

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 陈芸衣

学 号 24320182203182

实验时间 2020 年 3 月 25 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。

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。

2 实验环境

Windows10, wirehark, VS2017

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：

追踪 tcp 流，三次握手建立连接的记录如下：（第一次握手信号 SYN: seq=0; 第二次握手信号 SYN+ACK: seq=0,ack=1;第三次握手握手信号 ACK: seq=1,ack=1）

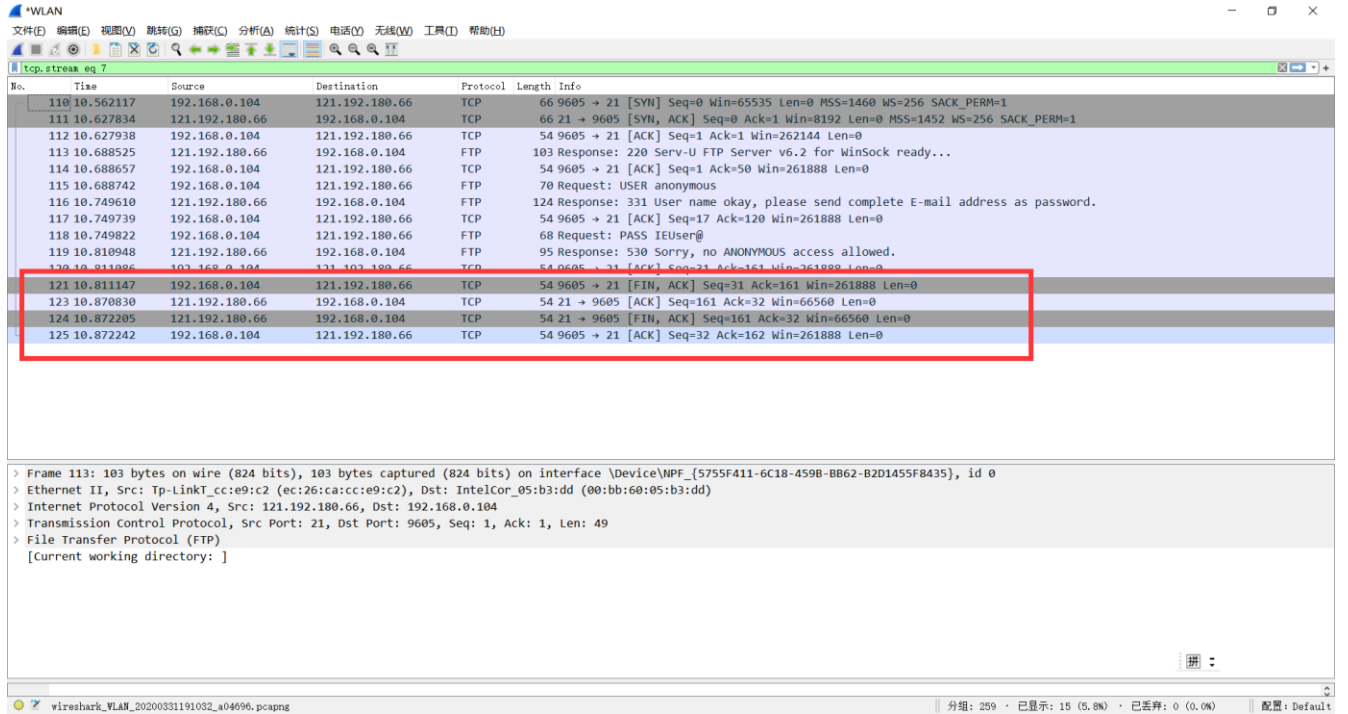
拥塞窗口: cwnd 拥塞的标志: 重传计时器超时, 连续收到 3 个冗余 ACK

Wireshark packet capture showing TCP three-way handshake and FTP data. The first three packets (110, 111, 112) are highlighted with a red circle, showing the SYN, SYN+ACK, and ACK exchange. The interface shows 'tcp.stream eq 7' and various packet details like '103 bytes on wire (824 bits)' and '103 bytes captured (824 bits)'.

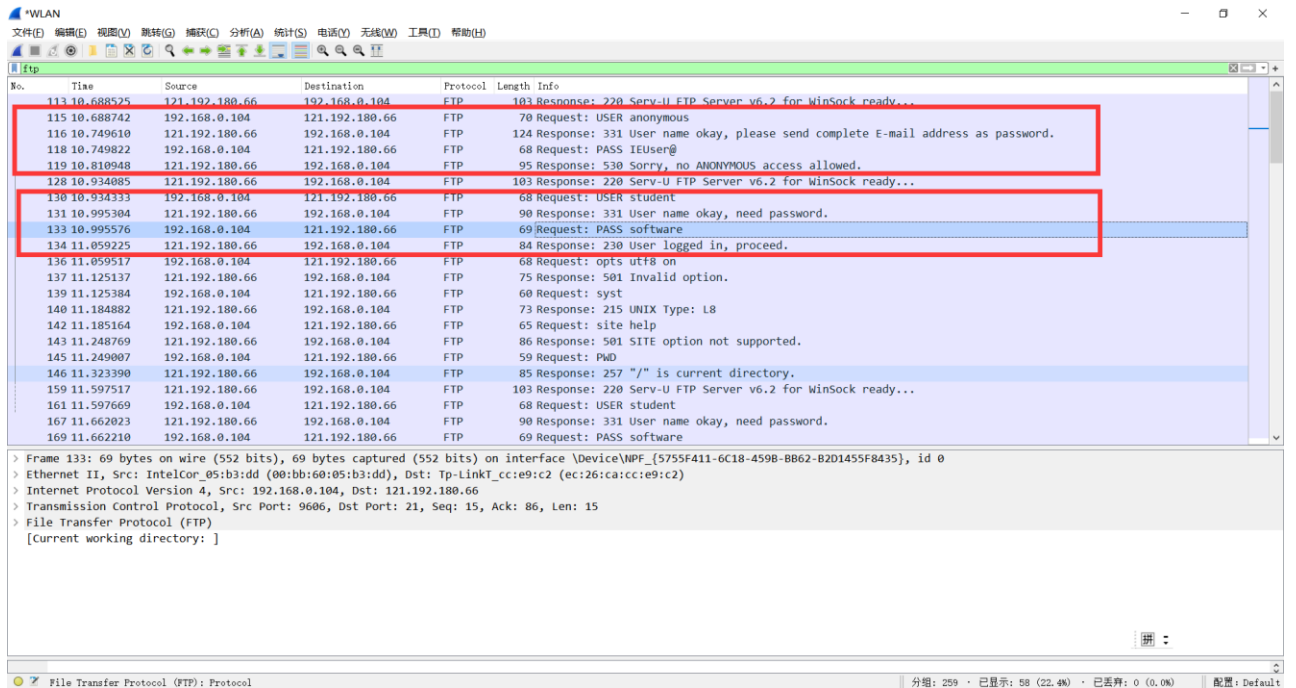
No.	Time	Source	Destination	Protocol	Length	Info
110	10.562117	192.168.0.104	121.192.180.66	TCP	66	66 9605 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
111	10.627834	121.192.180.66	192.168.0.104	TCP	66	66 21 → 9605 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452 WS=256 SACK_PERM=1
112	10.627550	192.168.0.104	121.192.180.66	TCP	54	54 9605 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=0
113	10.688525	121.192.180.66	192.168.0.104	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
114	10.688657	192.168.0.104	121.192.180.66	TCP	54	54 9605 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len=0
115	10.688742	192.168.0.104	121.192.180.66	FTP	70	Request: USER anonymous
116	10.749610	121.192.180.66	192.168.0.104	FTP	124	Response: 331 User name okay, please send complete E-mail address as password.
117	10.749739	192.168.0.104	121.192.180.66	TCP	54	54 9605 → 21 [ACK] Seq=17 Ack=120 Win=261888 Len=0
118	10.749822	192.168.0.104	121.192.180.66	FTP	68	Request: PASS IEUser@
119	10.810948	121.192.180.66	192.168.0.104	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
120	10.811086	192.168.0.104	121.192.180.66	TCP	54	54 9605 → 21 [ACK] Seq=31 Ack=161 Win=261888 Len=0
121	10.811147	192.168.0.104	121.192.180.66	TCP	54	54 9605 → 21 [FIN, ACK] Seq=31 Ack=161 Win=261888 Len=0
123	10.870830	121.192.180.66	192.168.0.104	TCP	54	54 21 → 9605 [ACK] Seq=161 Ack=32 Win=66560 Len=0
124	10.872205	121.192.180.66	192.168.0.104	TCP	54	54 21 → 9605 [FIN, ACK] Seq=161 Ack=32 Win=66560 Len=0
125	10.872242	192.168.0.104	121.192.180.66	TCP	54	54 9605 → 21 [ACK] Seq=32 Ack=162 Win=261888 Len=0

> Frame 113: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{5755F411-6C18-459B-BB62-B2D1455F8435}, id 0
> Ethernet II, Src: Tp-LinkT_cc:e9:c2 (ec:26:ca:cc:e9:c2), Dst: IntelCor_05:b3:dd (00:bb:60:05:b3:dd)
> Internet Protocol Version 4, Src: 121.192.180.66, Dst: 192.168.0.104
> Transmission Control Protocol, Src Port: 21, Dst Port: 9605, Seq: 1, Ack: 1, Len: 49
> File Transfer Protocol (FTP)
[Current working directory:]

四次挥手如下[FIN,ACK]、[ACK]、[FIN,ACK]、[ACK]信号：

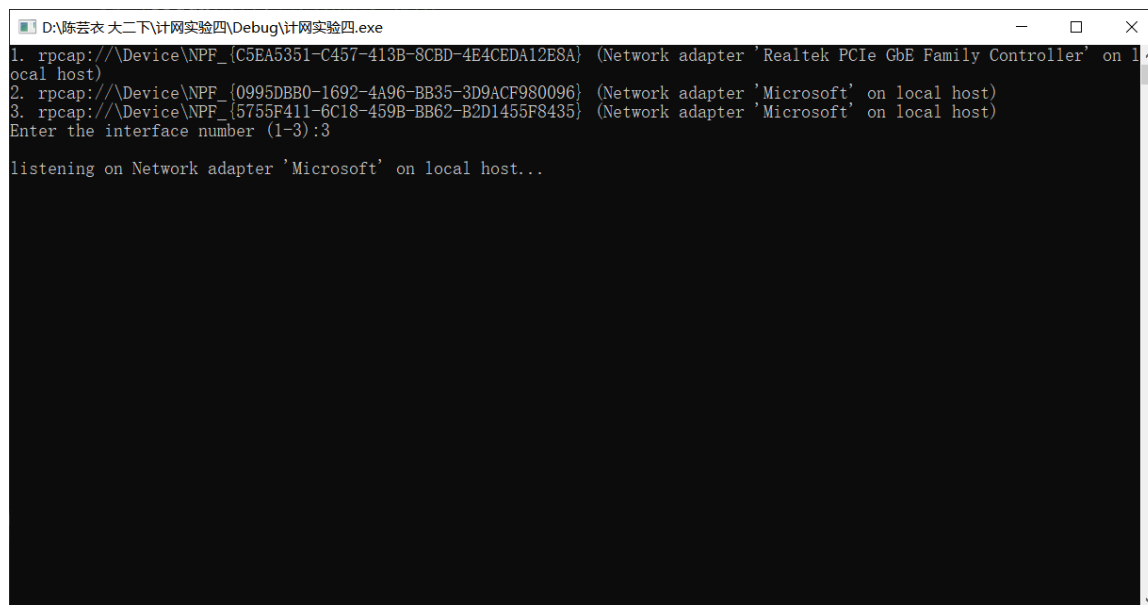


用 Wireshark 侦听并观察 FTP 数据（过滤器过滤 得到 ftp 数据）：登录名以“USER”开头，口令以“PASS”开头，可提取用户名和密码。登录成功以“230”开头，登录失败以“530”开头，以此判断登录是否成功。

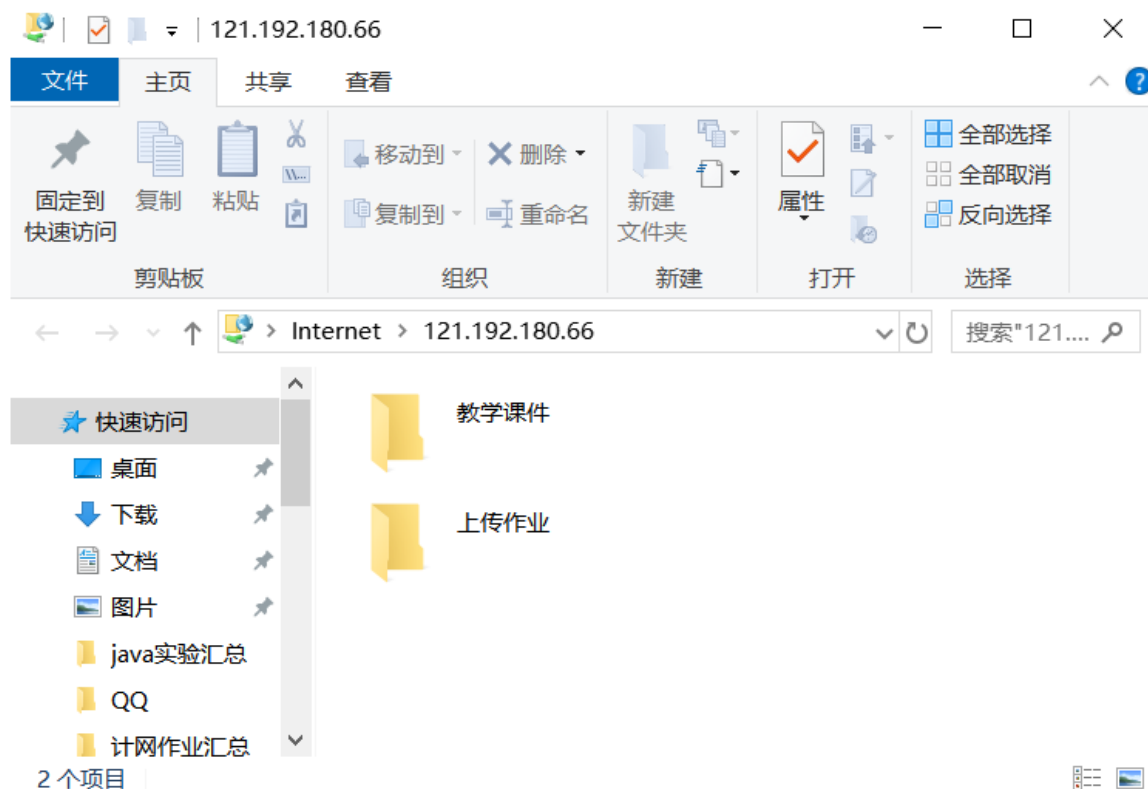


基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流：

运行程序，选择接口：



登录 FTP:



监听 FTP 数据流:

```
D:\陈芸衣 大二下\计网实验四\Debug\计网实验四.exe
1. rpcap://\Device\NPF_{C5EA5351-C457-413B-8CBD-4E4CEDA12E8A} (Network adapter 'Realtek PCIe GbE Family Controller' on local host)
2. rpcap://\Device\NPF_{0995DBB0-1692-4A96-BB35-3D9ACF980096} (Network adapter 'Microsoft' on local host)
3. rpcap://\Device\NPF_{5755F411-6C18-459B-BB62-B2D1455F8435} (Network adapter 'Microsoft' on local host)
Enter the interface number (1-3):3

listening on Network adapter 'Microsoft' on local host...
2020-03-31 20:34:09,00-BB-60-05-B3-DD,192.168.0.104,EC-26-CA-CC-E9-C2,121.192.180.66,anonymous,IEUser@,FAILED
2020-03-31 20:34:10,00-BB-60-05-B3-DD,192.168.0.104,EC-26-CA-CC-E9-C2,121.192.180.66,student,software,SUCCEED
2020-03-31 20:34:10,EC-26-CA-CC-E9-C2,121.192.180.66,00-BB-60-05-B3-DD,192.168.0.104,student,software,SUCCEED
2020-03-31 20:34:10,00-BB-60-05-B3-DD,192.168.0.104,EC-26-CA-CC-E9-C2,121.192.180.66,student,software,SUCCEED
```

Out.csv:

```
out1.csv - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2020-03-31 20:34:09,00-BB-60-05-B3-DD,192.168.0.104,EC-26-CA-CC-E9-C2,121.192.180.66,,IEUser@,FAILED
2020-03-31 20:34:10,00-BB-60-05-B3-DD,192.168.0.104,EC-26-CA-CC-E9-C2,121.192.180.66,,software,SUCCEED
2020-03-31 20:34:10,EC-26-CA-CC-E9-C2,121.192.180.66,00-BB-60-05-B3-DD,192.168.0.104,,software,SUCCEED
2020-03-31 20:34:10,00-BB-60-05-B3-DD,192.168.0.104,EC-26-CA-CC-E9-C2,121.192.180.66,,software,SUCCEED
```

以“FTP USER PAS STA”格式输出:

```
out.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:FALED
FTP:121.192.180.66 USR:student PAS:software STA:OK
FTP:192.168.0.104 USR:student PAS:software STA:OK
FTP:121.192.180.66 USR:student PAS:software STA:OK
```

4 实验总结

通过本次实验对 TCP 数据段有了更直观深刻的理解，学会在 wireshark 中用过滤器过滤数据，分析其建立连接的三次握手和撤销连接的四次挥手信号。学会用 wireshark 侦听并观察 ftp 数据，提取用户名、密码，观察登录成功情况。编写程序实现了监听网络上的 FTP 数据流。