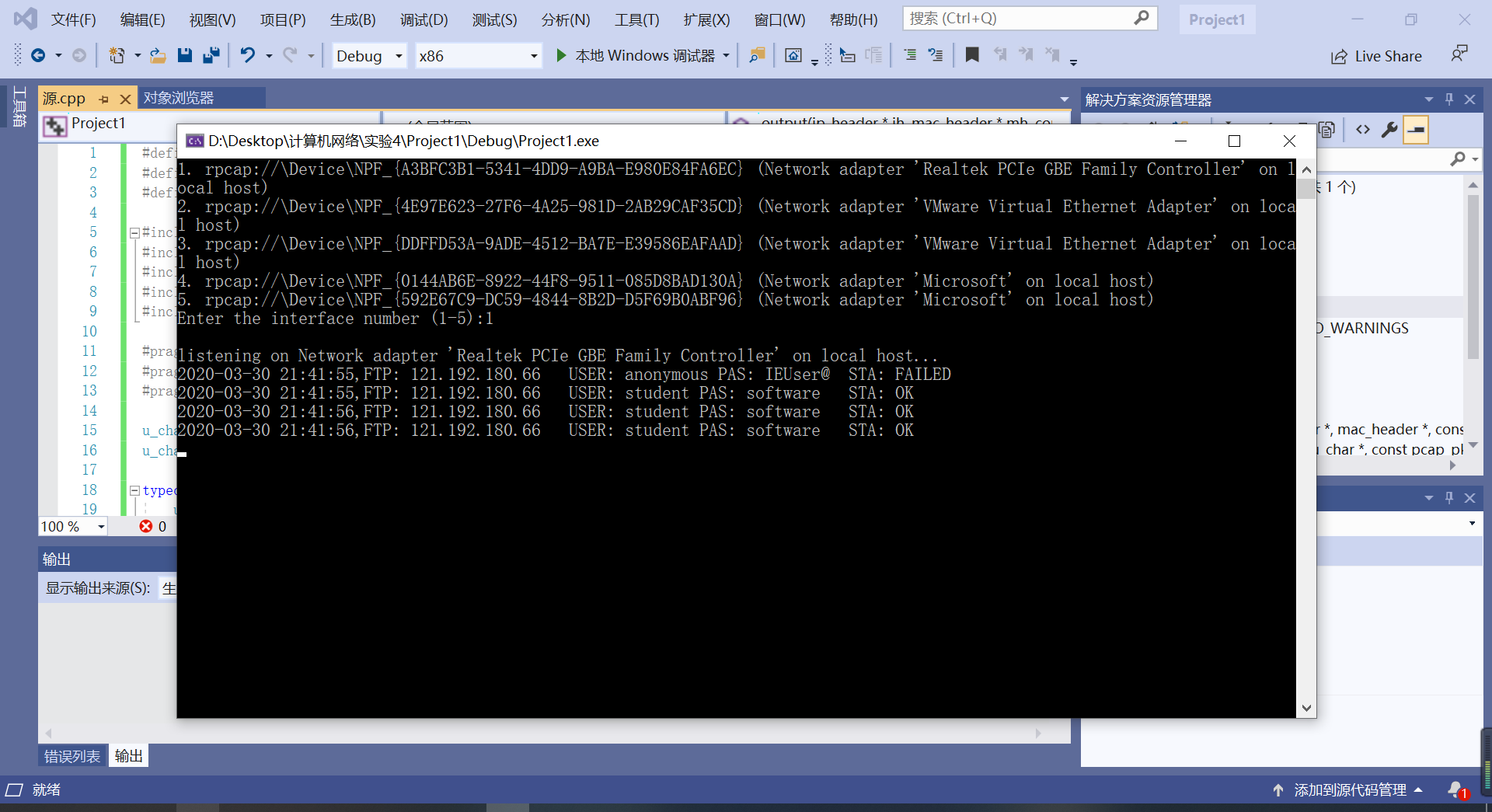
(7)第四次挥手，FTP确认信息



(8) 由观察可发现，用户名和密码分别跟在USER和PASS之后，且230表示成功登陆，530表示登陆失败



2. 编写程序，登陆学院FTP，并点击文件进行访问，结果如下图所示



# 实验总结

1. WireShark的使用过程比较顺利，成功提取了足够的关键信息，并对FTP报文的格式有了直观的认识，为编写代码提供了遍历。
2. 在编程过程中仍过度依赖示例代码，对loop函数的理解不够，完成相对困难。