

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三**用 PCAP 库侦听并分析网络流量

**班　　级 软件工程2019级1班**

**姓　　名 王冠霖**

**学　　号 22920192204282**

**实验时间 2021年4月02日**

**2021 年 4 月 02 日**

填写说明

1. 本文件为Word模板文件，建议使用Microsoft Word 2019打开，在可填写的区域中如实填写；
2. 填表时，勿破坏排版，勿修改字体字号，打印成PDF文件提交；
3. 文件总大小尽量控制在1MB以下，勿超过5MB；
4. 材料清单上传在代码托管平台上；
5. 在学期末将报告按“CNI-E1-00020190000000-张三”的命名后（其中E1是Experiment 1的缩写），压缩为zip文件，作为附件，以“计算机网络-实验报告-00020190000000-张三”发送至cni21@qq.com。

# 实验目的

理解 数据链路层、网络层、传输层 和 应用层 的基本原理。

掌握用 Wireshark 观察网络流量并辅助网络侦听相关的编程；

掌握用 Libpcap 或 WinPcap 库侦听并处理以太网帧和 IP 报文的方法；

熟悉 以太网帧、IP 报文、TCP 段和 FTP 命令的格式概念，掌握 TCP 协议的基本机制；

熟悉 帧头部 或 IP 报文头部 各字段的含义。

熟悉 TCP 段和 FTP 数据协议的概念，熟悉 段头部各字段 和 FTP 控制命令的指令和数据的含义。

# 实验环境

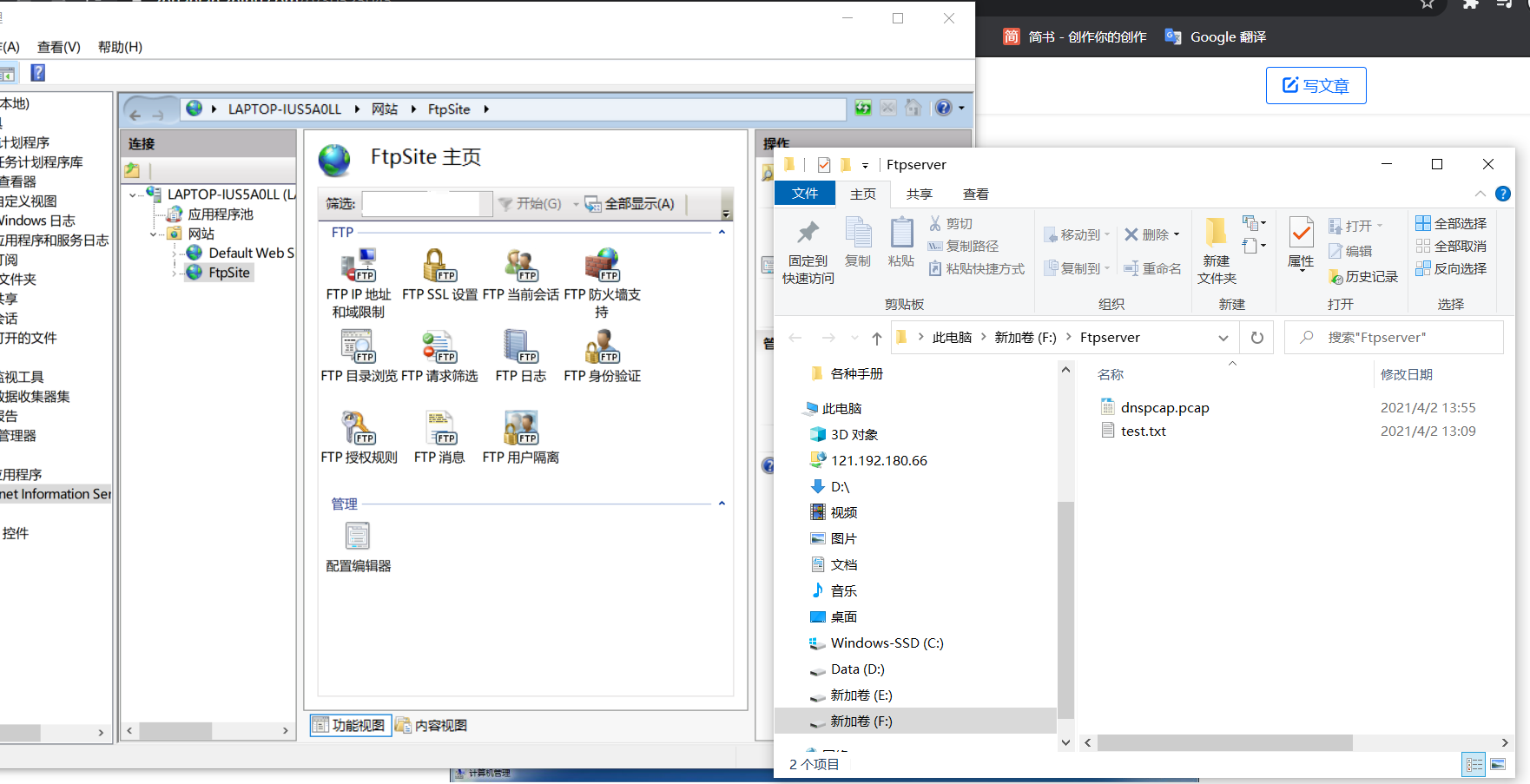
操作系统: Windows

编译器: Visual Studio2019

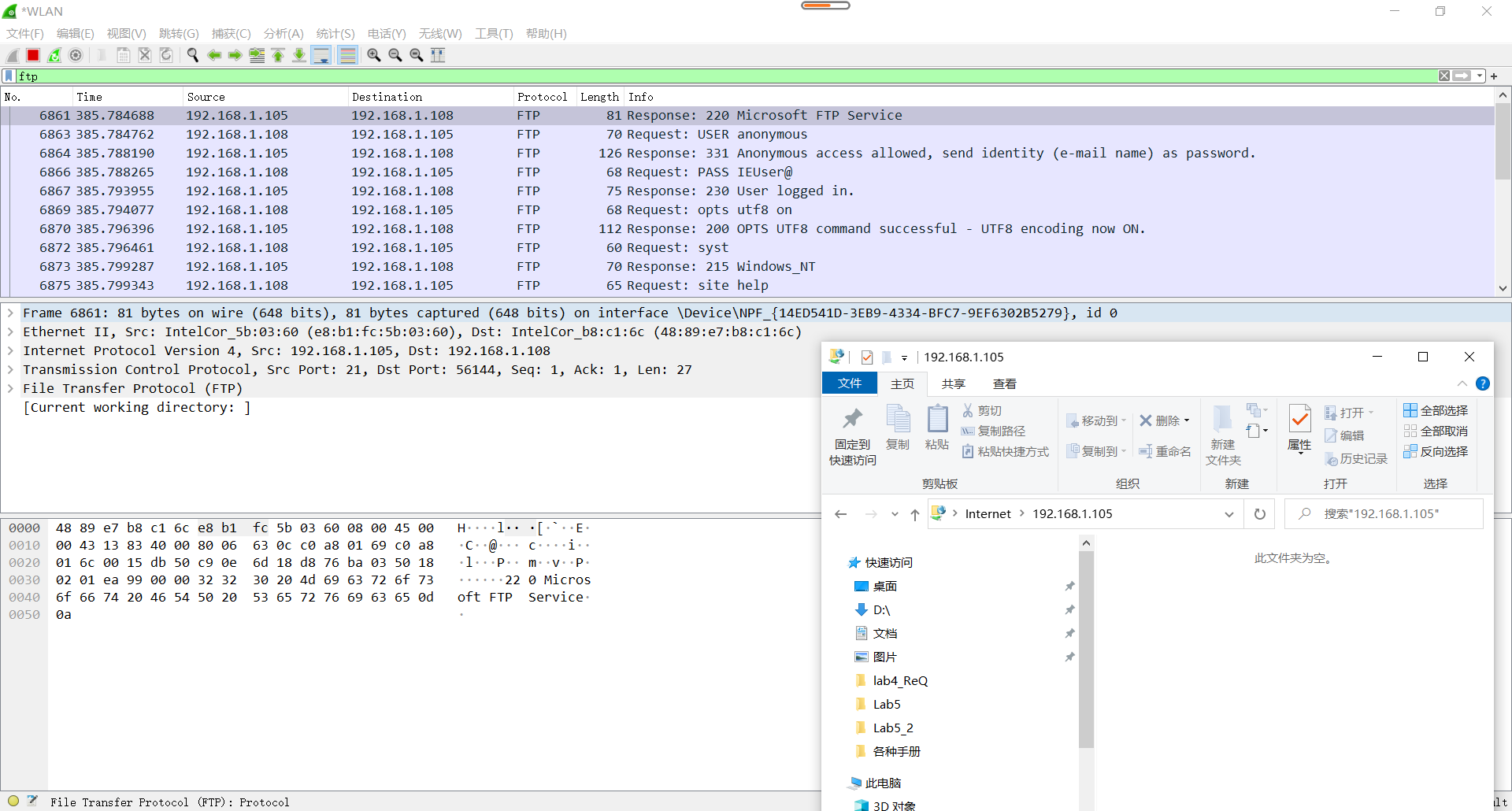
编程语言: C++

# 实验结果

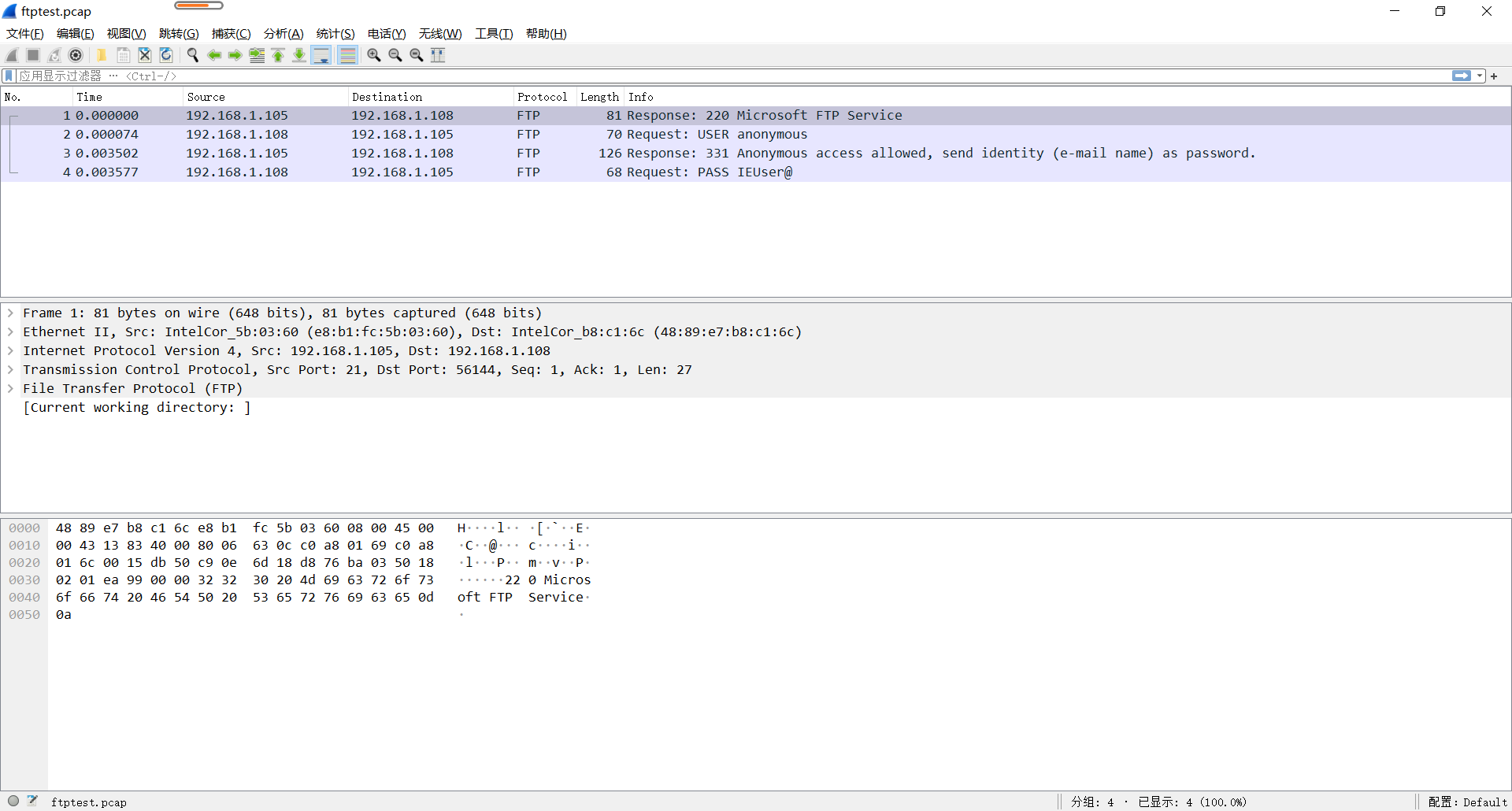
自行搭建ftp：



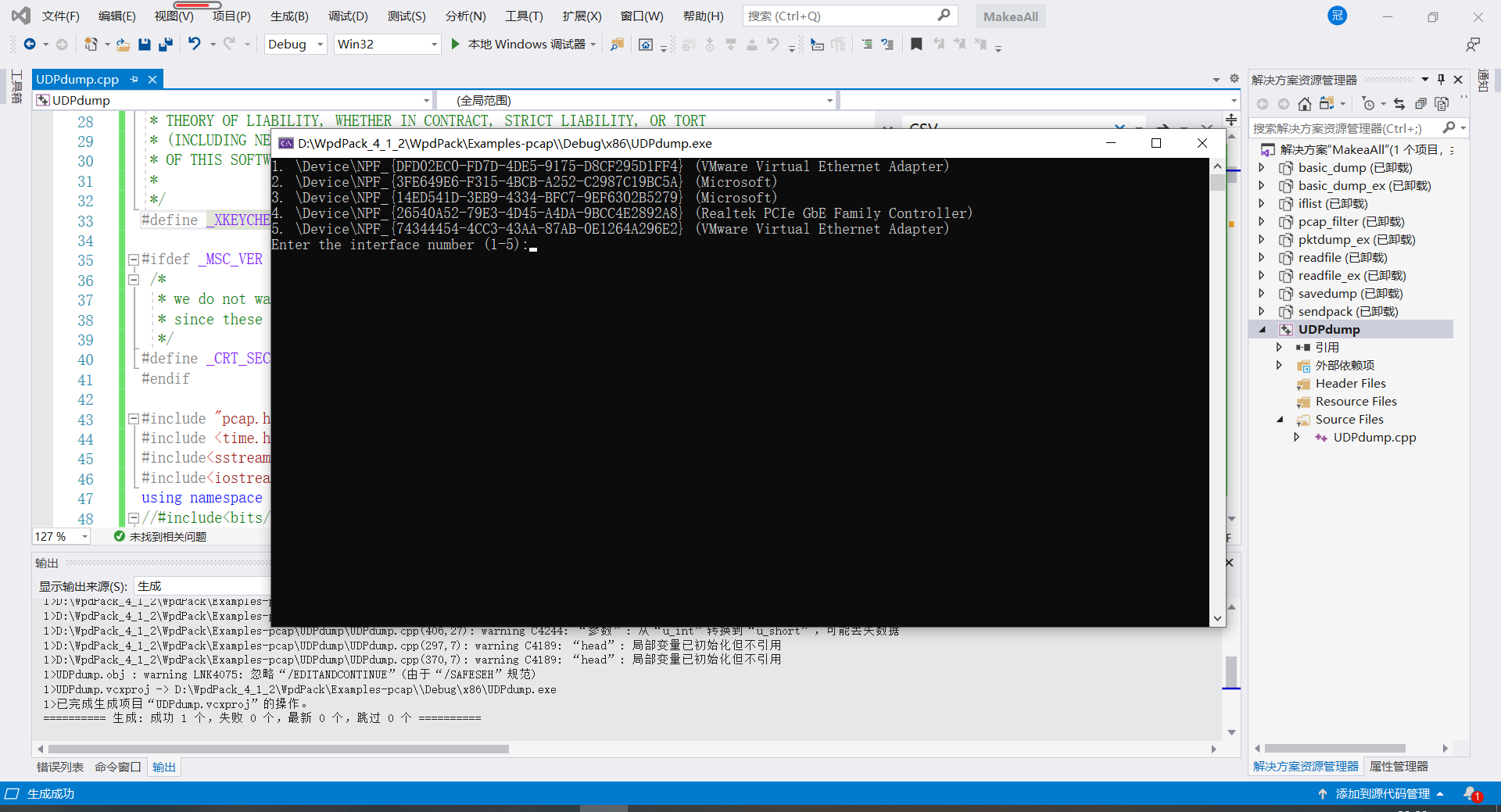
用 Wireshark 观察网络流量并辅助网络侦听，以下为监听记录：



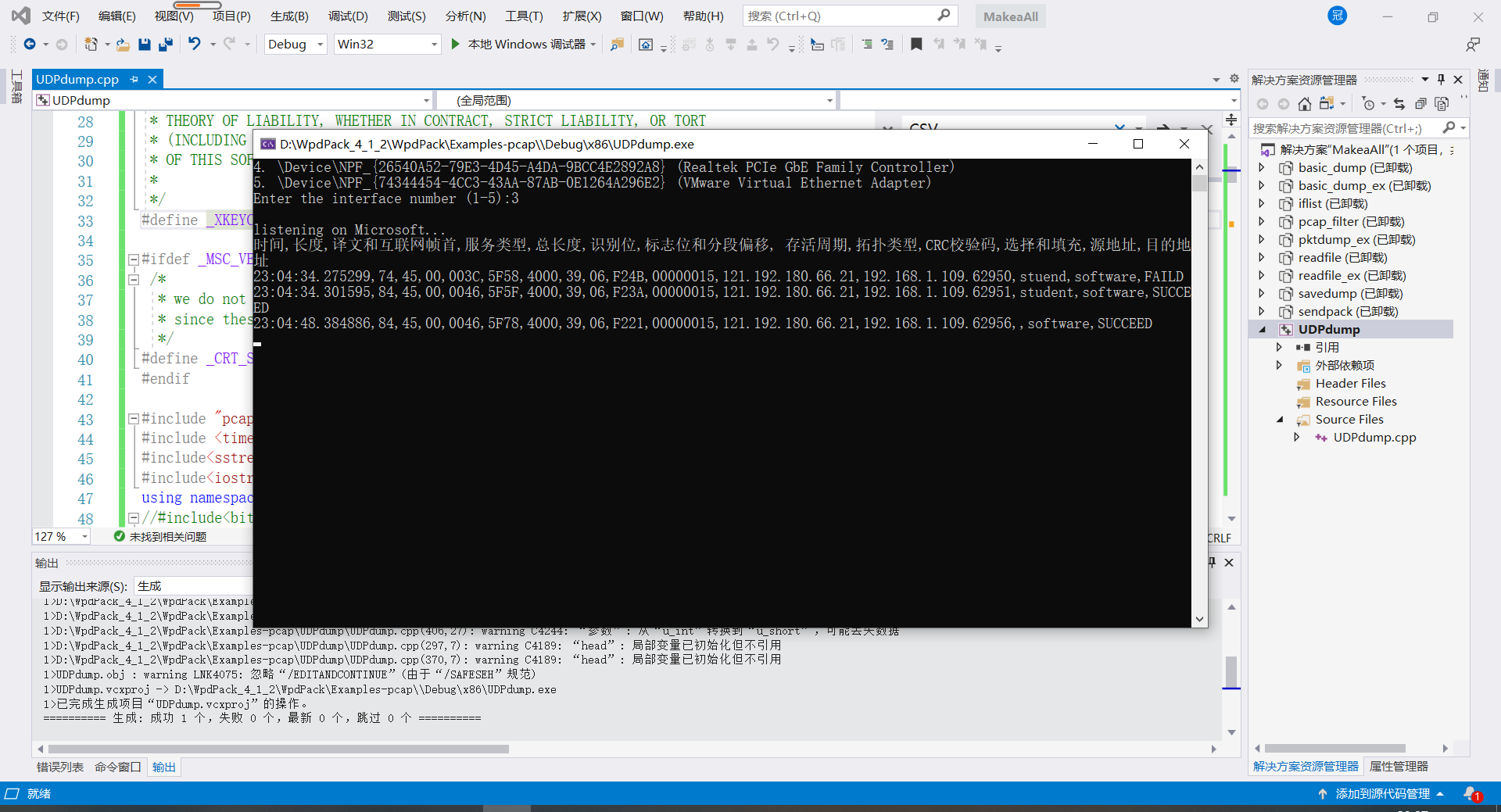
以下为仅查看ftp的记录：



进入选择网卡并利用WinPcap 库侦听并处理以太网帧和 IP 报文：



对ftp进行操作后通过程序解码得到监听结果



# 实验代码

本次实验的代码已上传于以下代码仓库：

<https://github.com/Yukinoshita-Yukinoml/Computer-Network.git>

# 实验总结

1. 在屏蔽了网络连接后ping其他同学自建的ftp时会监听到流量，但是仍然会收到其他流量，该问题还不知道原因。

待续…