

# 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 1 班

姓    名 罗贤甫

学    号 24320182203245

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。

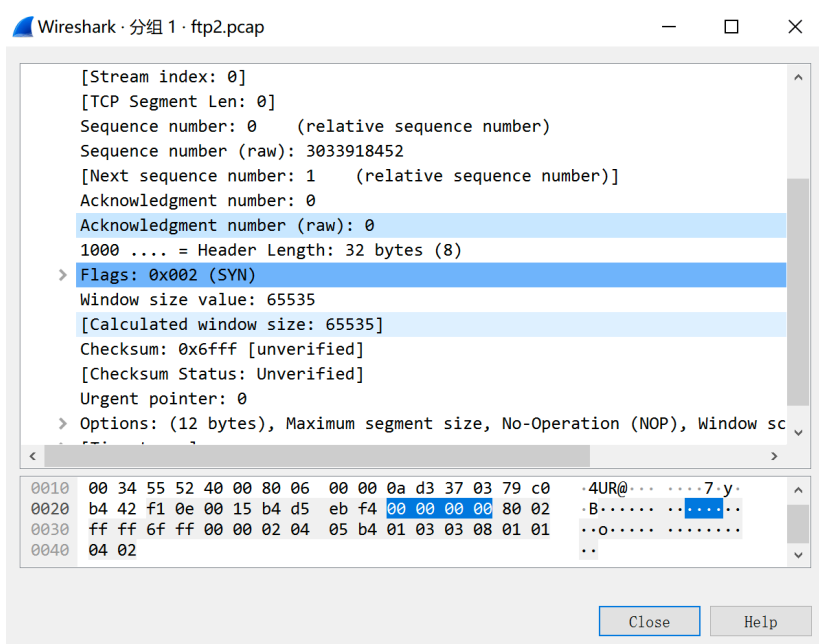
用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征，再总结出提取用户名密码的有效方法。基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

## 2 实验环境

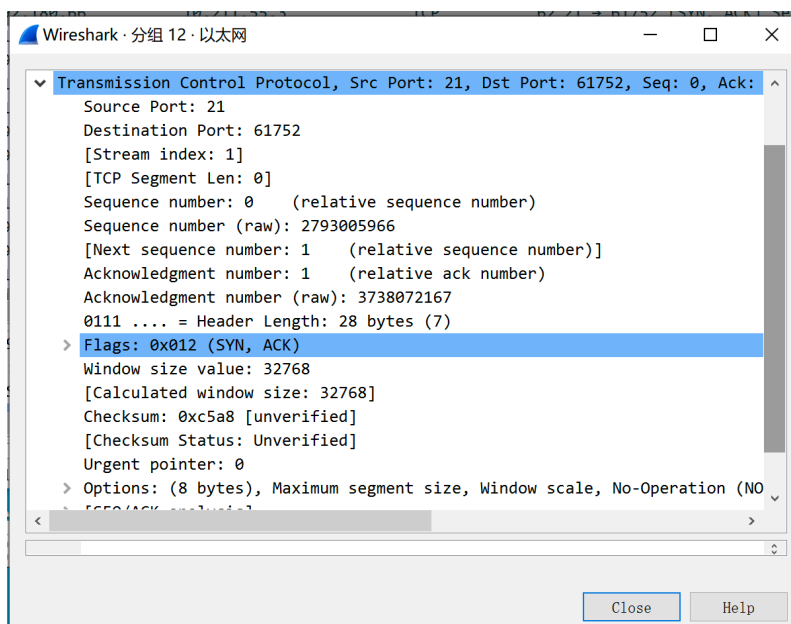
Win10 系统，Visual Studio 2019，WireShark 软件，C 语言

## 3 实验结果

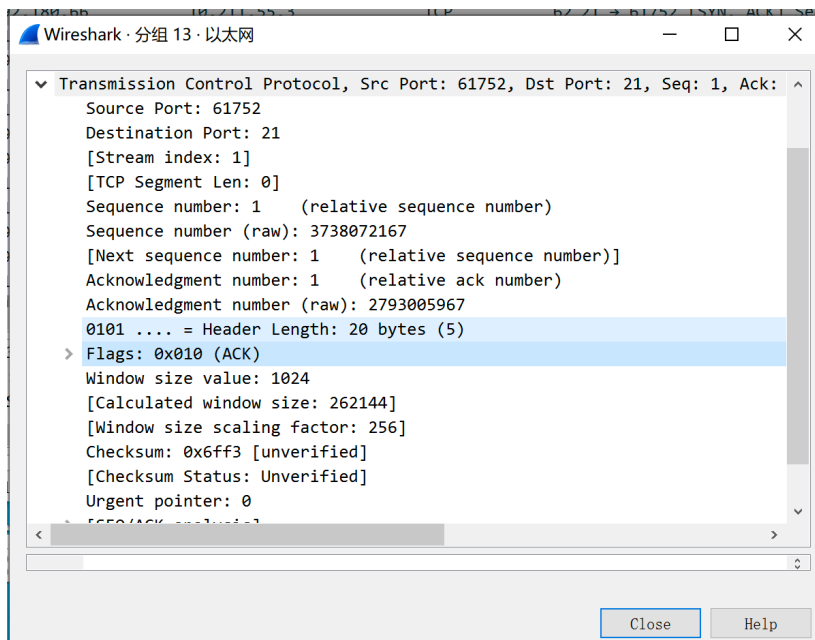
### 1. 本机向 ftp 服务器申请连接，flag=SYN



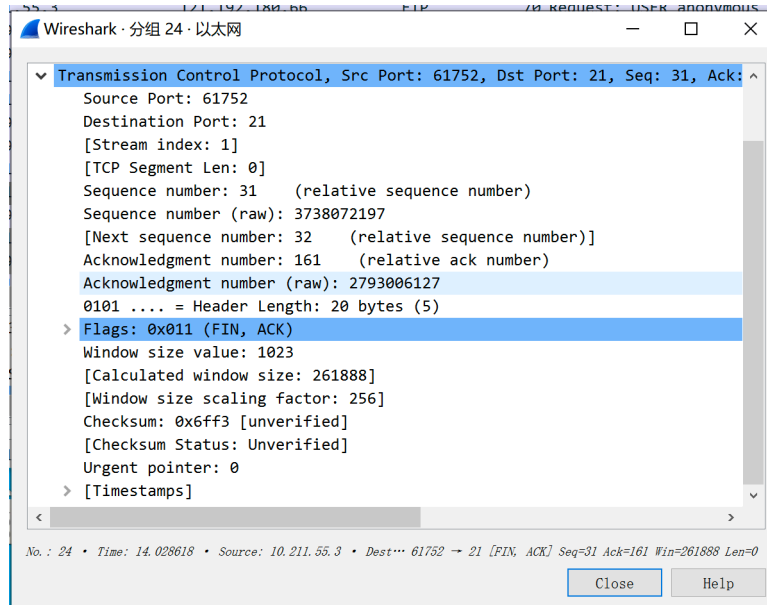
### 2. ftp 服务器回复本机，flag=SYN, ACK



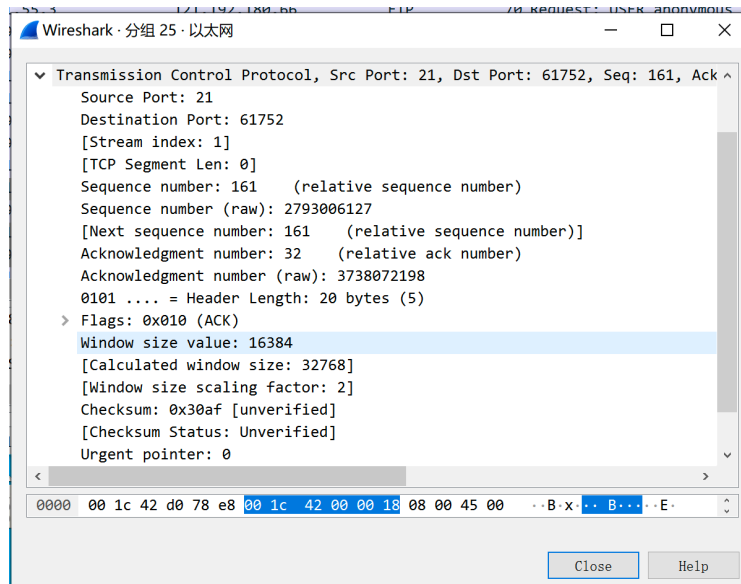
3. 本机收到，答复 FTP 服务器，flag=ACK



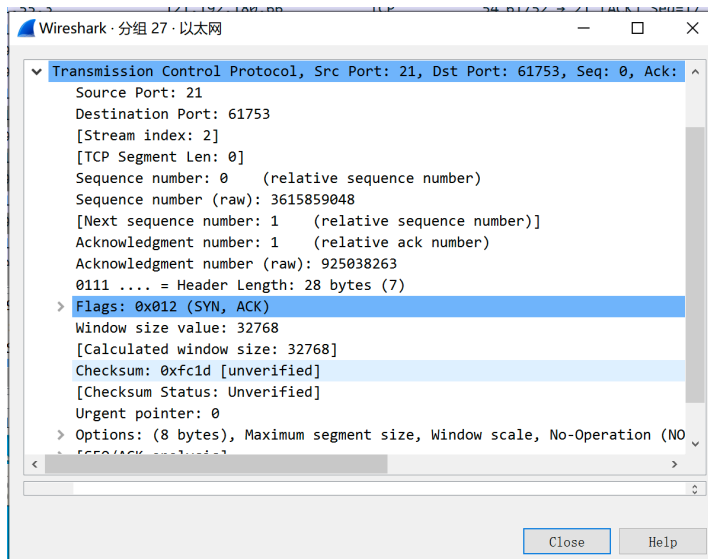
4. 本机向 ftp 申请断开，flag=FIN，ACK



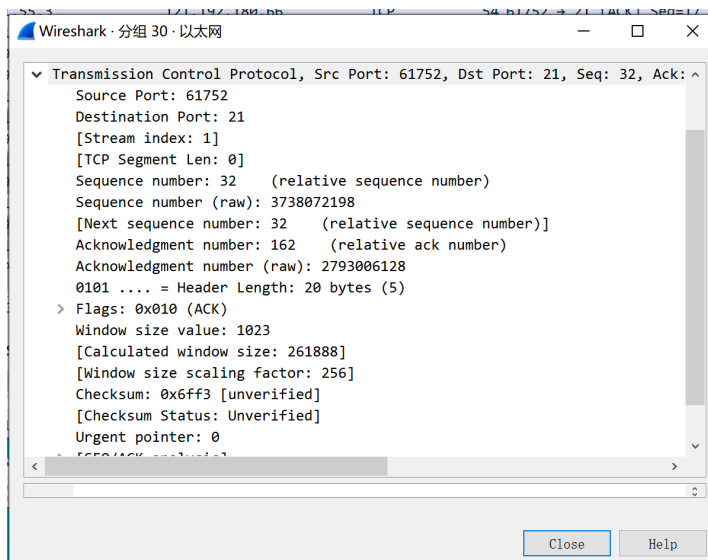
5. ftp 收到申请答复本机，flag=ACK



6. ftp 服务器已经断开与本机的连接，向本机发信，flag=FIN, ACK



7. 本机收到，断开与 ftp 服务器连接，向 ftp 服务器返信， flag=ACK



## 利用 Wireshark 来捕获相关数据，用于程序分析

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	124.225.118.86	10.211.55.3	TCP	60	80 → 61750 [FIN, ACK] Seq=1 Ack=1 Win=16384
2	0.000095	10.211.55.3	124.225.118.86	TCP	54	61750 → 80 [ACK] Seq=1 Ack=2 Win=1025 Len=0
3	0.000135	10.211.55.3	124.225.118.86	TCP	54	61750 → 80 [FIN, ACK] Seq=1 Ack=2 Win=1025 L
4	0.000300	124.225.118.86	10.211.55.3	TCP	60	80 → 61750 [ACK] Seq=2 Ack=2 Win=16384 Len=0
5	7.570582	10.211.55.3	121.192.180.66	TCP	66	61752 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1
6	7.613253	121.192.180.66	10.211.55.3	TCP	62	21 → 61752 [SYN, ACK] Seq=0 Ack=1 Win=32768
7	7.613333	10.211.55.3	121.192.180.66	TCP	54	61752 → 21 [ACK] Seq=1 Ack=1 Win=262144 Len=
8	7.656015	121.192.180.66	10.211.55.3	FTP	103	Response: 220 Serv-U FTP Server v6.2 for Win
9	7.656091	10.211.55.3	121.192.180.66	TCP	54	61752 → 21 [ACK] Seq=1 Ack=50 Win=261888 Len
10	7.656958	10.211.55.3	121.192.180.66	FTP	70	Request: USER anonymous
11	7.657620	121.192.180.66	10.211.55.3	TCP	60	21 → 61752 [ACK] Seq=50 Ack=17 Win=32768 Len
12	7.882878	121.192.180.66	10.211.55.3	FTP	124	Response: 331 User name okay, please send co
13	7.883053	10.211.55.3	121.192.180.66	TCP	54	61752 → 21 [ACK] Seq=17 Ack=120 Win=261888 L
14	7.883244	10.211.55.3	121.192.180.66	FTP	68	Request: PASS IEUser@
15	7.883337	121.192.180.66	10.211.55.3	TCP	60	21 → 61752 [ACK] Seq=120 Ack=31 Win=32768 Le
16	7.926225	121.192.180.66	10.211.55.3	FTP	95	Response: 530 Sorry, no ANONYMOUS access all
17	7.926302	10.211.55.3	121.192.180.66	TCP	54	61752 → 21 [ACK] Seq=31 Ack=161 Win=261888 L
18	7.926503	10.211.55.3	121.192.180.66	TCP	54	61752 → 21 [FIN, ACK] Seq=31 Ack=161 Win=261

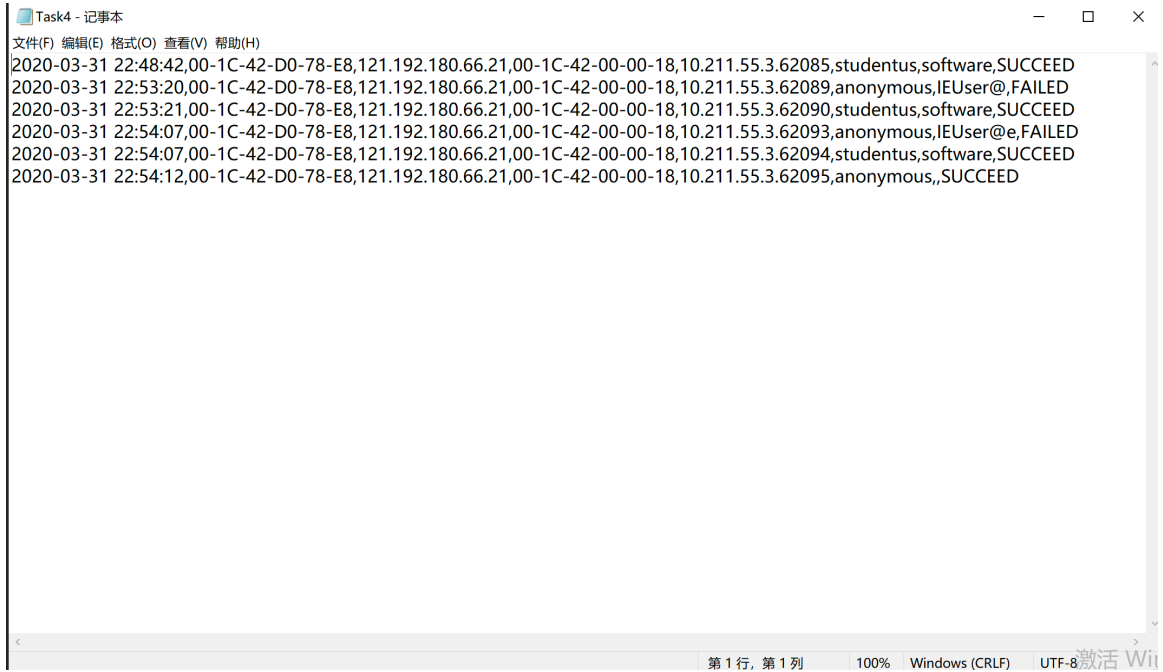
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
> Ethernet II, Src: Parallel\_00:00:18 (00:1c:42:00:00:18), Dst: Parallel\_d0:78:e8 (00:1c:42:d0:78:e8)  
> Internet Protocol Version 4, Src: 124.225.118.86, Dst: 10.211.55.3  
> Transmission Control Protocol, Src Port: 80, Dst Port: 61750, Seq: 1, Ack: 1, Len: 0

编写程序后运行，得到结果：

```
Microsoft Visual Studio 调试控制台
2020-03-31 17:54:46, 00-1C-42-D0-78-E8, 121.192.180.66, 21, 00-1C-42-00-00-18, 10.211.55.3, 61752, anonymous, IEUser@, FAILED
CCDASDFTYUBYI
2020-03-31 17:54:46, 00-1C-42-D0-78-E8, 121.192.180.66, 21, 00-1C-42-00-00-18, 10.211.55.3, 61753, studentus, software, SUCCEED
CCDASDFTYUBYI
2020-03-31 17:54:52, 00-1C-42-D0-78-E8, 121.192.180.66, 21, 00-1C-42-00-00-18, 10.211.55.3, 61754, studentus, software, SUCCEED

\\Mac\Home\Desktop\WpdPack\Examples-peap\Debug\x86\UDPDump.exe (进程 10024) 已退出，代码为 0。
要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口。 . . .
```

## 在实时条件下监听,输出到文件中



```
Task4 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2020-03-31 22:48:42,00-1C-42-D0-78-E8,121.192.180.66.21,00-1C-42-00-00-18,10.211.55.3.62085,studentus,software,SUCCEED
2020-03-31 22:53:20,00-1C-42-D0-78-E8,121.192.180.66.21,00-1C-42-00-00-18,10.211.55.3.62089,anonymous,IEUser@,FAILED
2020-03-31 22:53:21,00-1C-42-D0-78-E8,121.192.180.66.21,00-1C-42-00-00-18,10.211.55.3.62090,studentus,software,SUCCEED
2020-03-31 22:54:07,00-1C-42-D0-78-E8,121.192.180.66.21,00-1C-42-00-00-18,10.211.55.3.62093,anonymous,IEUser@e,FAILED
2020-03-31 22:54:07,00-1C-42-D0-78-E8,121.192.180.66.21,00-1C-42-00-00-18,10.211.55.3.62094,studentus,software,SUCCEED
2020-03-31 22:54:12,00-1C-42-D0-78-E8,121.192.180.66.21,00-1C-42-00-00-18,10.211.55.3.62095,anonymous,,SUCCEED
```

## 4 实验总结

本次实验于上次实验相似,难度上有所提升,帮助我更好地理解网络传输过程中的不同位置上的数据代表的含义也帮助我理解网络上的 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。