

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 林晖

学 号 24320182203231

实验时间 2020 年 3 月 25 日

2020 年 3 月 30 日

1 实验目的

本实验是“用 PCAP 库侦听并解析 FTP 口令”实验的第二部分。

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

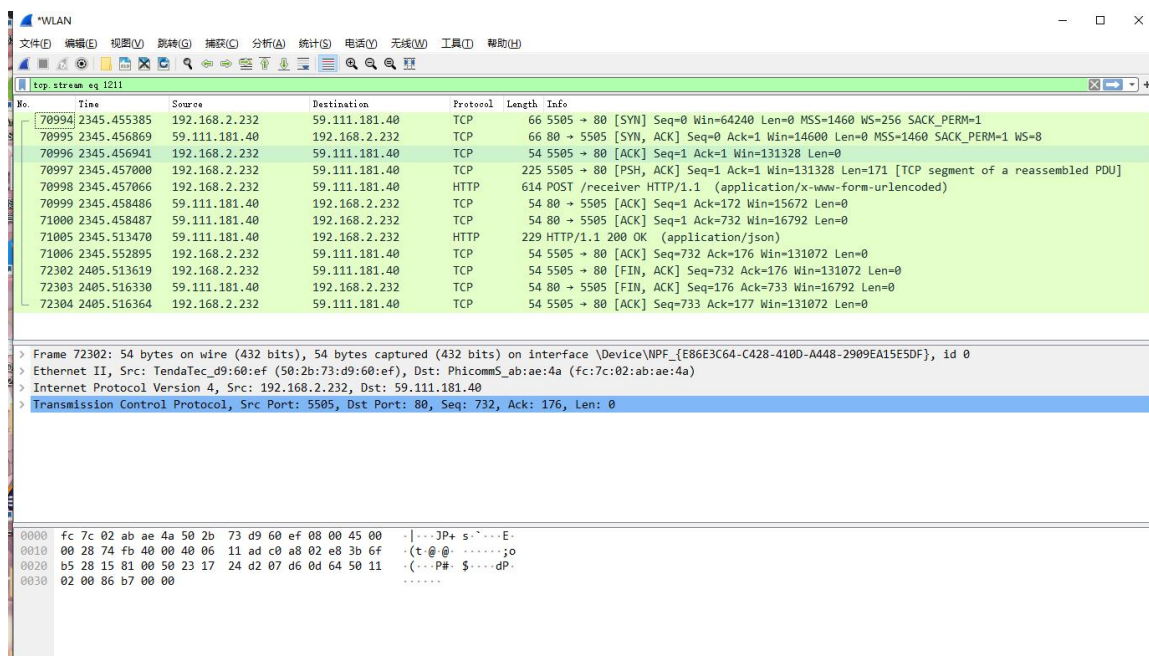
D5-72,192.168.33.2,student,software1,FAILED

2 实验环境

操作系统：Windows 10，编程语言：C。

3 实验结果

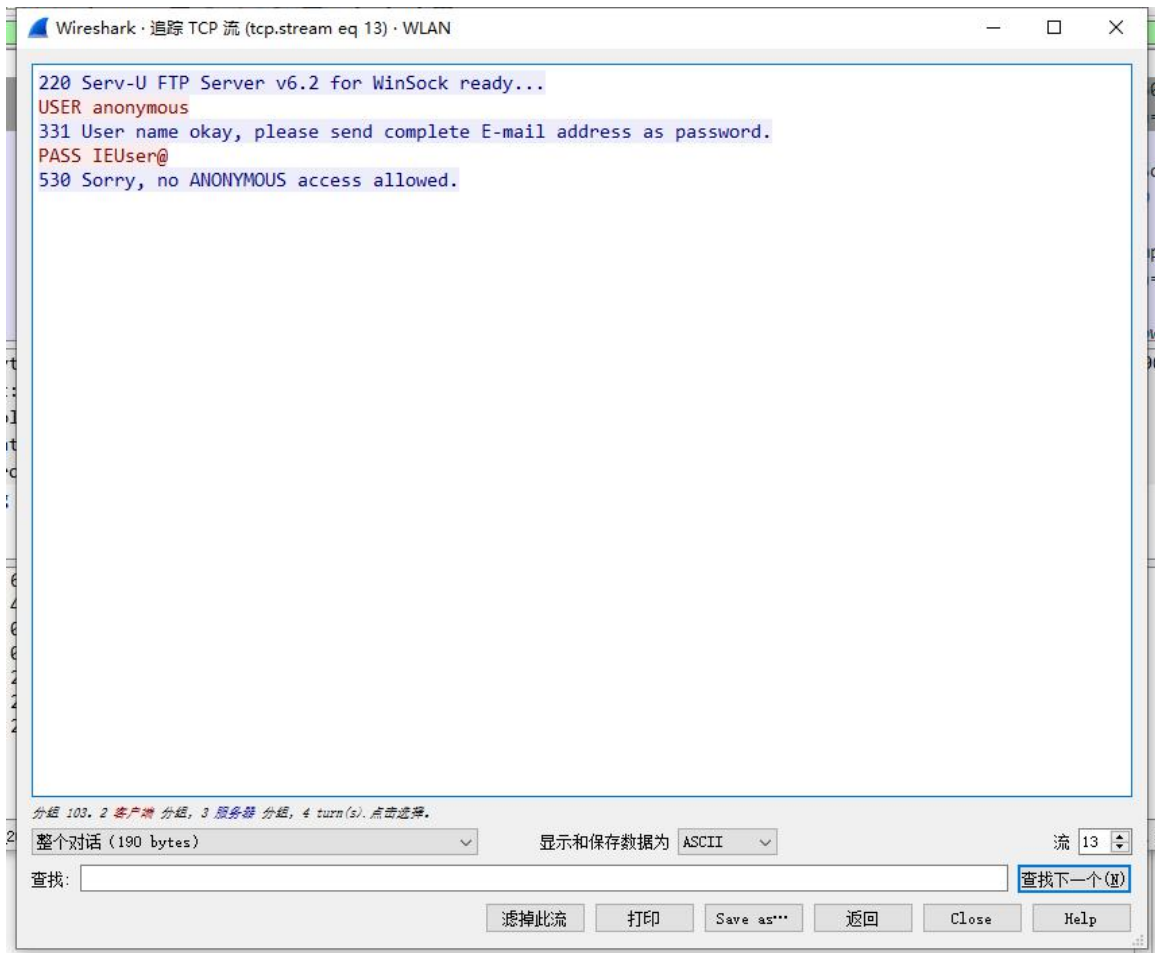
WireShark 侦听 TCP:



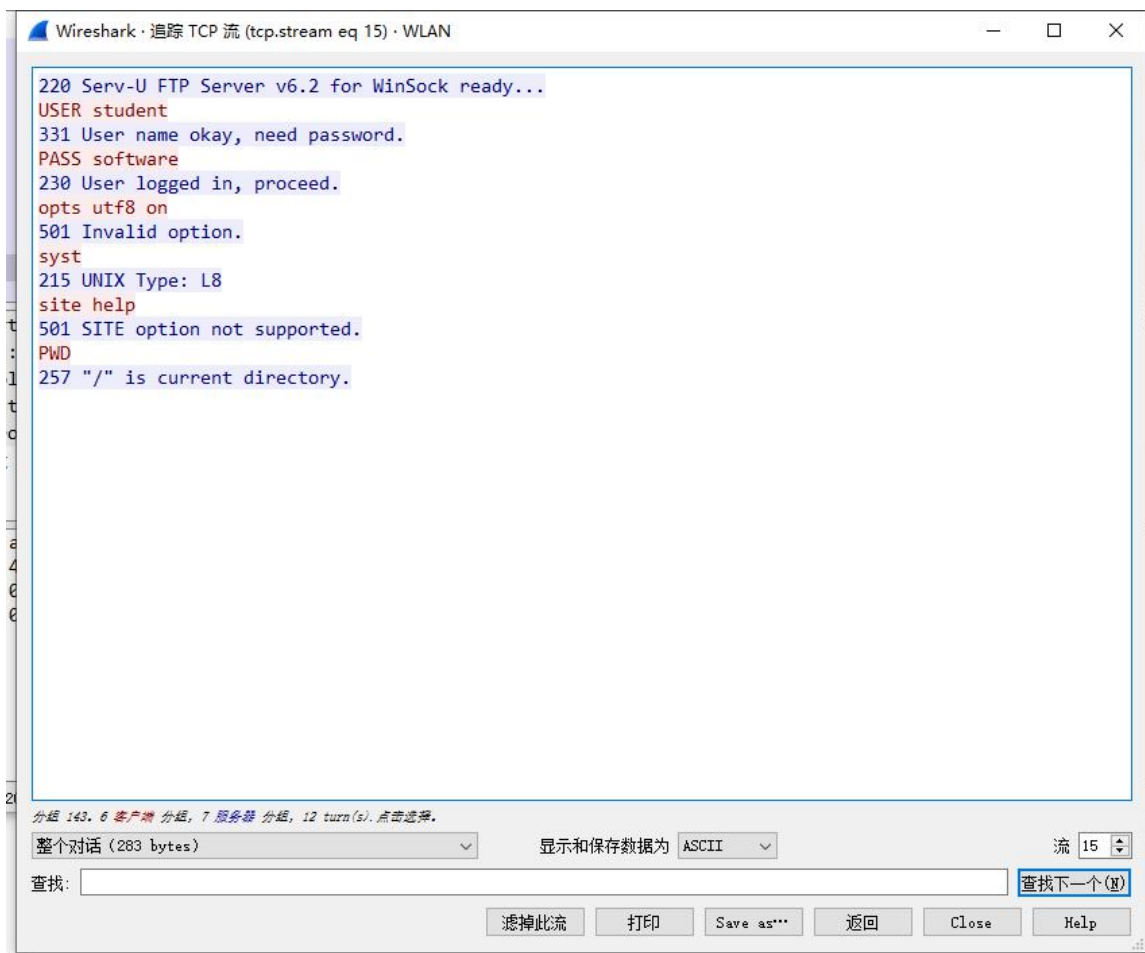
观察 TCP 报文段接收的三次握手以及断开的四次挥手过程。

同时观察其接收窗口大小，即窗口机制，以及拥塞控制机制等。

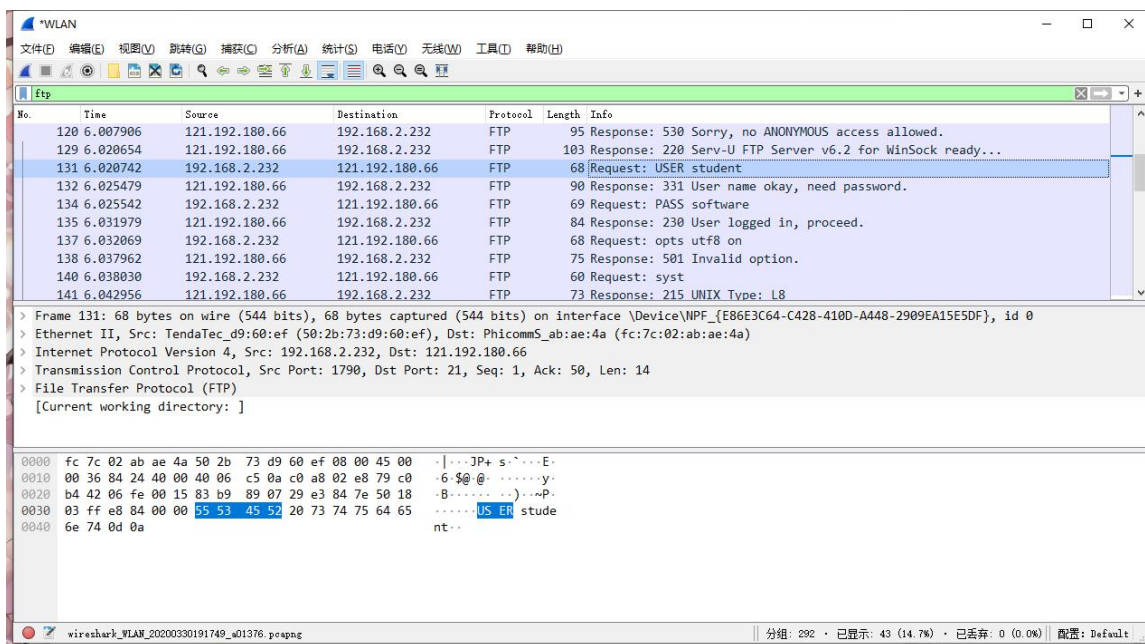
Wireshark 侦听 FTP:

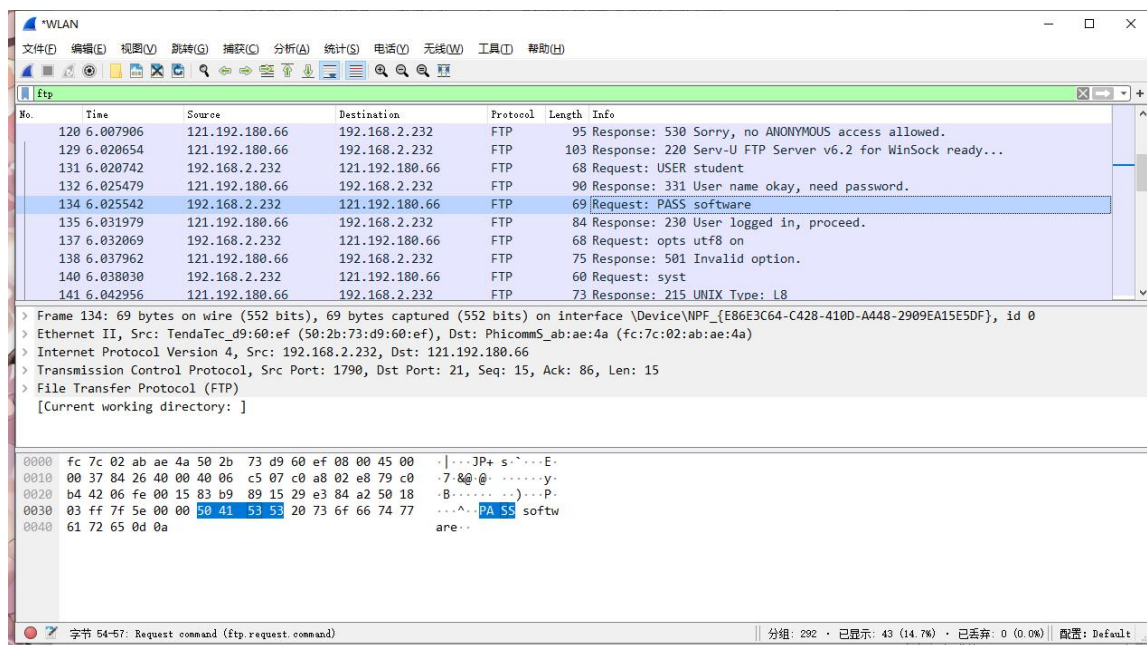


登录失败时: 显示 530 Sorry, no ANONYMOUS access allowed.



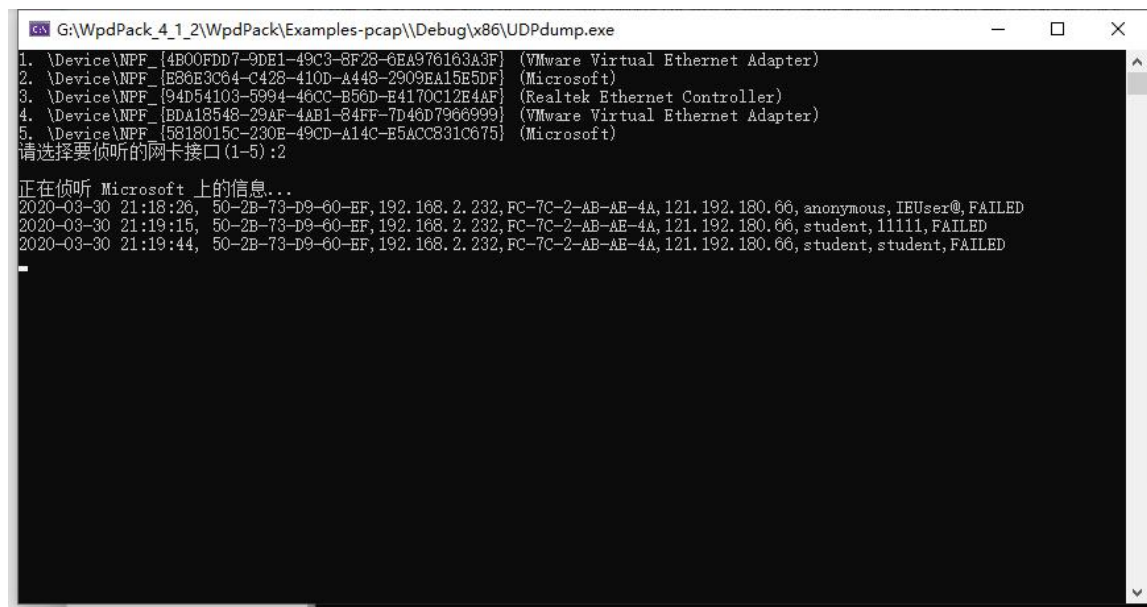
登录成功时：显示 230 User logged in, proceed.





观察发现：存在 USER 和 PASS 开始的报文用于登录。

登录 FTP：



登录失败：显示 FAILED

```
G:\WpdPack_4_1_2\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe

1. \Device\NPF_{4B00FDD7-9DE1-49C3-8F28-6EA976163A3F} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{E86E3C64-C428-410D-A448-2909EA15E5DF} (Microsoft)
3. \Device\NPF_{94D54103-5994-46CC-B56D-E4170C12E4AF} (Realtek Ethernet Controller)
4. \Device\NPF_{BDA18548-29AF-4AB1-84FF-7D46D7966999} (VMware Virtual Ethernet Adapter)
5. \Device\NPF_{5818015C-230E-49CD-A14C-E5ACC831C675} (Microsoft)
请选择要倾听的网卡接口(1-5):2

正在倾听 Microsoft 上的信息...
2020-03-30 21:18:26, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, anonymous, IEUser@, FAILED
2020-03-30 21:19:15, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 11111, FAILED
2020-03-30 21:19:44, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, student, FAILED
2020-03-30 21:19:57, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, software, SUCCEED
2020-03-30 21:19:57, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, software, SUCCEED
```

登录成功：显示 SUCCEED

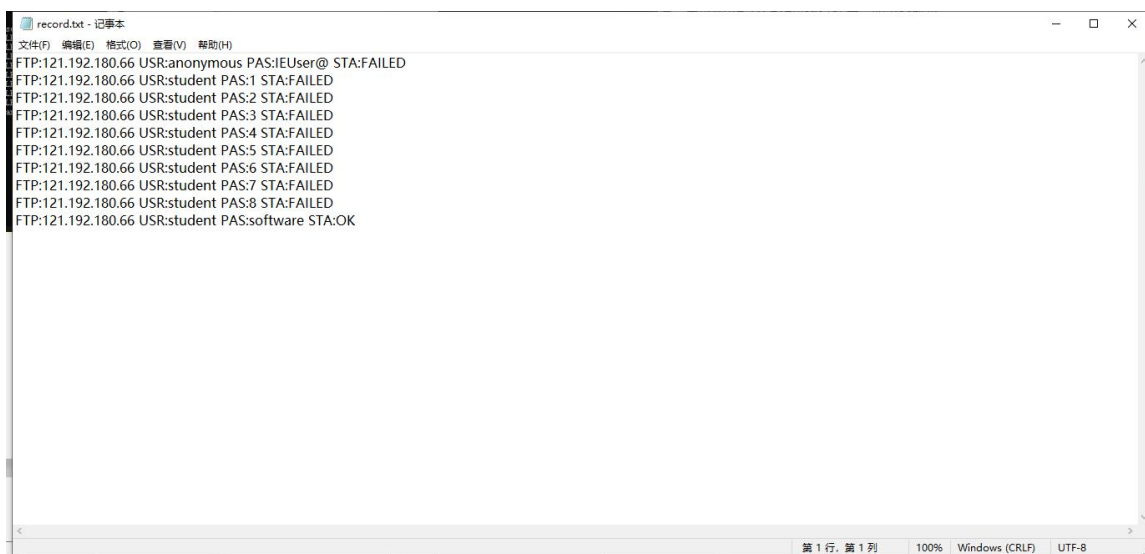
```
Microsoft Visual Studio 调试控制台

1. \Device\NPF_{4B00FDD7-9DE1-49C3-8F28-6EA976163A3F} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{E86E3C64-C428-410D-A448-2909EA15E5DF} (Microsoft)
3. \Device\NPF_{94D54103-5994-46CC-B56D-E4170C12E4AF} (Realtek Ethernet Controller)
4. \Device\NPF_{BDA18548-29AF-4AB1-84FF-7D46D7966999} (VMware Virtual Ethernet Adapter)
5. \Device\NPF_{5818015C-230E-49CD-A14C-E5ACC831C675} (Microsoft)
请选择要倾听的网卡接口(1-5):2

正在倾听 Microsoft 上的信息...
2020-03-30 23:21:29, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, anonymous, IEUser@, FAILED
2020-03-30 23:21:31, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 1, FAILED
2020-03-30 23:21:33, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 2, FAILED
2020-03-30 23:21:34, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 3, FAILED
2020-03-30 23:21:35, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 4, FAILED
2020-03-30 23:21:38, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 5, FAILED
2020-03-30 23:21:39, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 6, FAILED
2020-03-30 23:21:41, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 7, FAILED
2020-03-30 23:21:42, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, 8, FAILED
2020-03-30 23:21:51, 50-2B-73-D9-60-EF, 192.168.2.232, FC-7C-2-AB-AE-4A, 121.192.180.66, student, software, SUCCEED

G:\WpdPack_4_1_2\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe (进程 29232)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。...
```

读取 FTP 登录信息，并将其写入文件 record.txt



```
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:1 STA:FAILED
FTP:121.192.180.66 USR:student PAS:2 STA:FAILED
FTP:121.192.180.66 USR:student PAS:3 STA:FAILED
FTP:121.192.180.66 USR:student PAS:4 STA:FAILED
FTP:121.192.180.66 USR:student PAS:5 STA:FAILED
FTP:121.192.180.66 USR:student PAS:6 STA:FAILED
FTP:121.192.180.66 USR:student PAS:7 STA:FAILED
FTP:121.192.180.66 USR:student PAS:8 STA:FAILED
FTP:121.192.180.66 USR:student PAS:software STA:OK

第 1 行, 第 1 列  100%  Windows (CRLF)  UTF-8
```

record.txt 文件内容

4 实验总结

实际实现了侦听 TCP 和 FTP 报文段的功能，观察了 TCP 握手和挥手的过程，并且实现了搭建 FTP 服务器，并通过监听 FTP 通信了解了 FTP 登录的通信过程，更加熟悉了报文格式。