

****

软 件 学 院

《计算机网络》实验报告

**题　　目 用 WinPCAP 监听并解析 FTP 命令**

**姓　　名 陈澄**

**学　　号 32420212202930**

**班　　级 软工三班**

**实验时间 2023.04.20**

**2023 年 04 月 20 日**

# 实验目的

通过捕获并解析 FTP 连接的建立于与断开过程的数据帧，达到以下目的：

熟悉并学会分析 TCP 连接的建立、断开过程；

熟悉常见的 FTP 命令，熟悉并学会分析 FTP 连接的建立、断开过程；

掌握使用代码实现解析以太网数据帧的技能，提高编码能力。

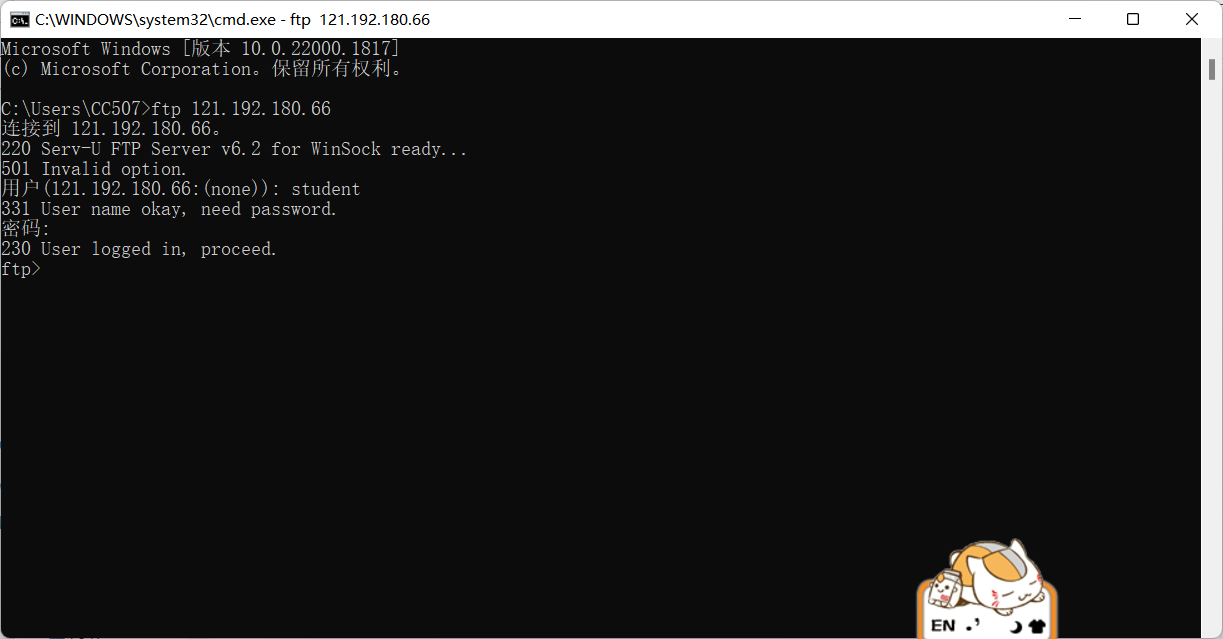
# 实验环境

操作系统：Windows10

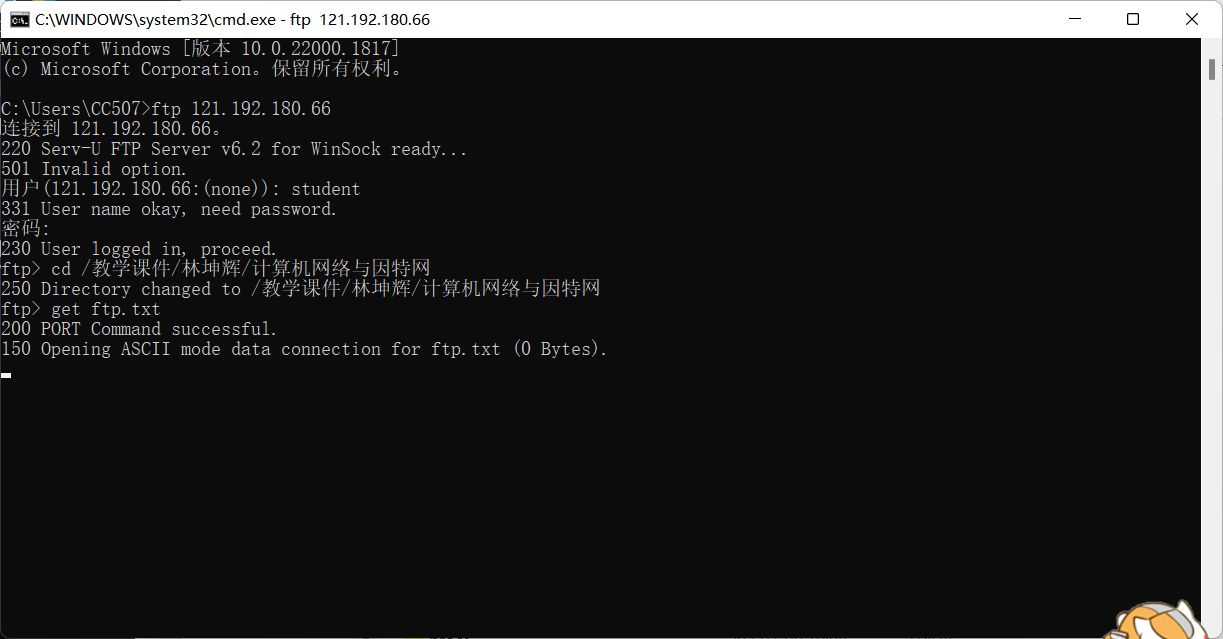
编程语言：C++

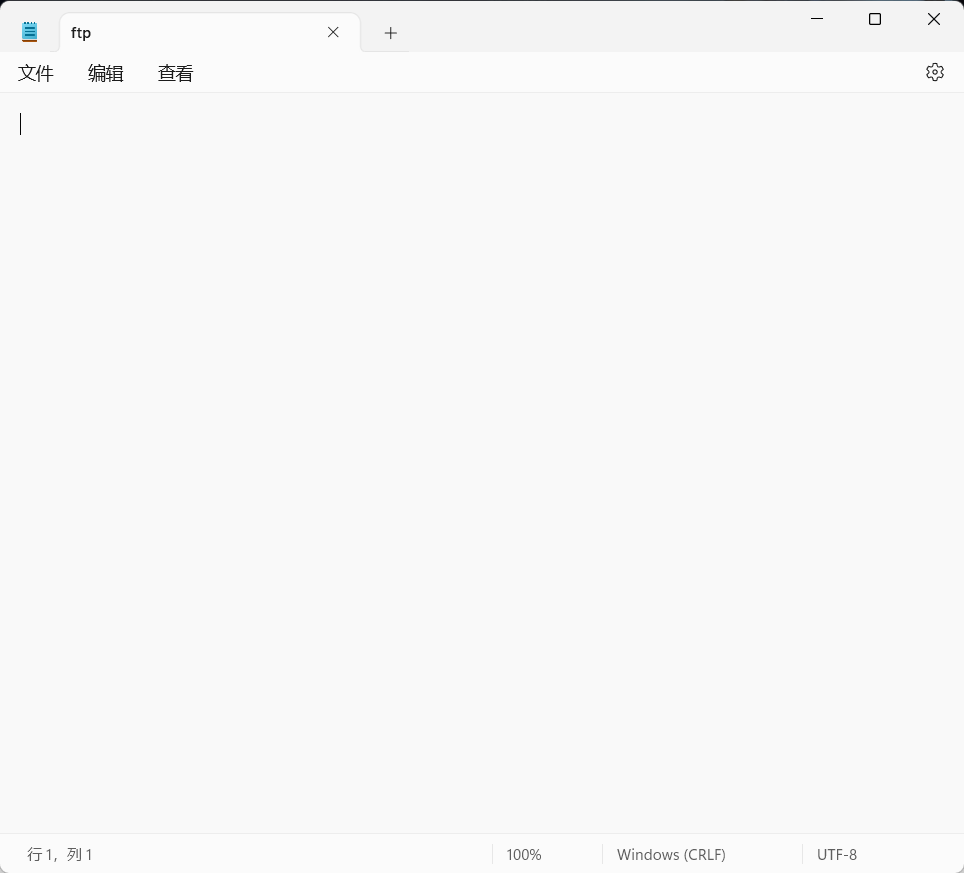
# 实验结果

1.以命令行的方式登录FTP 服务器



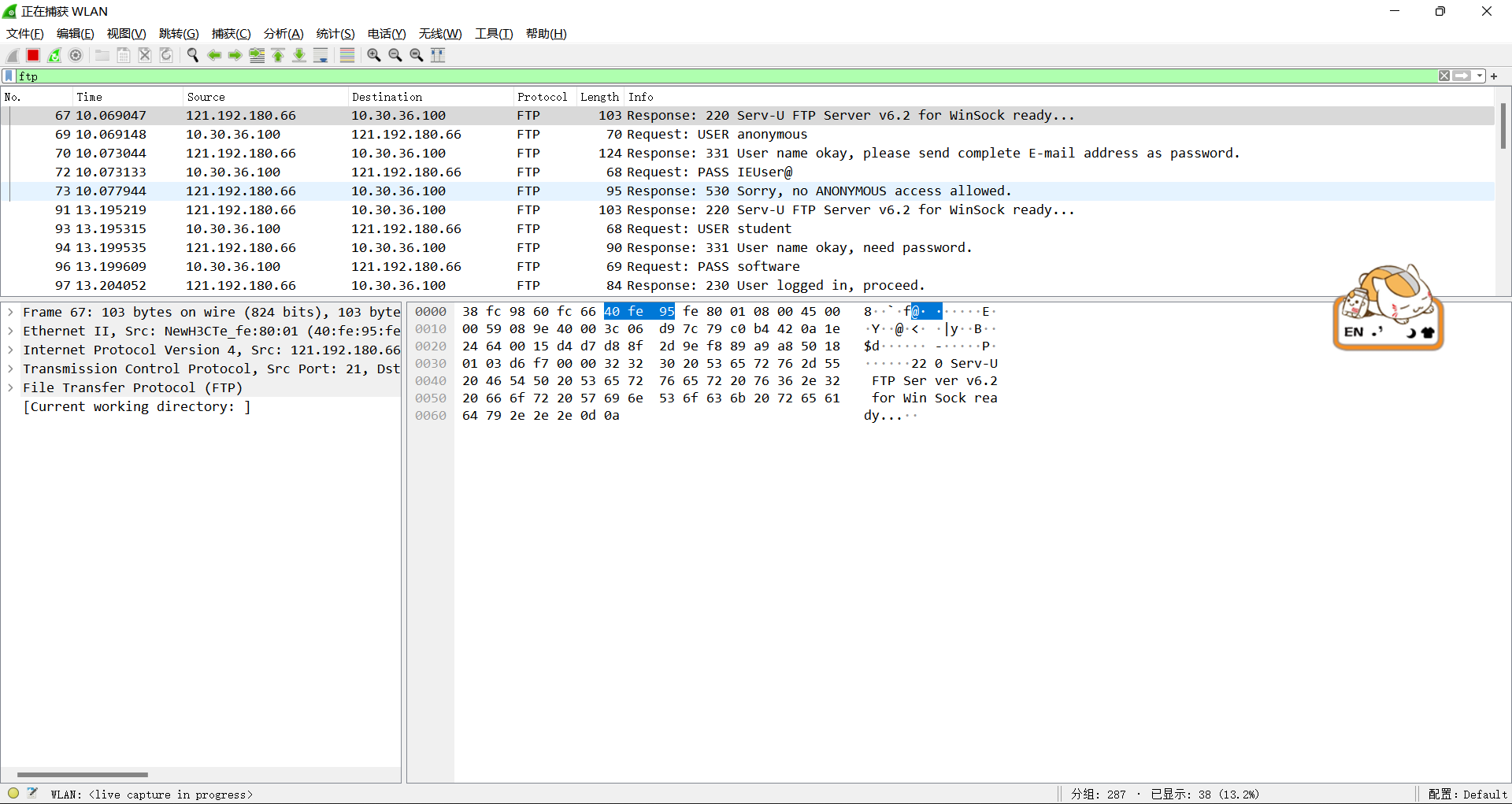
下载文件“/教学课件/林坤辉/计算机网络与因特网/ftp.txt”



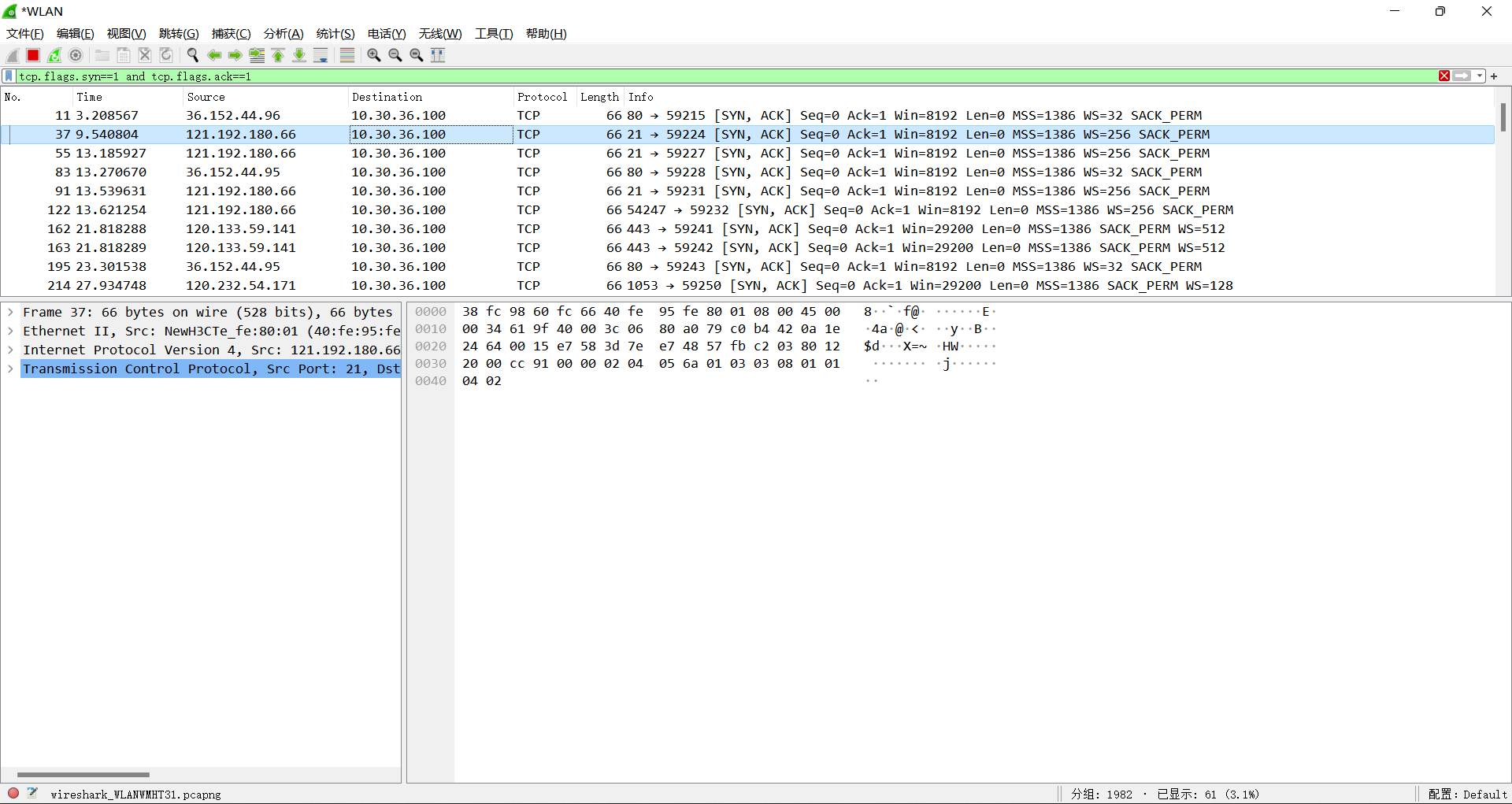


1. 使用 Wireshark 等抓包工具监听网络上的数据流，定位出TCP 连接建立、断开过程

设置过滤条件为：ftp以捕获与ftp连接与断开的相关包

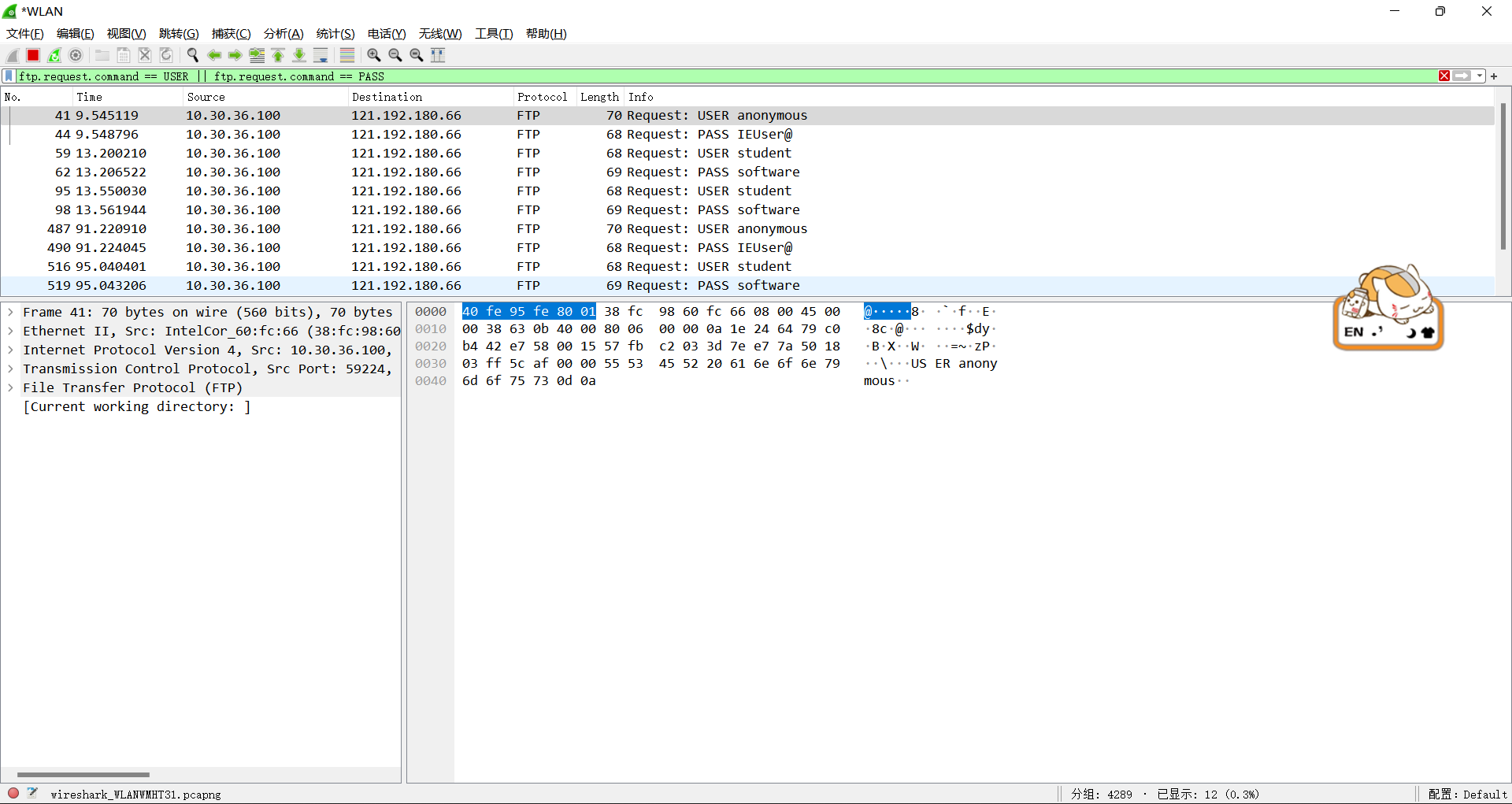


进一步设置条件为：tcp.flags.syn==1 and tcp.flags.ack==1以捕获第二次握手包

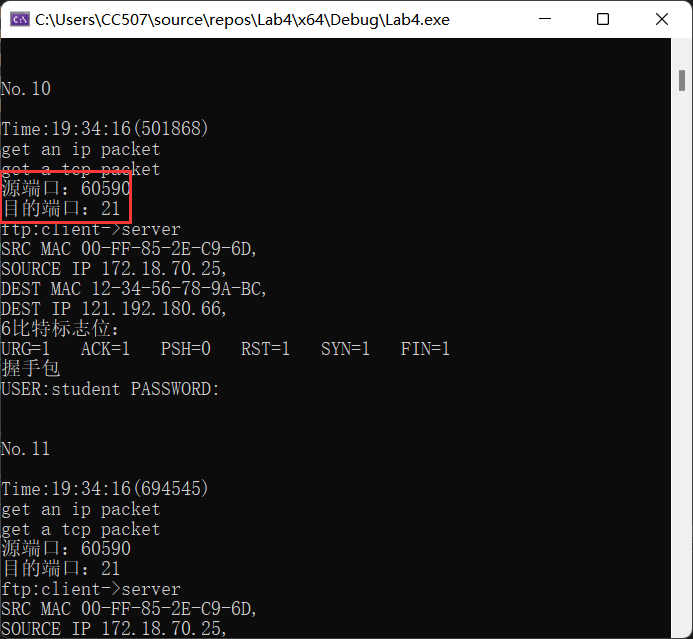


1. 使用 Wireshark 等抓包工具监听网络上的数据流，定位出FTP 连接建立过程根据要求找出软件抓取到的对应数据帧，如包含登录密码的那一帧；

在过滤器框中输入 "ftp.request.command == USER || ftp.request.command == PASS" 来筛选出包含 "USER" 或 "PASS" 命令的FTP请求数据包



1. 配置好实验环境；设置相应的过滤条件；分析 TCP/FTP 连接建立过程更加方便
2. 编写程序，捕获到 TCP 连接建立的数据帧，并能够解析出目的端口、源端口



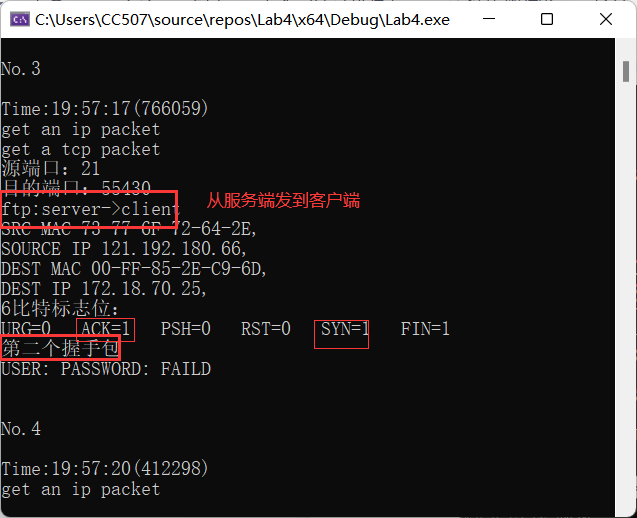
①对遇到的异常情况分析；如为什么会出现 “TCP Out-ofOrder”；这部分看实

际过程中遇到的异常；

答：当TCP数据包在传输过程中出现乱序时，就会出现 "TCP Out-of-Order" 的情况。这种情况通常发生在网络拥塞或网络质量较差的情况下。

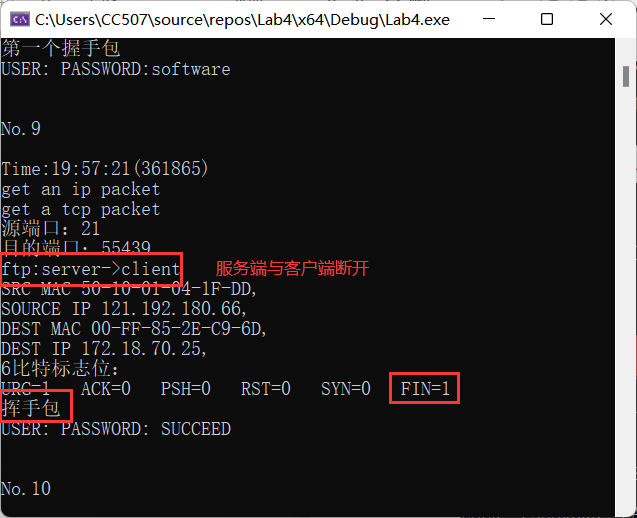
②在程序的输出能明确指出握手包的前2个

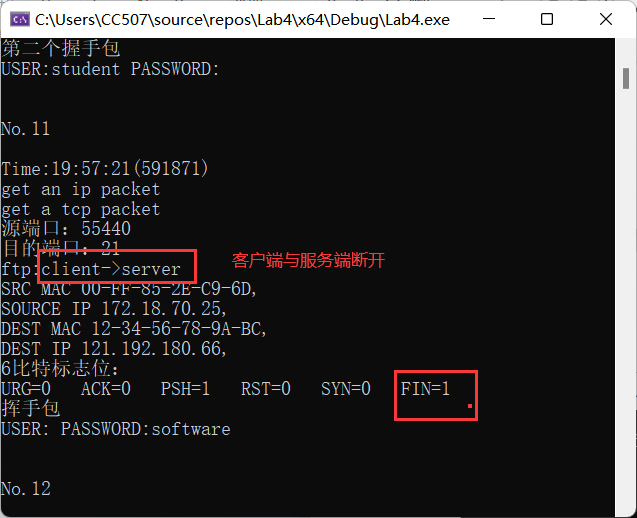




③在程序输出能明确指出客户端与 FTP 服务器、FTP 服务器与客户端断开

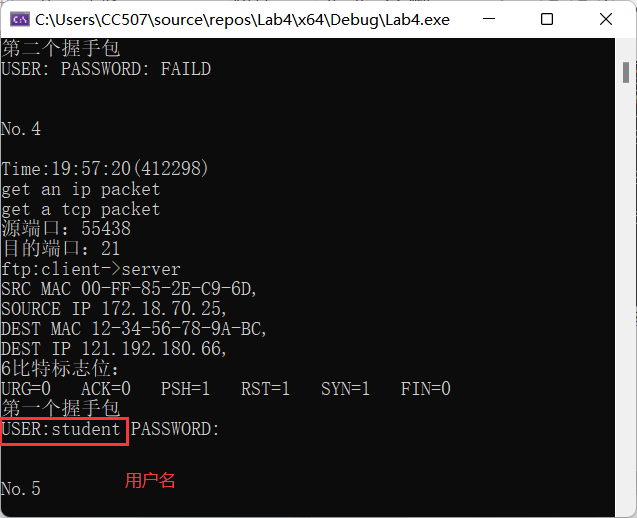
TCP 连接而发出的挥手包



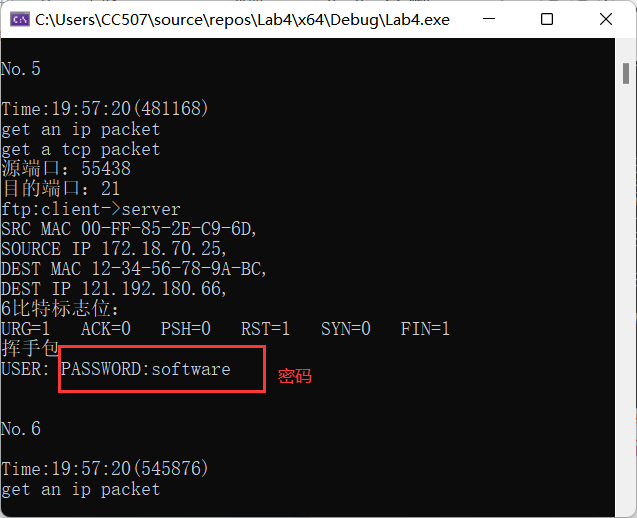


1. 编写程序，捕获到 FTP 连接建立的数据帧，并能够解析出对应的 FTP 命令

①知道常用 FTP 命令的含义：如 USER，同时打印出对应的用户名；如 PASS，同时打印出对应密码；



②对于数据连接，解析出对应的客户端、FTP 服务器使用的端口号（或者能从你的输出结果中找到判断依据）



# 实验总结

经过实验，我学会了如何使用 WinPCAP 监听并解析 FTP 命令。WinPCAP 提供了强大的 API 函数，使得我能够轻松地捕获和过滤网络数据包。同时，解析 FTP 命令也是一项相对简单的任务，只需要提取出命令和参数字符串并进行解码即可。该实验帮助我更深入地理解网络应用程序的通信原理，并为以后的网络编程工作奠定基础。