

廈門大學



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 刘明成

学 号 24320182203236

实验时间 2020 年 3 月 31 日

2020 年 3 月 31 日

1 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

2015-03-14 13:05:16, 60-36-DD-7D-D5-21, 192.168.33.1, 60-36-DD-7D-D5-72, 192.168.33.2, student, software, SUCCEED

2015-03-14 13:05:16, 60-36-DD-7D-D5-21, 192.168.33.1, 60-36-DD-7D-D5-72, 192.168.33.2, student, software1, FAILED

2 实验环境

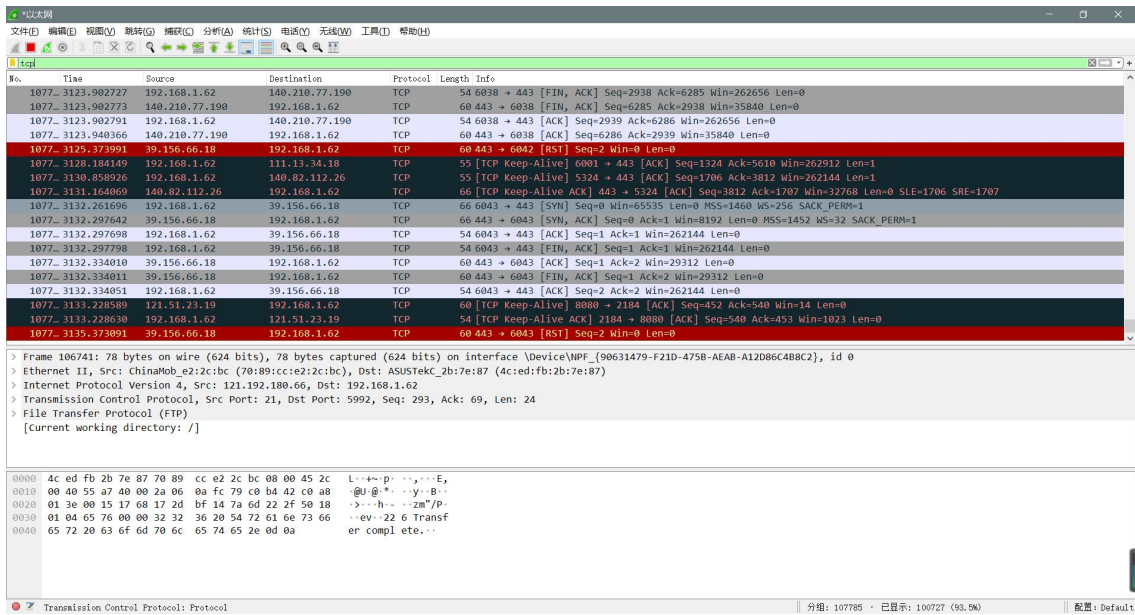
实验机：Windows10 x64 位

软件：Visual Studio 2019、Wireshark

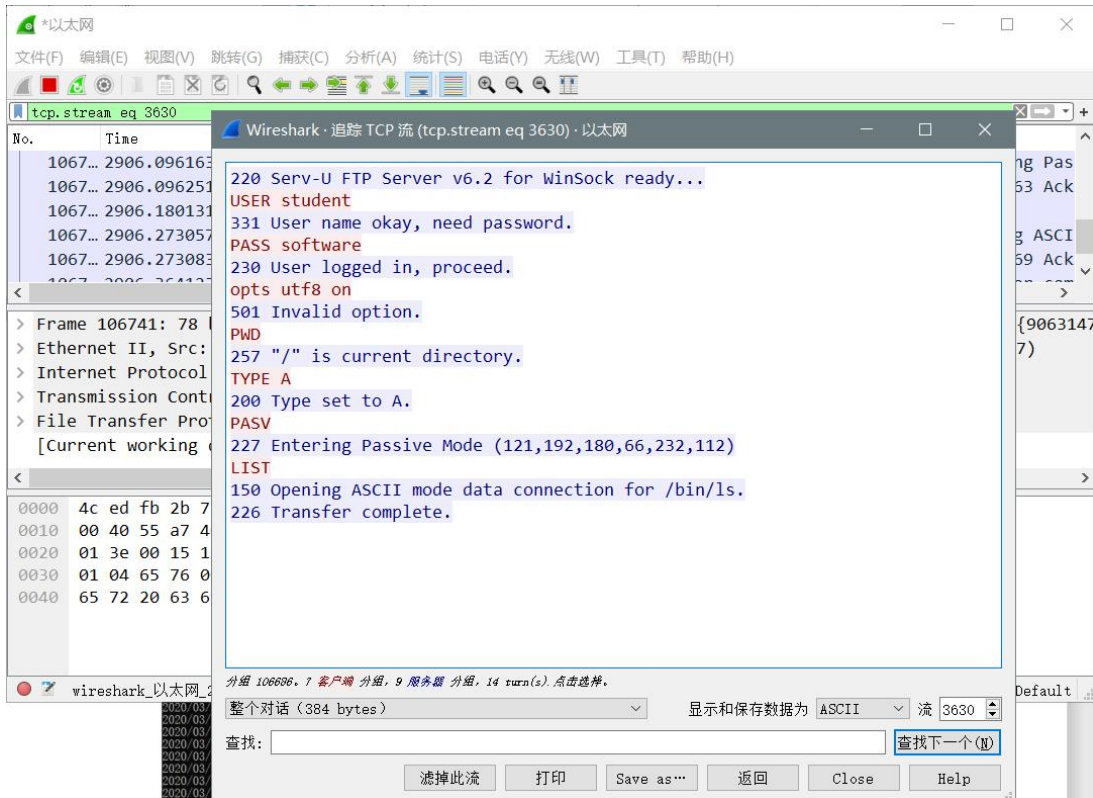
编程语言：C

3 实验结果

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

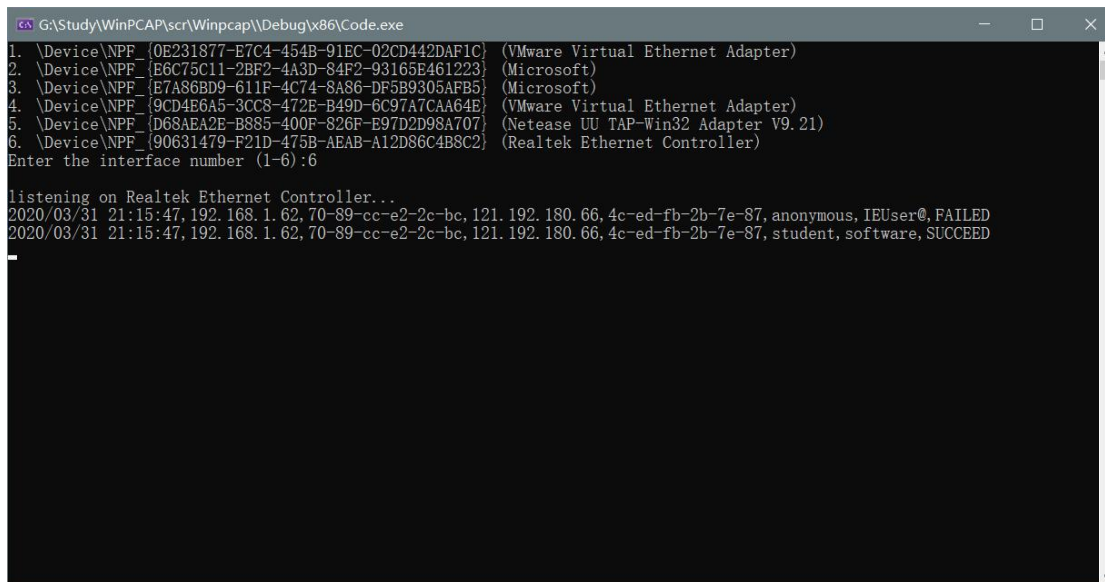


用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征



登录报文包括一个头部是 USER 的包，一个头部是 PASS 的包，以及头部是 230 代表成功（530 表示登录失败）的包。

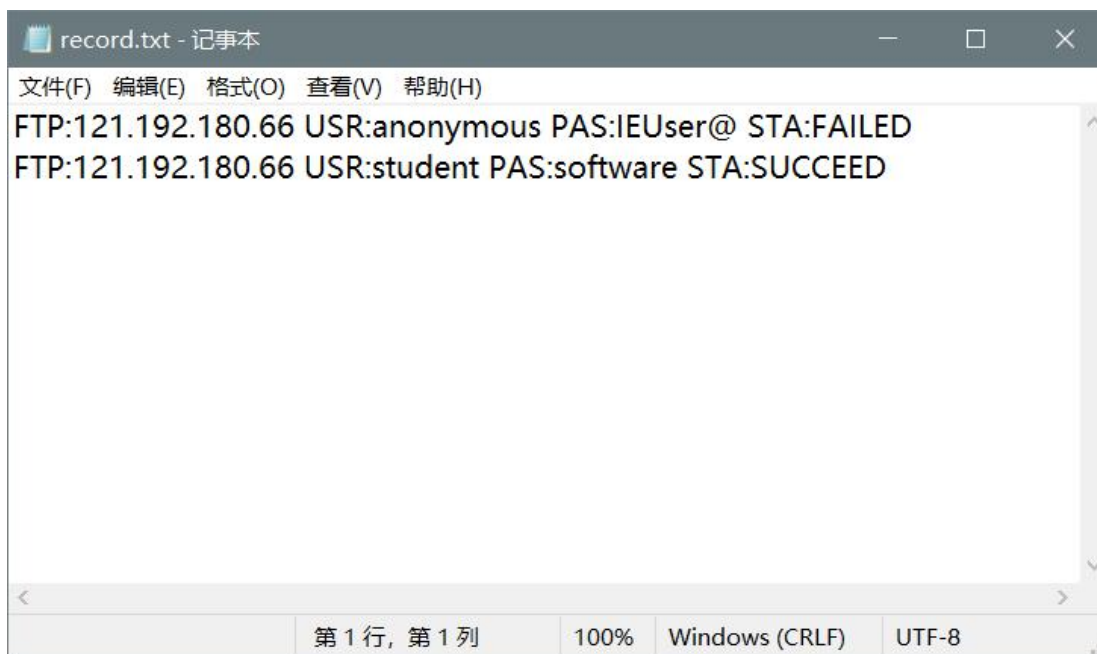
监听网络上的 FTP 数据流，解析协议内容，并作记录与统计：



```
G:\Study\WinPCAP\scr\Winpcap\Debug\x86\Code.exe
1. \Device\NPF_{0E231877-E7C4-454B-91EC-02CD442DAF1C} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{E6C75C11-2BF2-4A3D-84F2-93165E461223} (Microsoft)
3. \Device\NPF_{E7A86BD9-611F-4C74-8A86-DF5B9305AFB5} (Microsoft)
4. \Device\NPF_{9CD4E6A5-3CC8-472E-B49D-6C97A7CAA64E} (VMware Virtual Ethernet Adapter)
5. \Device\NPF_{D68AEA2E-B885-400F-S26F-E97D2D98A707} (Netease UU TAP-Win32 Adapter V9.21)
6. \Device\NPF_{90631479-F21D-475B-AEAB-A12D86C4B8C2} (Realtek Ethernet Controller)
Enter the interface number (1-6):6

listening on Realtek Ethernet Controller...
2020/03/31 21:15:47, 192.168.1.62, 70-89-cc-e2-2c-bc, 121.192.180.66, 4c-ed-fb-2b-7e-87, anonymous, IEUser@, FAILED
2020/03/31 21:15:47, 192.168.1.62, 70-89-cc-e2-2c-bc, 121.192.180.66, 4c-ed-fb-2b-7e-87, student, software, SUCCEED
```

写入文件：



```
record.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
FTP:121.192.180.66 USR:anonymous PAS:IEUser@ STA:FAILED
FTP:121.192.180.66 USR:student PAS:software STA:SUCCEED
第 1 行, 第 1 列 100% Windows (CRLF) UTF-8
```

4 实验总结

学习了利用 Wireshark 侦听并观察 TCP 与 FTP 数据段，了解了 FTP 数据用户名密码所在报文的上下文特征。