厦門大學

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 赖彦丞

学　　号 24320182203216

实验时间 2020 年 4 月 6 日

2020 年　4　月　6 日

1 实验目的

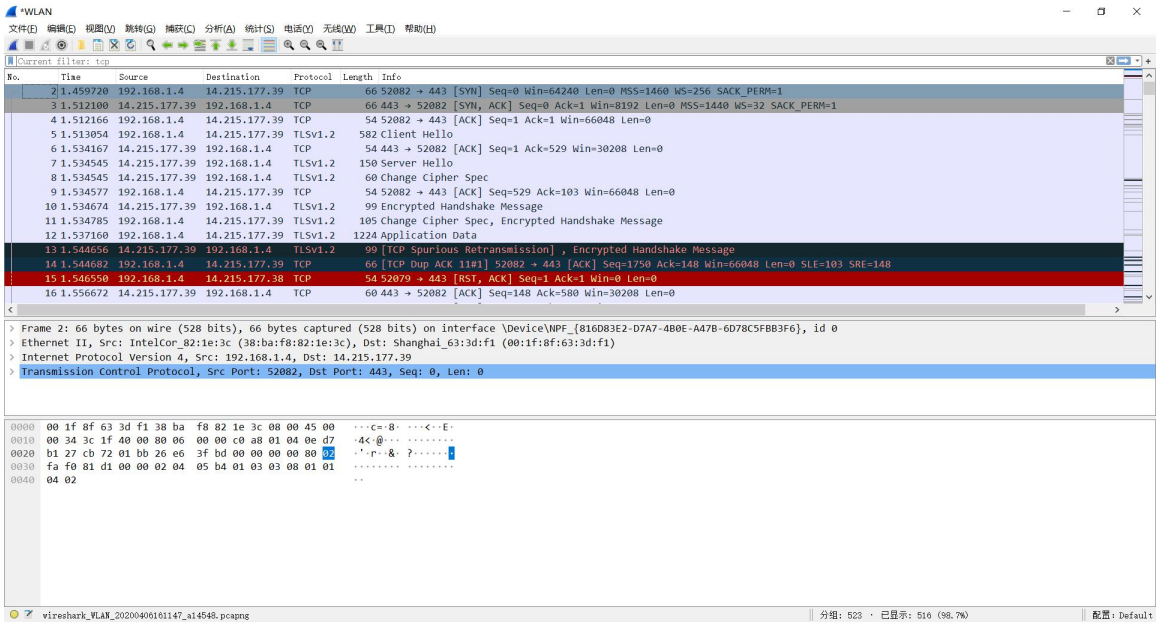
一, Wireshark 侦听并观察 TCP 数据段。观察其建立和撤除连接的过程，观察段 ID、窗口机制和拥塞控制机制等。

二,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。

2 实验环境

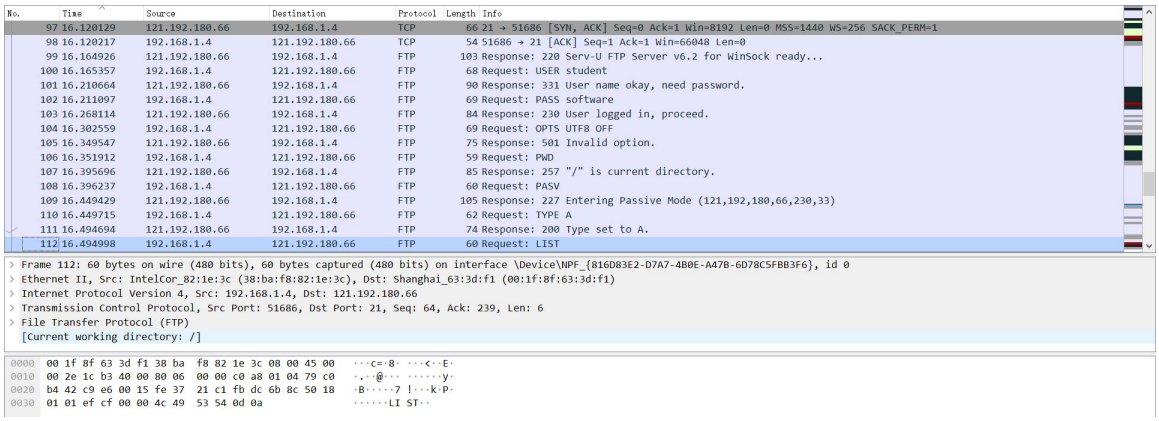
本实验在 Windows10 系统下完成,编程语言是 C++,用到的第三方库是 Pcap。

3 实验结果

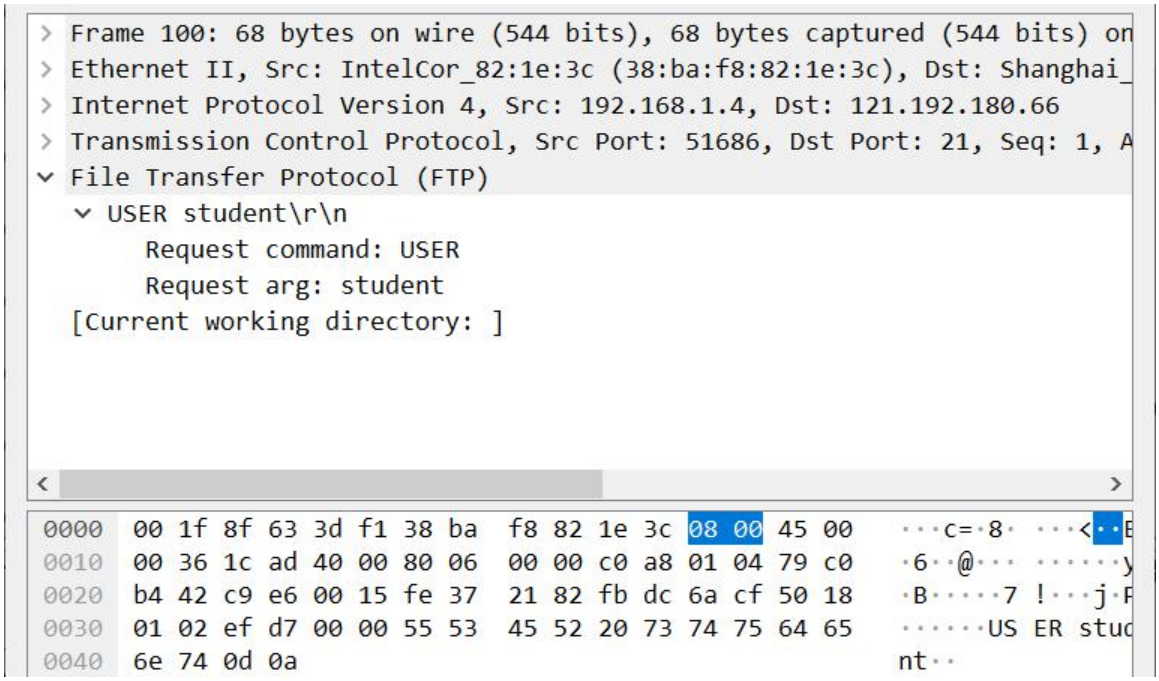


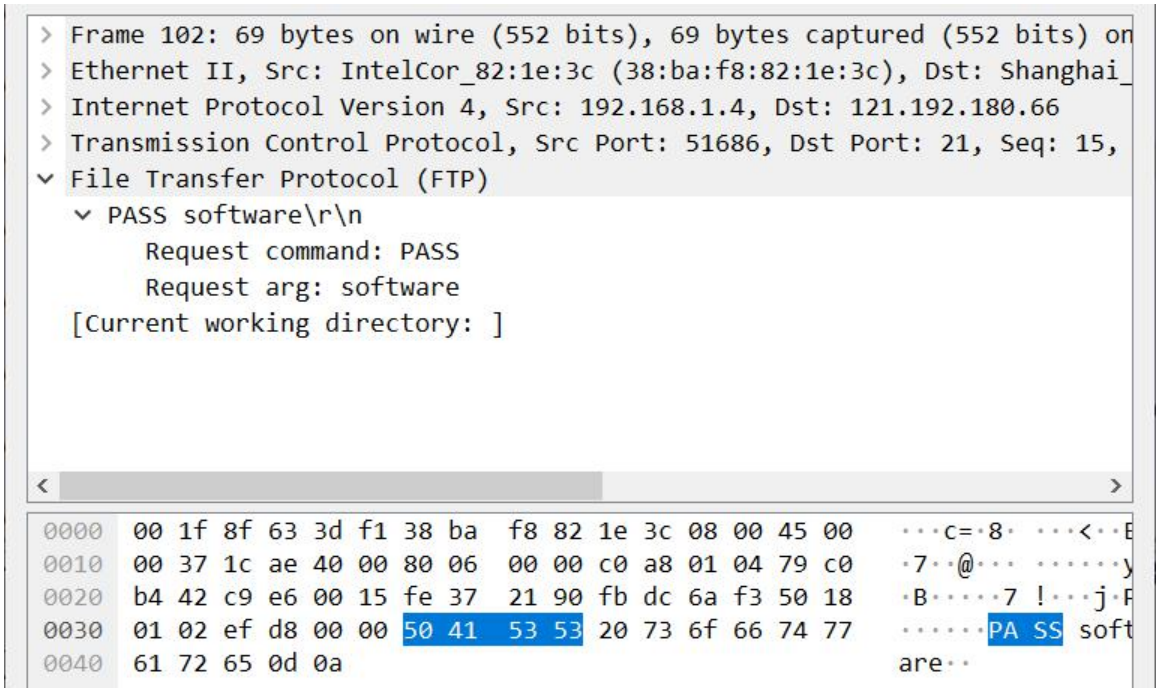
访问了域名 www.baidu.com 进行 TCP 的分析,

客户端发送 TCP，请求建立连接。服务器发了一个确认包。客户端再次发送确认包。在经过三次握手后建立连接。然后第四次挥手之后断开连接.



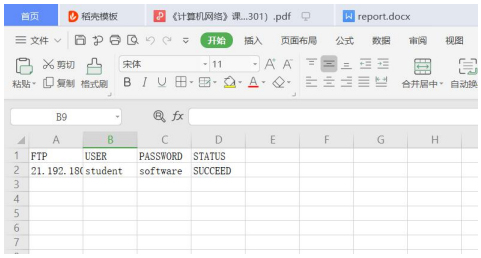
访问学院 FTP,分析 FTP 的内容.220 代表 FTP 被访问。331 表示需要密码，230 表示登陆成功。

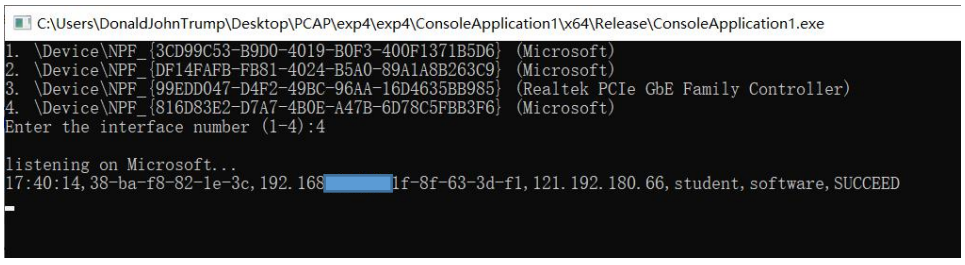




可以看到,在 Request arg 其中的内容分别表示输入的用户名和密码。

在 Winpcap 编程过程中,可以通过修改 packet_handler 函数的功能实现对 TCP 包的解析和输出.





4 实验总结

学习到了 TCP 和 FTP 报文头的一些相关知识。