厦門大學

信息学院软件工程系

《计算机网络》实验报告

题　　目 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 郑钧元

学　　号 34520182201779

实验时间 2020 年 3 月 30 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。

实验环境

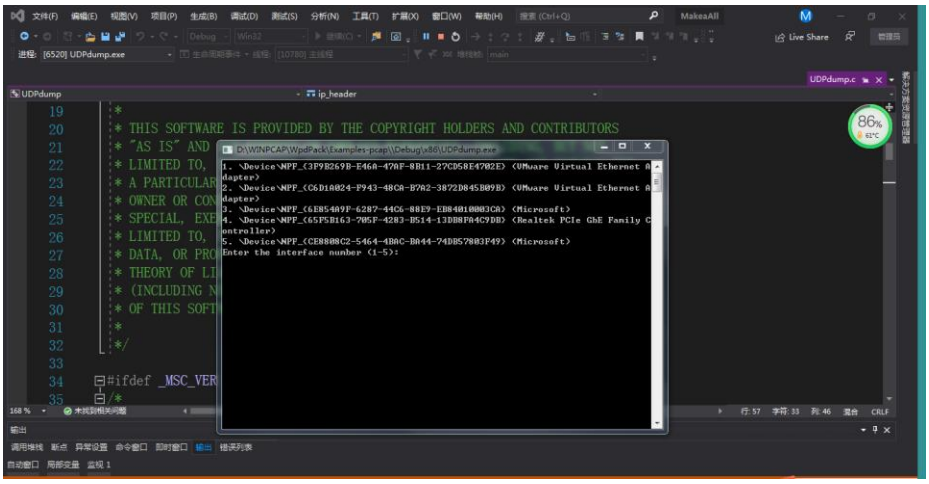
Windows 64 位操作系统 WinPCAP Visual Studio 2019 FTP Rash

编程语言 C

软件：WinPcap 以及 Wireshark 软件 （也可以用）Omnipeek 软件

2 实验结果

选取并用 Visual Studio 2019 启动 MakeaAll.sin 项目程序。



对 UDPdump.exe 文件执行 F10 断点调试获取运行的 main()文件并对它进行运行，得到 5 个网卡。

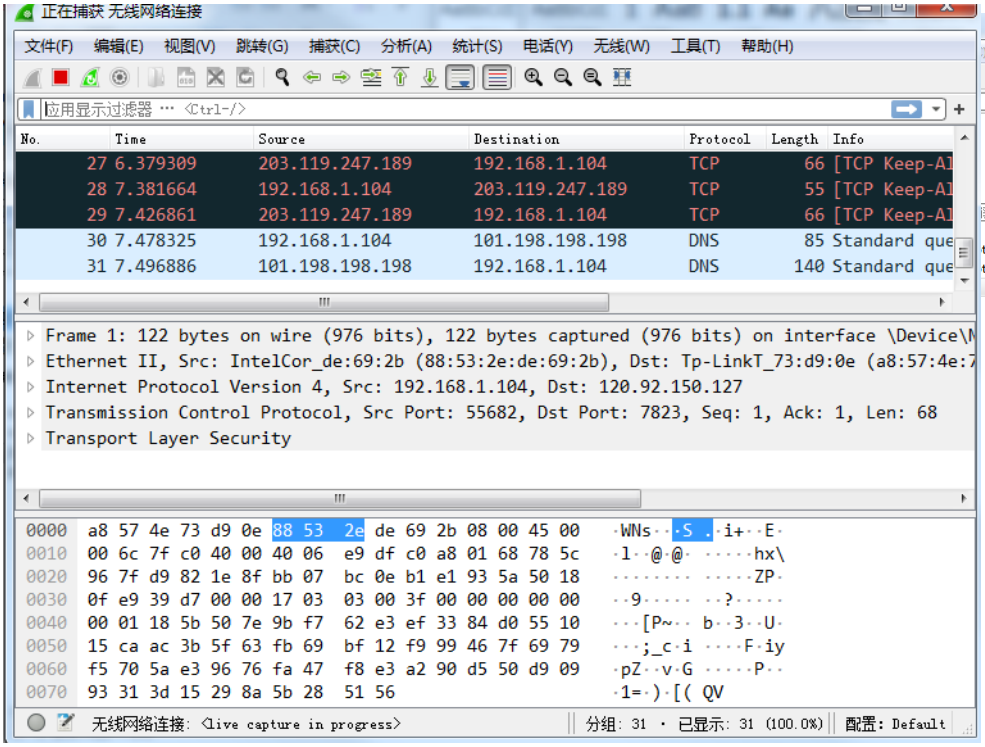
```
17:07:28.878228 len:216 192.168.1.104.65248 -> 239.255.255.250.1900
17:07:29.878831 len:216 192.168.1.104.65248 -> 239.255.255.250.1900
17:07:30.878916 len:216 192.168.1.104.65248 -> 239.255.255.250.1900
17:07:31.355132 len:74 192.168.1.104.52283 -> 114.114.114.114.53
17:07:31.376721 len:159 114.114.114.114.53 -> 192.168.1.104.52283
17:07:31.466694 len:90 45.113.201.39.53 -> 192.168.1.104.52283
17:07:33.909842 len:219 192.168.1.104.52284 -> 239.255.255.250.1900
17:07:34.911027 len:219 192.168.1.104.52284 -> 239.255.255.250.1900
17:07:35.911145 len:219 192.168.1.104.52284 -> 239.255.255.250.1900
17:07:36.912149 len:219 192.168.1.104.52284 -> 239.255.255.250.1900
17:07:38.355932 len:90 192.168.1.104.55857 -> 114.114.114.114.53
17:07:38.365903 len:106 114.114.114.114.53 -> 192.168.1.104.55857
17:07:38.376440 len:155 114.114.114.114.53 -> 192.168.1.104.55857
17:07:40.204591 len:85 192.168.1.104.53317 -> 114.114.114.114.53
17:07:40.231195 len:140 114.114.114.114.53 -> 192.168.1.104.53317
17:07:44.655366 len:94 192.168.1.104.58855 -> 114.114.114.114.53
17:07:44.663253 len:110 114.114.114.114.53 -> 192.168.1.104.58855
17:07:44.683966 len:189 114.114.114.114.53 -> 192.168.1.104.58855
17:07:57.065525 len:312 192.168.1.104.58862 -> 221.181.72.250.53
```

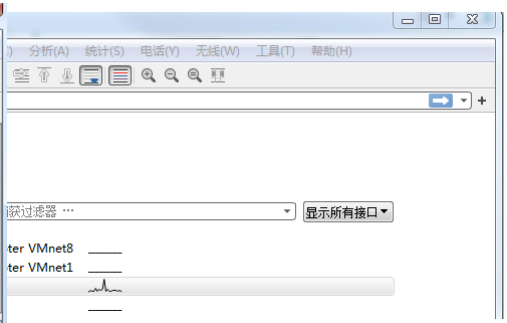
随机选取调试，得到结果……

```
Enter the interface number (1-5):3

listening on Microsoft...
17:06:33.564615 len:82 192.168.1.104.53794 -> 192.168.1.255.1947
```

打开 WindShark，　先对 FTP 进行测验与运行





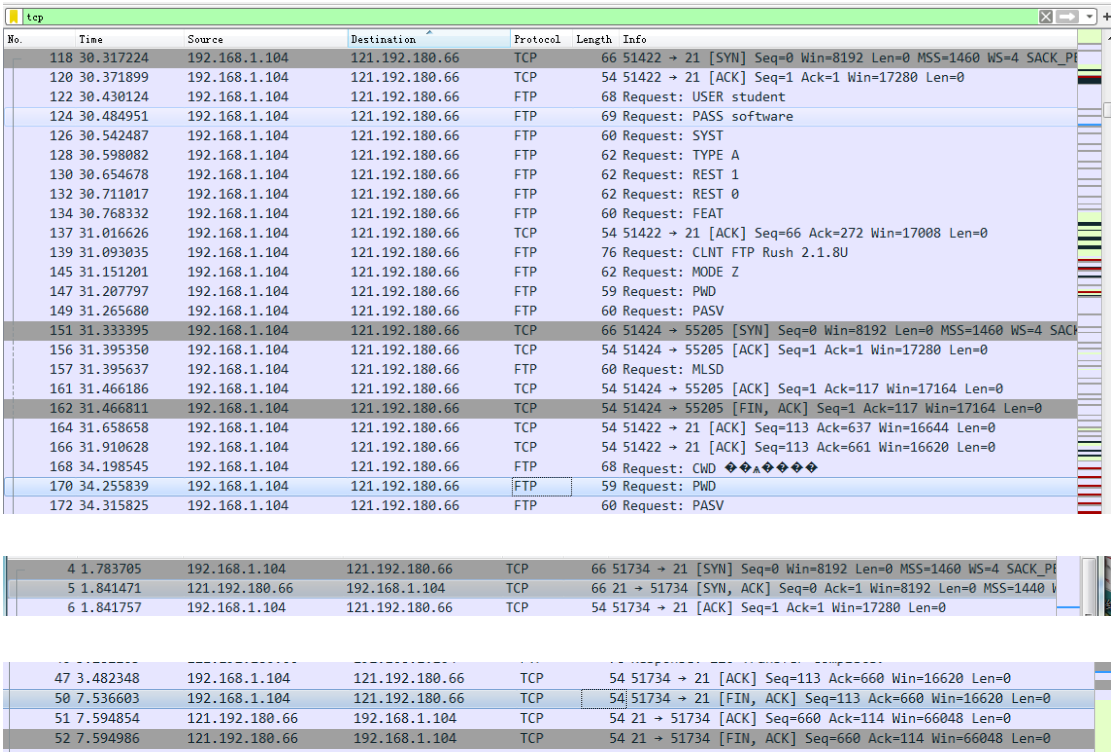
选择无线网络连接

选取某一段作为报文导出并保存到目的文件夹

本机 IP: 192.168.1.104　　FTP 地址：121.192.180.66

1. TCP 握手协议。TCP 握手协议在 TCP/IP 协议中，TCP 协议提供可靠的连接服务，采用三次握手建立一个连接，四次挥手。

下图是运行 ftp 服务器时进行产生的 TCP 的报文，



No.	Time	Source	Destination	Protocol	Length	Info
118	30.317224	192.168.1.104	121.192.180.66	TCP	66	51422 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PE
120	30.371899	192.168.1.104	121.192.180.66	TCP	54	51422 → 21 [ACK] Seq=1 Ack=1 Win=17280 Len=0
122	30.430124	192.168.1.104	121.192.180.66	FTP	68	Request: USER student
124	30.484951	192.168.1.104	121.192.180.66	FTP	69	Request: PASS software
126	30.542487	192.168.1.104	121.192.180.66	FTP	60	Request: SYST
128	30.598082	192.168.1.104	121.192.180.66	FTP	62	Request: TYPE A
130	30.654678	192.168.1.104	121.192.180.66	FTP	62	Request: REST 1
132	30.711017	192.168.1.104	121.192.180.66	FTP	62	Request: REST 0
134	30.768332	192.168.1.104	121.192.180.66	FTP	60	Request: FEAT
137	31.016626	192.168.1.104	121.192.180.66	TCP	54	51422 → 21 [ACK] Seq=66 Ack=272 Win=17008 Len=0
139	31.093035	192.168.1.104	121.192.180.66	FTP	76	Request: CLNT FTP Rush 2.1.8U
145	31.151201	192.168.1.104	121.192.180.66	FTP	62	Request: MODE Z
147	31.207797	192.168.1.104	121.192.180.66	FTP	59	Request: PWD
149	31.265680	192.168.1.104	121.192.180.66	FTP	60	Request: PASV
151	31.333395	192.168.1.104	121.192.180.66	TCP	66	51424 → 55205 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK
156	31.395350	192.168.1.104	121.192.180.66	TCP	54	51424 → 55205 [ACK] Seq=1 Ack=1 Win=17280 Len=0
157	31.395637	192.168.1.104	121.192.180.66	FTP	60	Request: MLSD
161	31.466186	192.168.1.104	121.192.180.66	TCP	54	51424 → 55205 [ACK] Seq=1 Ack=117 Win=17164 Len=0
162	31.466811	192.168.1.104	121.192.180.66	TCP	54	51424 → 55205 [FIN, ACK] Seq=1 Ack=117 Win=17164 Len=0
164	31.658658	192.168.1.104	121.192.180.66	TCP	54	51422 → 21 [ACK] Seq=113 Ack=637 Win=16644 Len=0
166	31.910628	192.168.1.104	121.192.180.66	TCP	54	51422 → 21 [ACK] Seq=113 Ack=661 Win=16620 Len=0
168	34.198545	192.168.1.104	121.192.180.66	FTP	68	Request: CWD ??A????
170	34.255839	192.168.1.104	121.192.180.66	FTP	59	Request: PWD
172	34.315825	192.168.1.104	121.192.180.66	FTP	60	Request: PASV

4	1.783705	192.168.1.104	121.192.180.66	TCP	66	51734 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PE
5	1.841471	121.192.180.66	192.168.1.104	TCP	66	21 → 51734 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 W
6	1.841757	192.168.1.104	121.192.180.66	TCP	54	51734 → 21 [ACK] Seq=1 Ack=1 Win=17280 Len=0

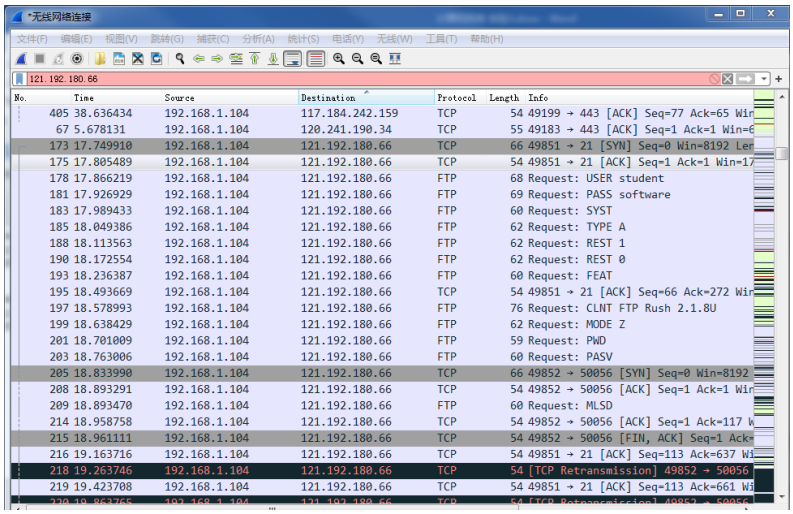
47	3.482348	192.168.1.104	121.192.180.66	TCP	54	51734 → 21 [ACK] Seq=113 Ack=660 Win=16620 Len=0
50	7.536603	192.168.1.104	121.192.180.66	TCP	54	51734 → 21 [FIN, ACK] Seq=113 Ack=660 Win=16620 Len=0
51	7.594854	121.192.180.66	192.168.1.104	TCP	54	21 → 51734 [ACK] Seq=660 Ack=114 Win=66048 Len=0
52	7.594986	121.192.180.66	192.168.1.104	TCP	54	21 → 51734 [FIN, ACK] Seq=660 Ack=114 Win=66048 Len=0

截图：依据实验步骤，我们在的登录的同时马上观察，发现了可以比较明显的出现前面三次的 TCP 握手和后面的四次挥手

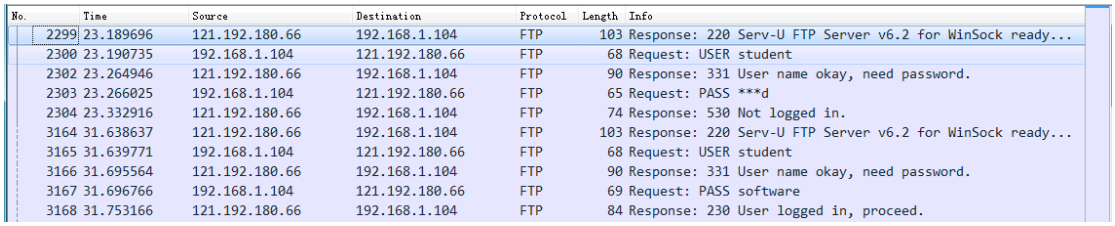
最上面是包括了 FTP 进程的总体报文，中间是大致的三次握手协议（因为中间必然存在一定的错误和延迟，没有连在一起，但是依旧是满足条件的）

接下来我们对 FTP 的对应的密码和值进行分析和观测 ：

1.按照实验步骤，自主测试了错误的密码数据和正确的密码数据，在 FTPrush 环境下，错误密码不会显示出来而正确的密码最后还是显示出来并且成功得到登进



观察到有用到 USER 和 PASS 的值的下面字段（下截图）

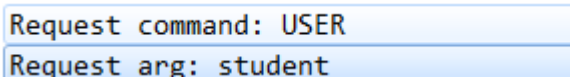


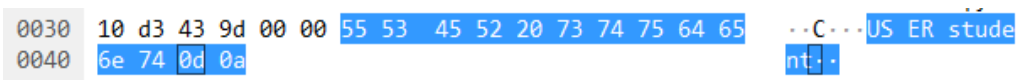
No.	Time	Source	Destination	Protocol	Length	Info
2299	23.189696	121.192.180.66	192.168.1.104	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
2300	23.190735	192.168.1.104	121.192.180.66	FTP	68	Request: USER student
2302	23.264946	121.192.180.66	192.168.1.104	FTP	90	Response: 331 User name okay, need password.
2303	23.266025	192.168.1.104	121.192.180.66	FTP	65	Request: PASS ***d
2304	23.332916	121.192.180.66	192.168.1.104	FTP	74	Response: 530 Not logged in.
3164	31.638637	121.192.180.66	192.168.1.104	FTP	103	Response: 220 Serv-U FTP Server v6.2 for WinSock ready...
3165	31.639771	192.168.1.104	121.192.180.66	FTP	68	Request: USER student
3166	31.695564	121.192.180.66	192.168.1.104	FTP	90	Response: 331 User name okay, need password.
3167	31.696766	192.168.1.104	121.192.180.66	FTP	69	Request: PASS software
3168	31.753166	121.192.180.66	192.168.1.104	FTP	84	Response: 230 User logged in, proceed.

以为 FTP 为关键字分别截取了成功的报文和失败的报文，成功显示 logged in 失败显示 Not logged in 对内部分别进行分析：都是

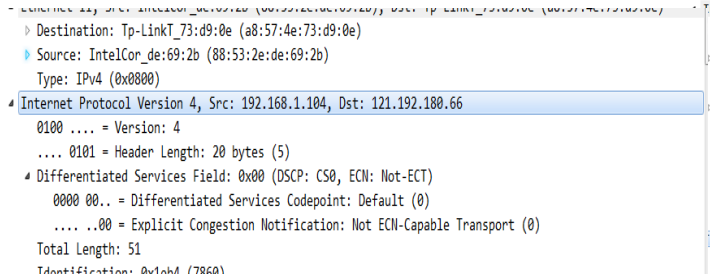
Internet Protocol Version 4, Src: 192.168.1.104, Dst: 121.192.180.66

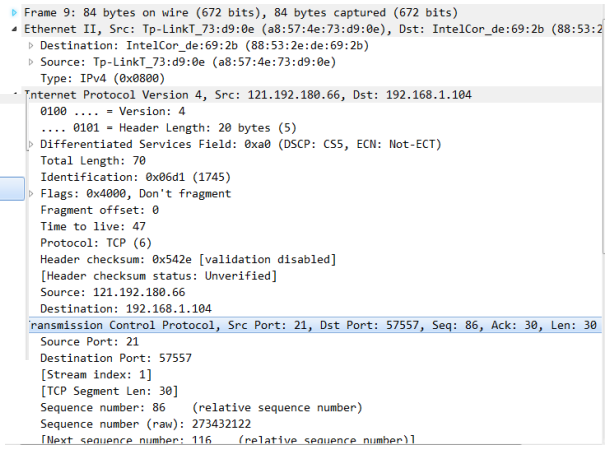
1. User student :





总体参数





2. PASS ***(error):

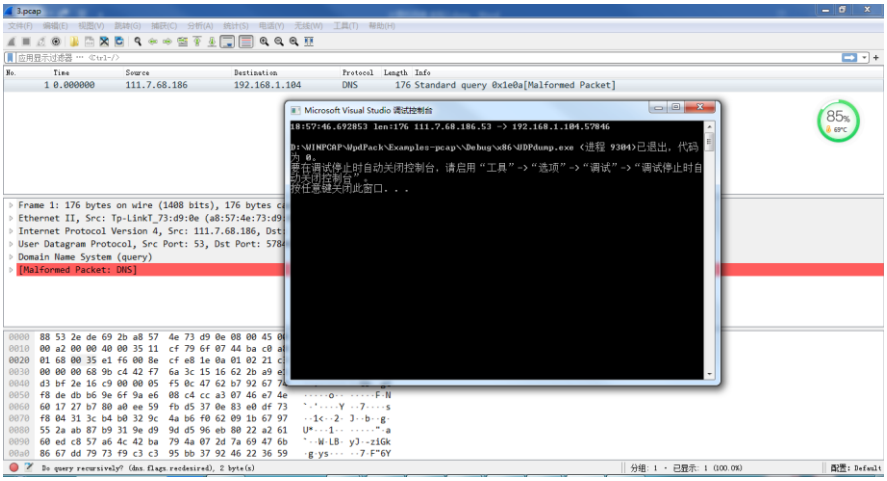
```
0030  10 ca f6 f2 00 00 50 41  53 53 20 2a 2a 2a 64 0d   ......PA SS ***d·
0040  0a                                                 ·
```

3. (Not) logged in:　状态：成功：230　失败：530

```
0030  01 02 83 4b 00 00 32 33  30 20 55 73 65 72 20 6c   ···K··23 0 User l
0040  6f 67 67 65 64 20 69 6e  2c 20 70 72 6f 63 65 65   ogged in , procee
0050  64 2e 0d 0a                                       d.··
```

其中：230 等价于 32 33 30　530 等价于 35 33 30

更改 UDPdump.c 文件以适配相应的报文。（可以从对应项目同级目录中找到 readfile.c 文件并截取/* Open the capture file */段函数并 copy 在 UDPdump.c 中），运行程序，得到结果。



图：与报文内容基本一致

结合之前样例，对同样的 C 文件进行追加和改进，把原始定义的整个结构体的相关系数进行输出，得到更多的相关系数的处理、可视化，最后再执行运行，发现也是与相同原来的.pcap 文件相同的 Source 和 Destination：

```
2020-03-31 20:20:00.253493 len:84
Source: 121.192.180.66.21 -> Destination: 192.168.1.104.57557
        Source address:: 79 C0 B4 42  121.192.180.66.
        distination address: C0 A8 01 68  192.168.1.104.
USER: student PASS : software.    succeed.
```

```
2020-03-31 20:20:57.833243 len:74
Source: 121.192.180.66.21 -> Destination: 192.168.1.104.57555
        Source address:: 79 C0 B4 42  121.192.180.66.
        distination address: C0 A8 01 68  192.168.1.104.
USER: student PASS : softwar.    failed.
```

3 实验总结

本次实验涉及的应用软件范围广，初次接触网络编程自然比较陌生。需要下载一定的网络软件以进行调试和处理。其中比较重要的是 Visual Studio 的开发应用，选取运行，以及相关辅助软件对报文的截取，编程中，我们继续对 WinPcap 包下的 C 文件，科来数据包播放器，以及 Wireshark 软件都进行了一定的实际操作和处理，发现报文可以实现截取，观察发现相同数据，表明成功。但是同时我们也不能避免一定的误码等问题发生。此外，相比上一次实验，我们添加了 FTP 并对其中的相关进程进行提取和分析，观察是否能够得到进程中生成的用户名以及密码，然后对此作出了验证，最终也是对 UDPdump.c 做出重构与要素提取，最终合成.csv 文件并输出，了解到整个 FTP 登录的流程、如何判断是否登录成功以及相关的参数。