

**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**
   * 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。
   * 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**

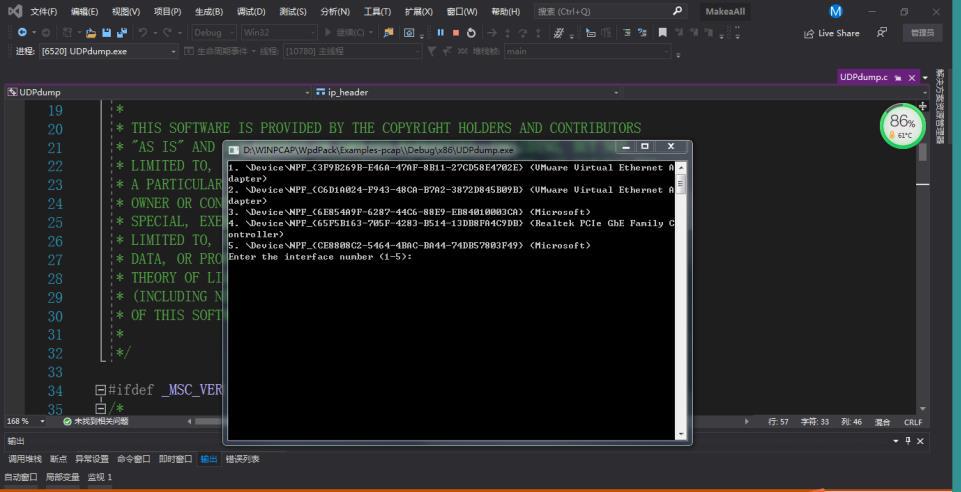
Windows 64 位操作系统 WinPCAP Visual Studio 2019 FTP Rash

编程语言 C

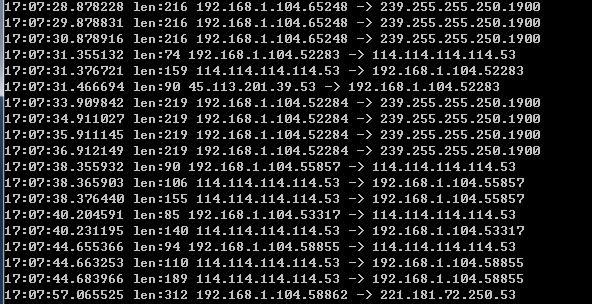
软件：WinPcap 以及 Wireshark 软件 （也可以用）Omnipeek 软件

1. **实验结果**

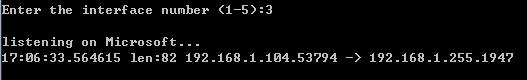
选取并用 Visual Studio 2019 启动 MakeaAll.sin 项目程序。



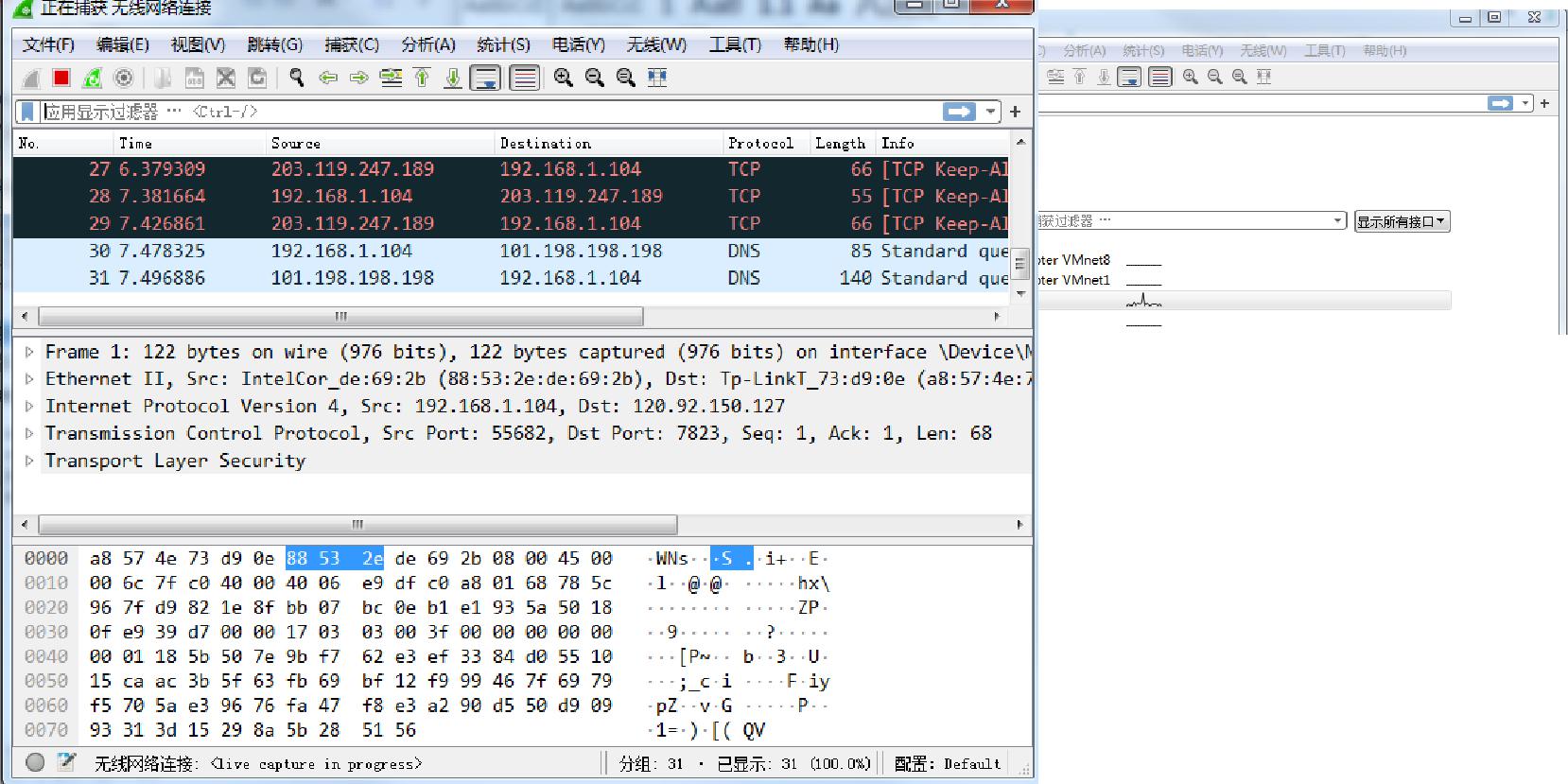
对 UDPdump.exe 文件执行 F10 断点调试获取运行的main()文件并对它进行运行，得到 5 个网卡。



随机选取调试，得到结果……



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

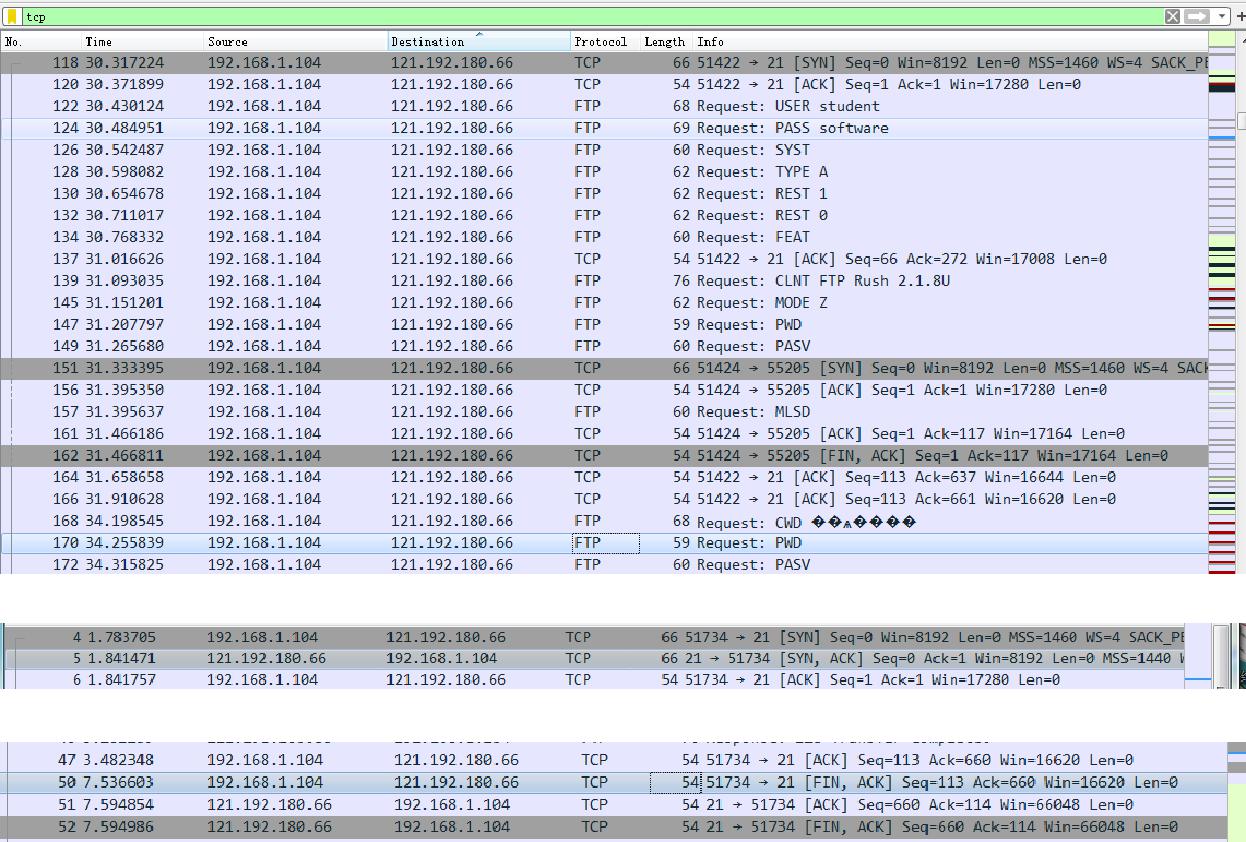
文导出并保存到目

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，

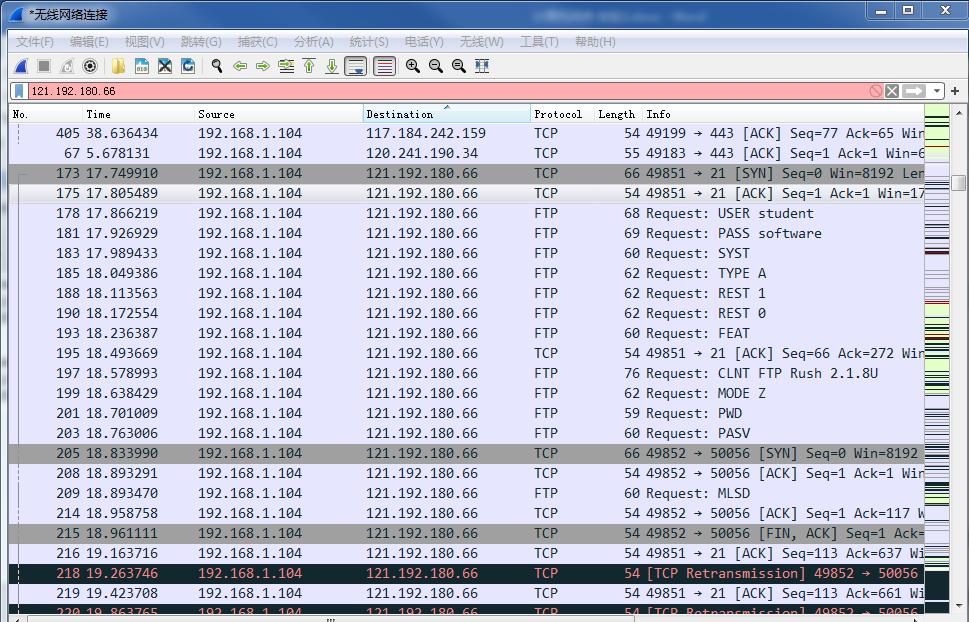


截图：依据实验步骤，我们在的登录的同时马上观察，发现了可以比较明显的出现前面三次的 TCP 握手和后面的四次挥手

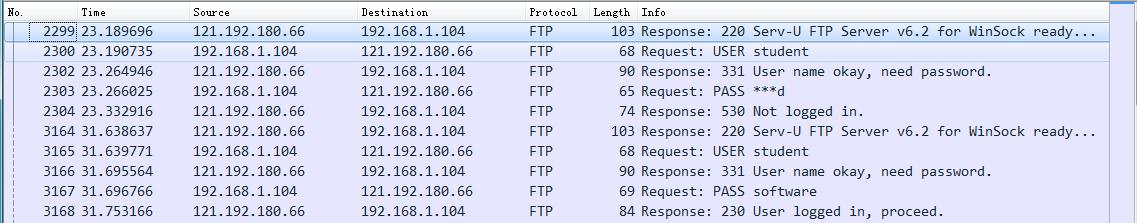
最上面是包括了 FTP 进程的总体报文，中间是大致的三次握手协议（因为中间必然存在一定的错误和延迟，没有连在一起，但是依旧是满足条件的）

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）

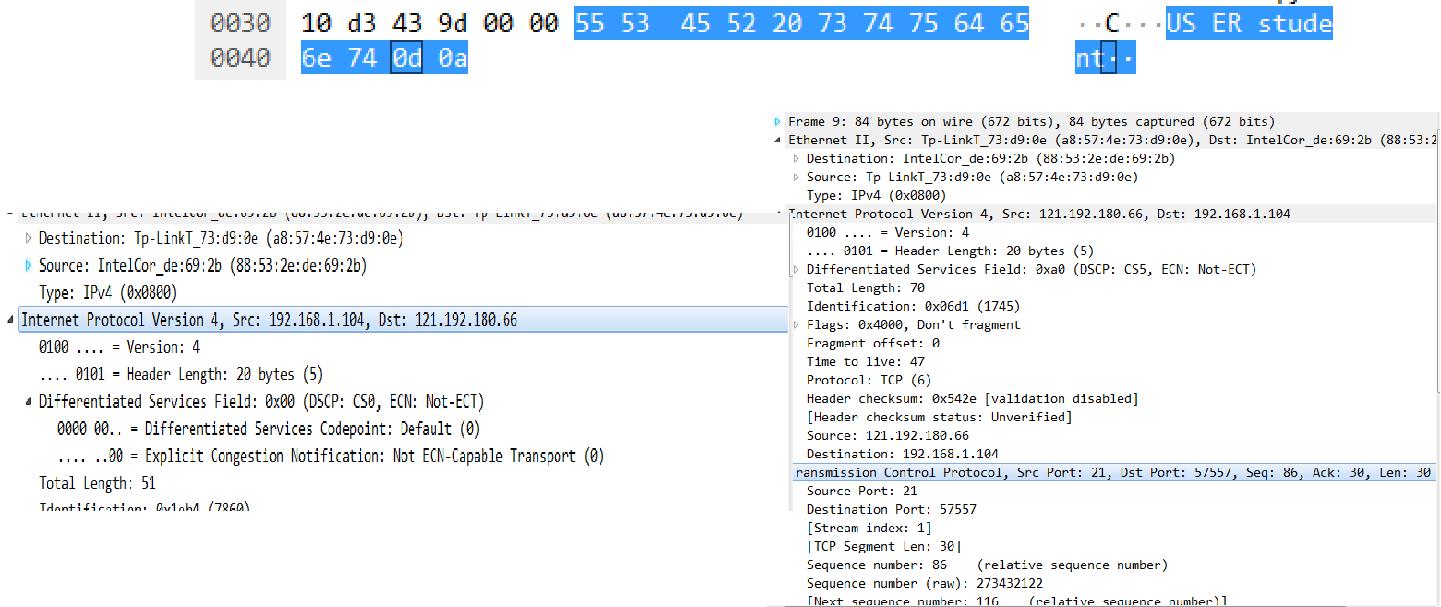


以为 FTP 为关键字分别截取了成功的报文和失败的报文，成功显示 logged in 失败显示 Not logged in 对内部分别进行分析：都是

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

1. User student :

总体参数



2. PASS \*\*\*(error):

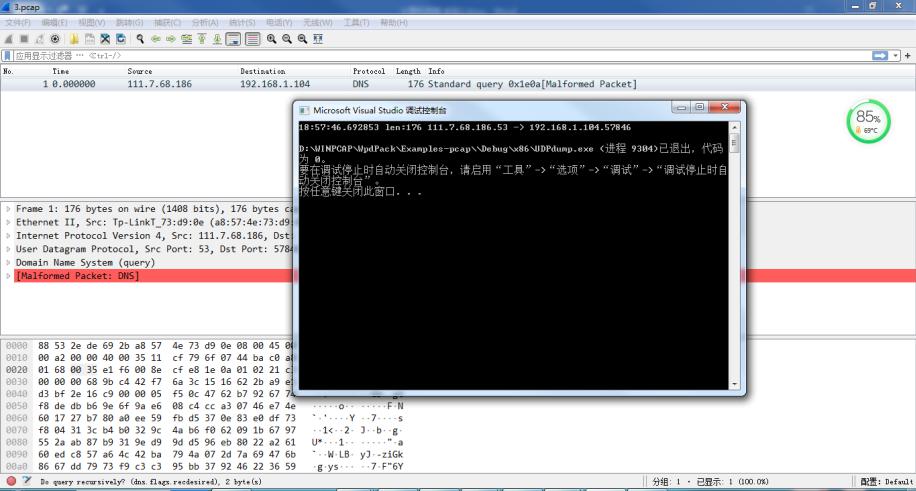


3. (Not) logged in: 状态：成功：230 失败：530



|  |  |
| --- | --- |
| 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

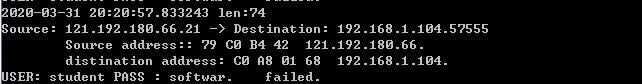
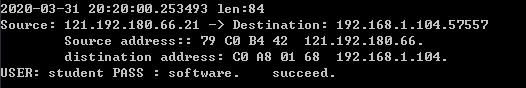


结果。

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：



1. **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。