

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三　基于 PCAP 库侦听并分析网络流量**

**班　　级 软件工程2019级1班**

**姓　　名 雷鸿宇**

**学　　号 22920192204173**

**实验时间 2021年3月28日**

**2021 年 3 月 28 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. 应将材料清单上传在代码托管平台上；
5. 在学期最后一节课前按要求打包发送至cni21@qq.com。

# 实验目的

# 通过完成实验，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。

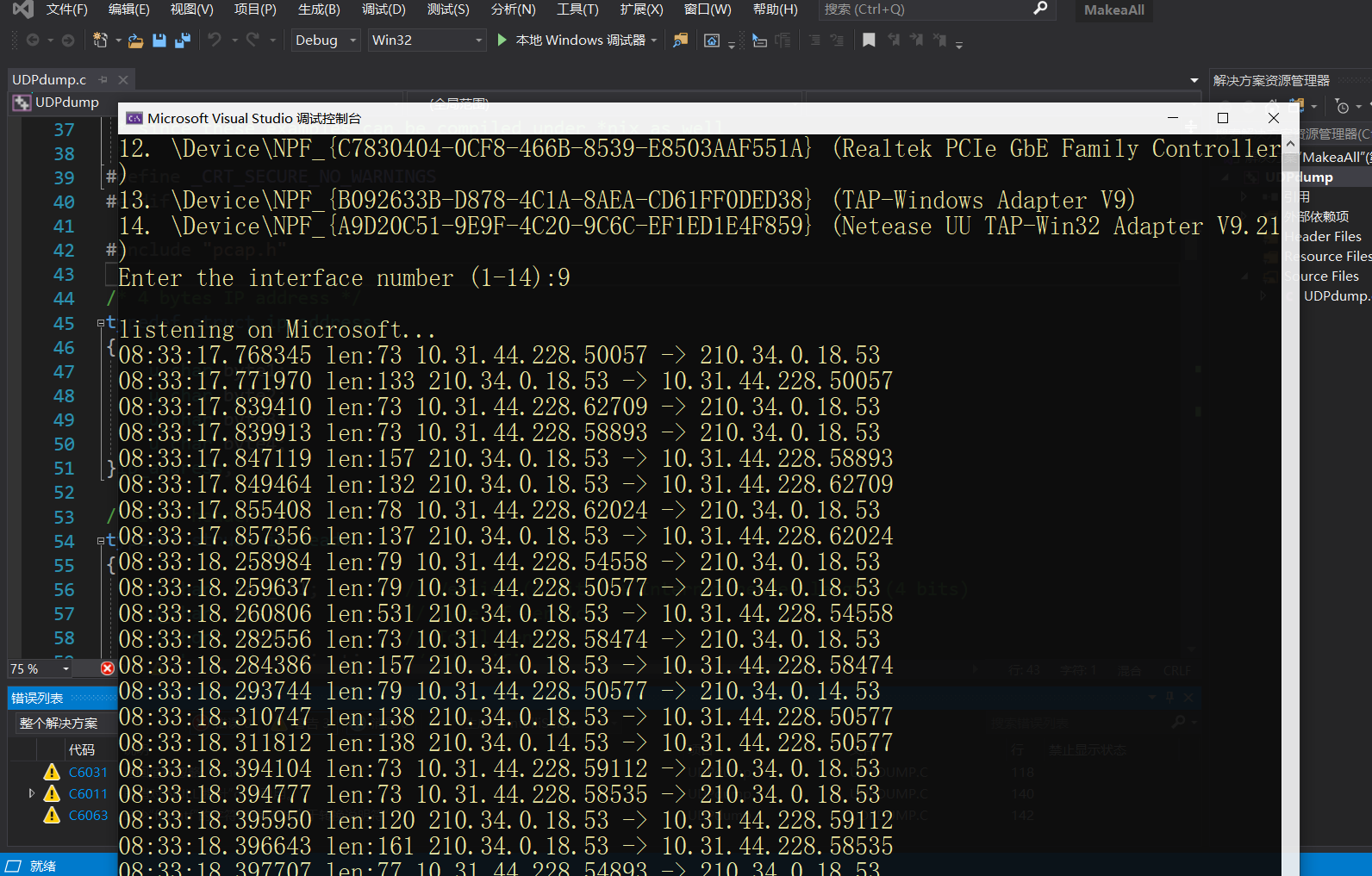
# 实验环境

Windows 10、 Winpcap、 Wireshark

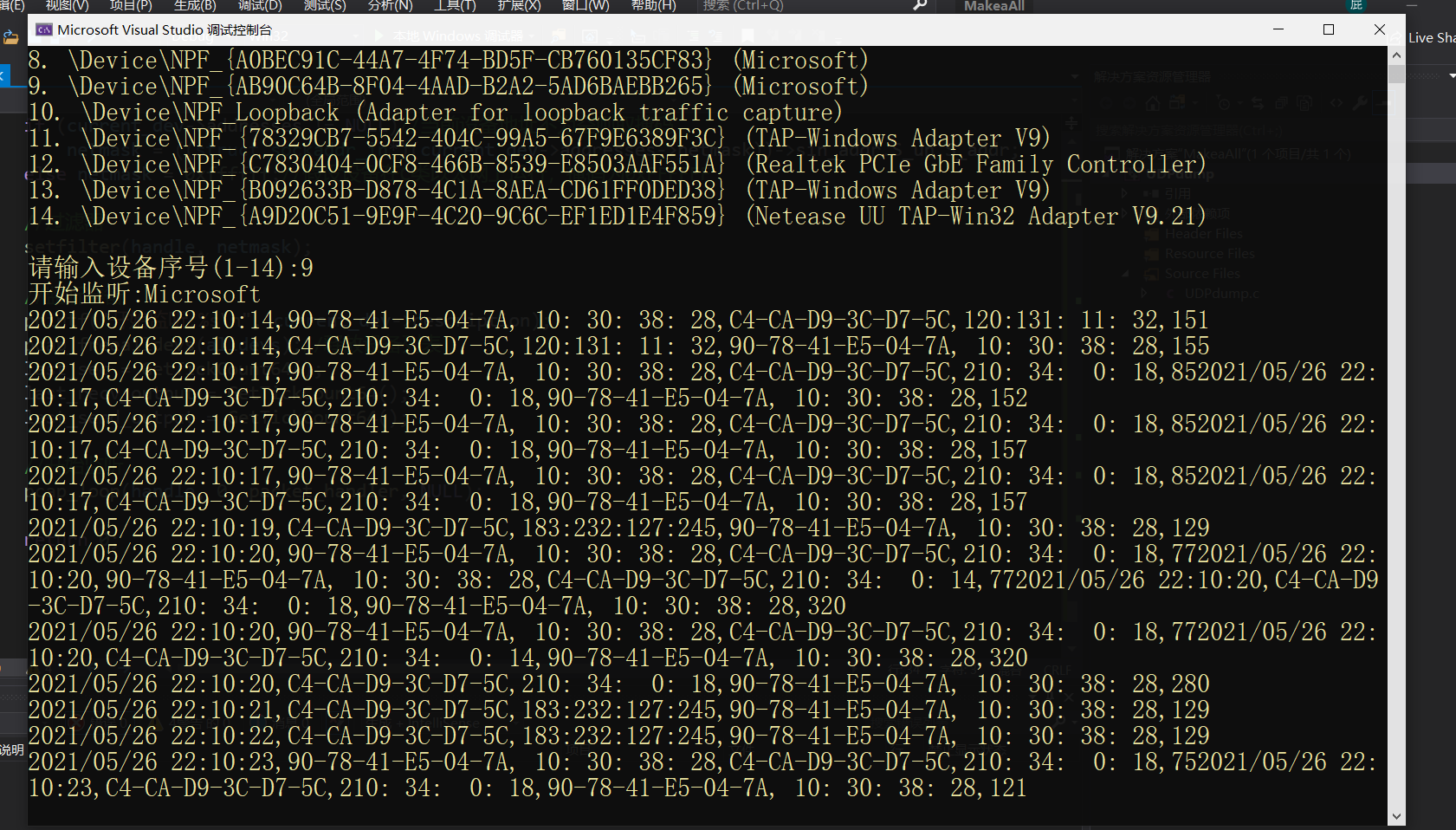
编程语言：c

# 实验结果

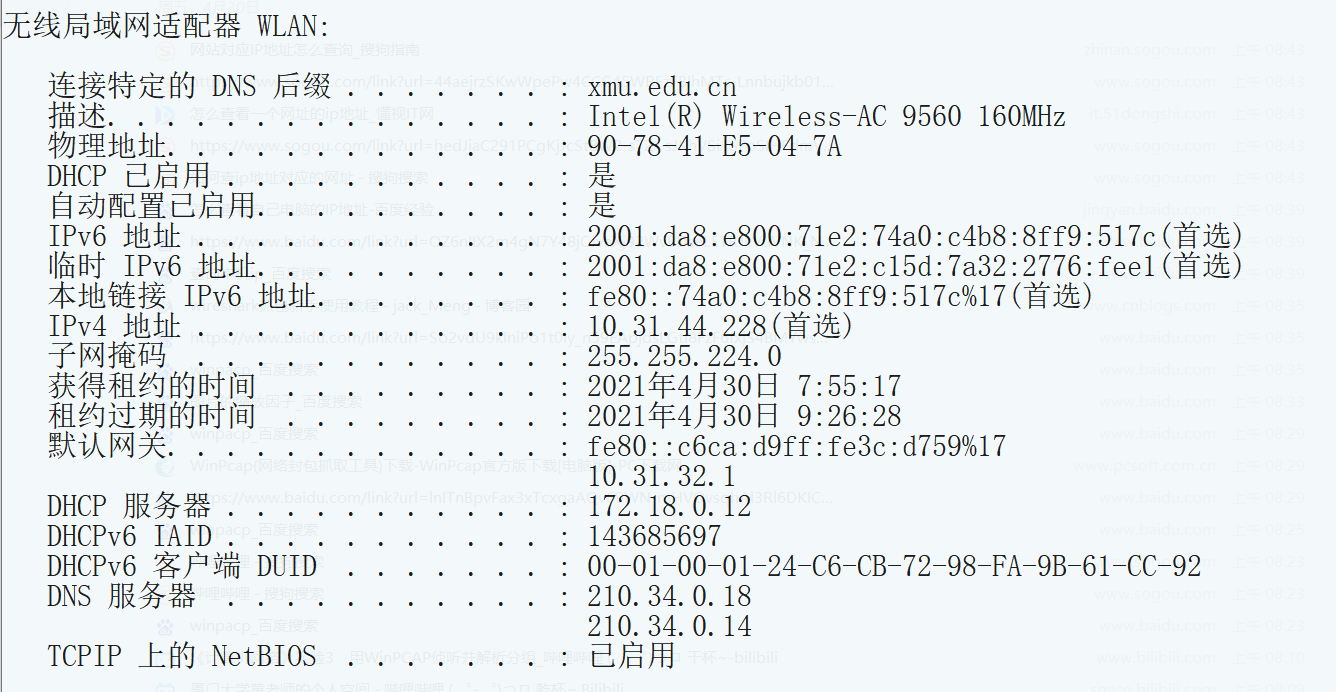
# 下载并配置好winpacp，运行源代码



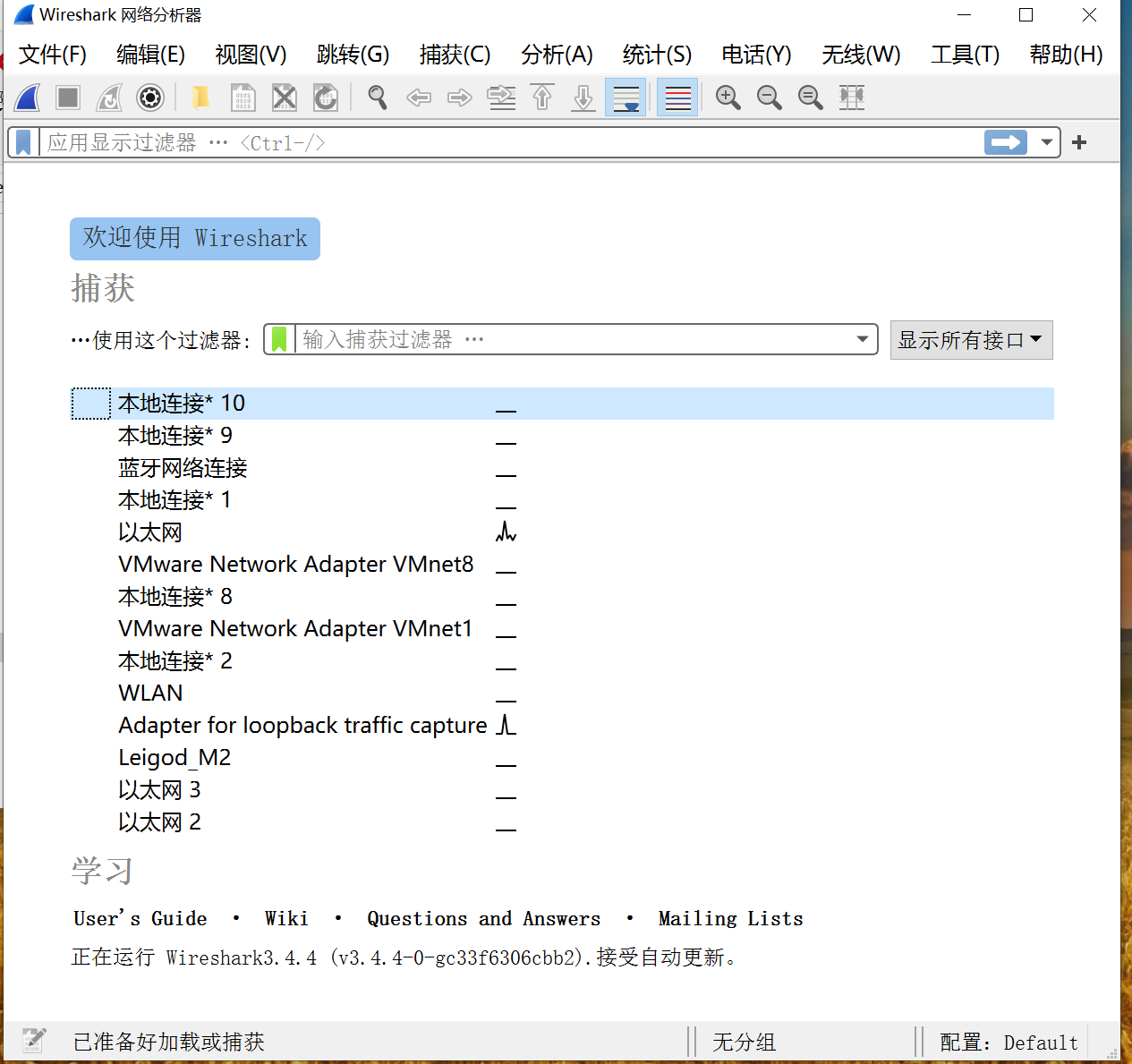
修改代码，让其额外显示源MAC、目的MAC以及帧长度等信息



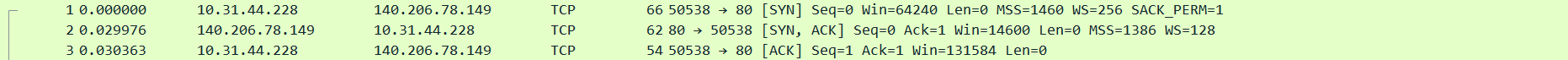
使用wireshark前，先ipconfig本机的网络信息



安装wireshark，观察相关界面

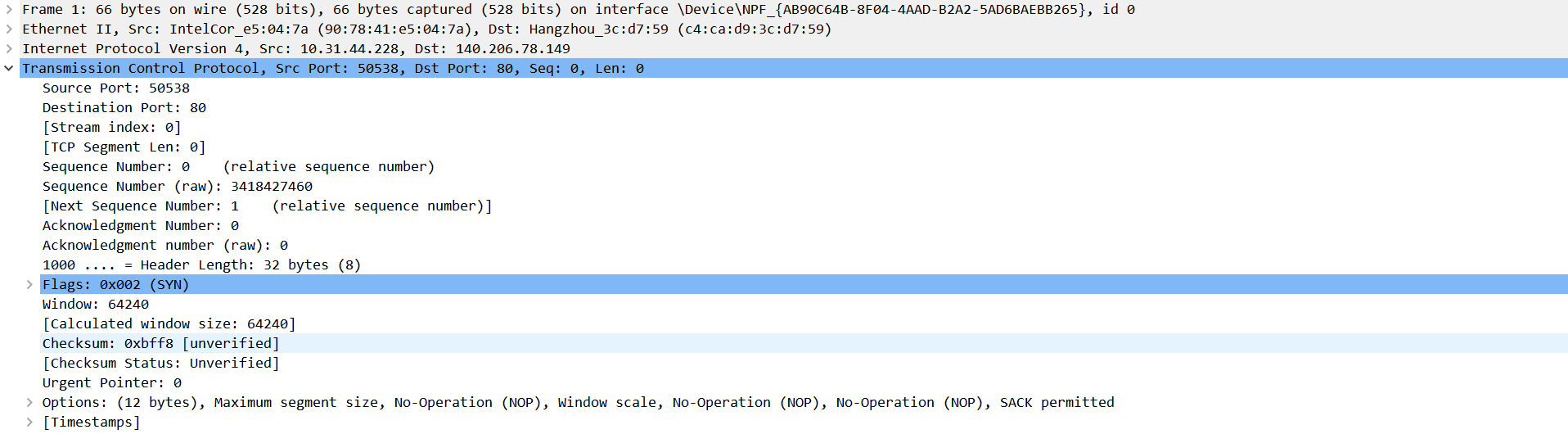


观察到一个TCP连接的三次握手

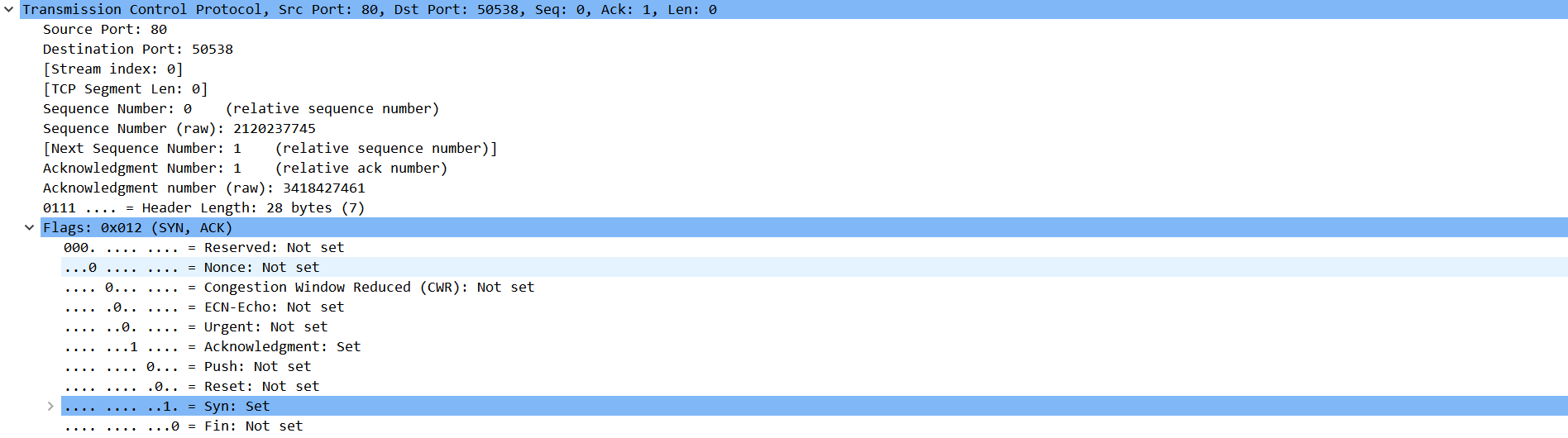


点击查看每一项的详细信息

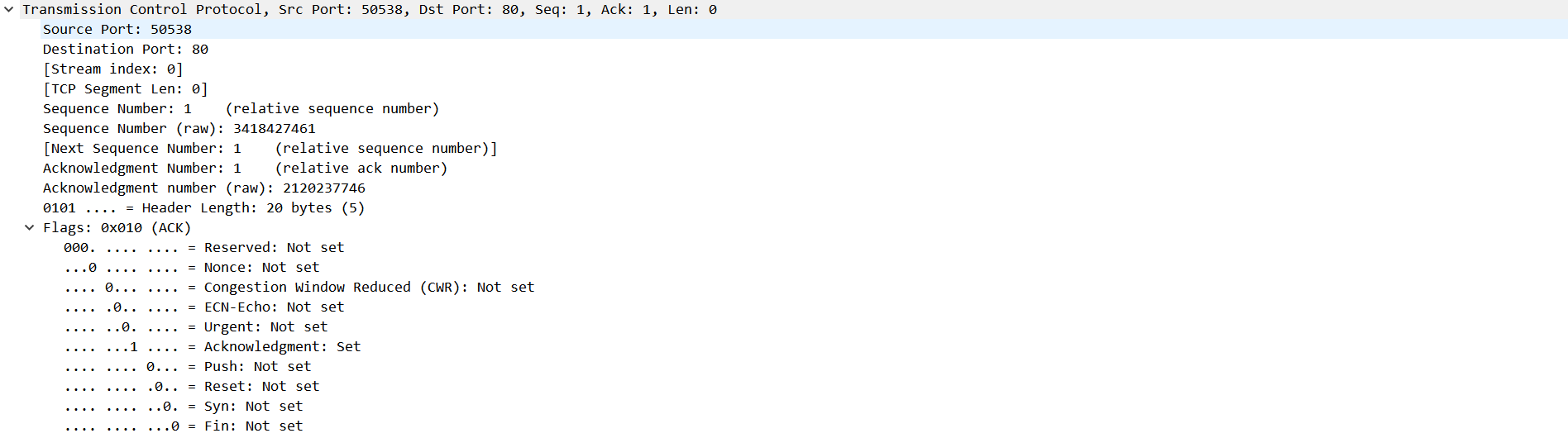
第一次握手



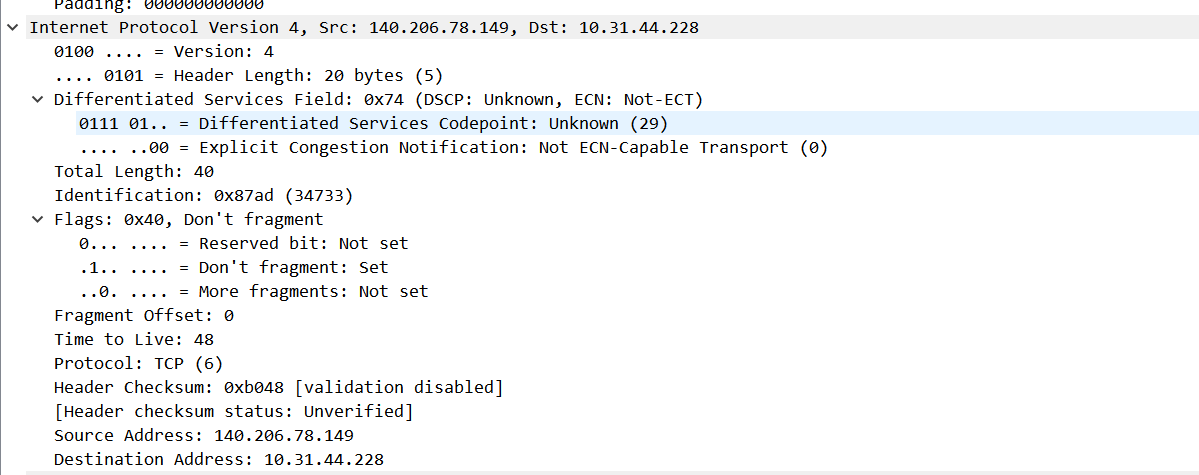
第二次握手



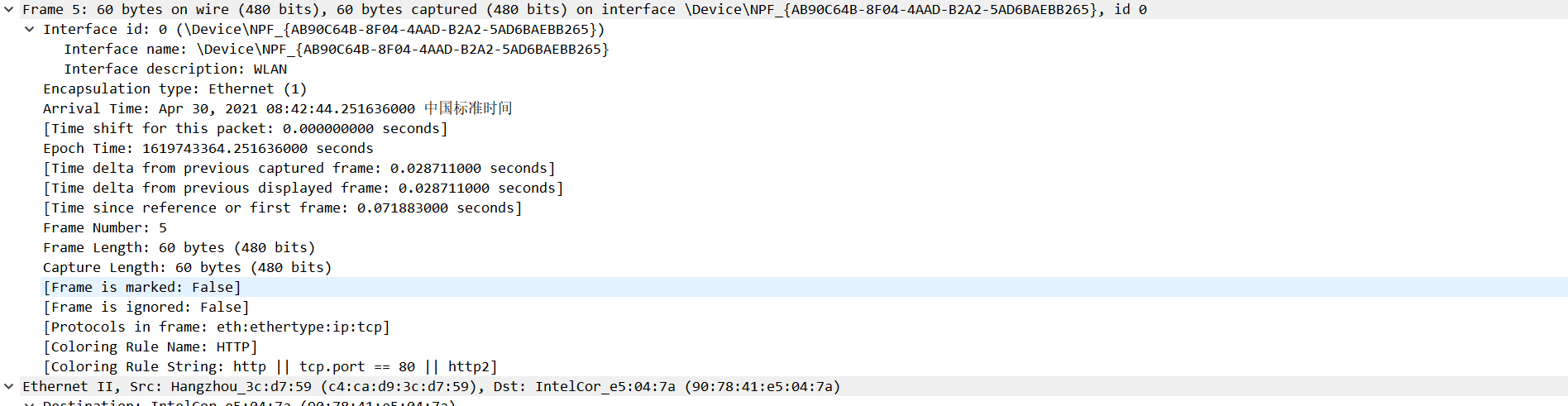
第三次握手（flags下可以看到个标记的值）



观察一个ip报文（可以看到版本、头长度、是否分片、源地址、目的地址等信息）



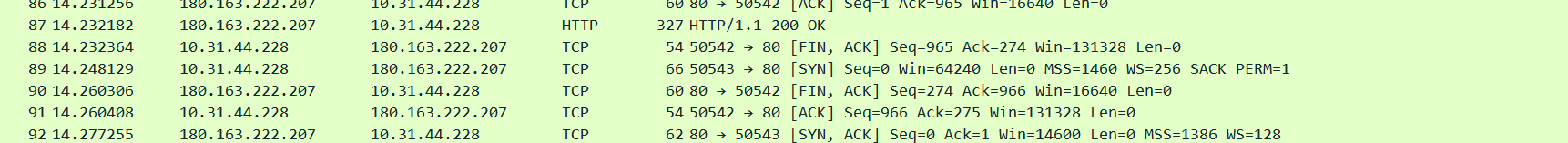
帧分析器（60字节）



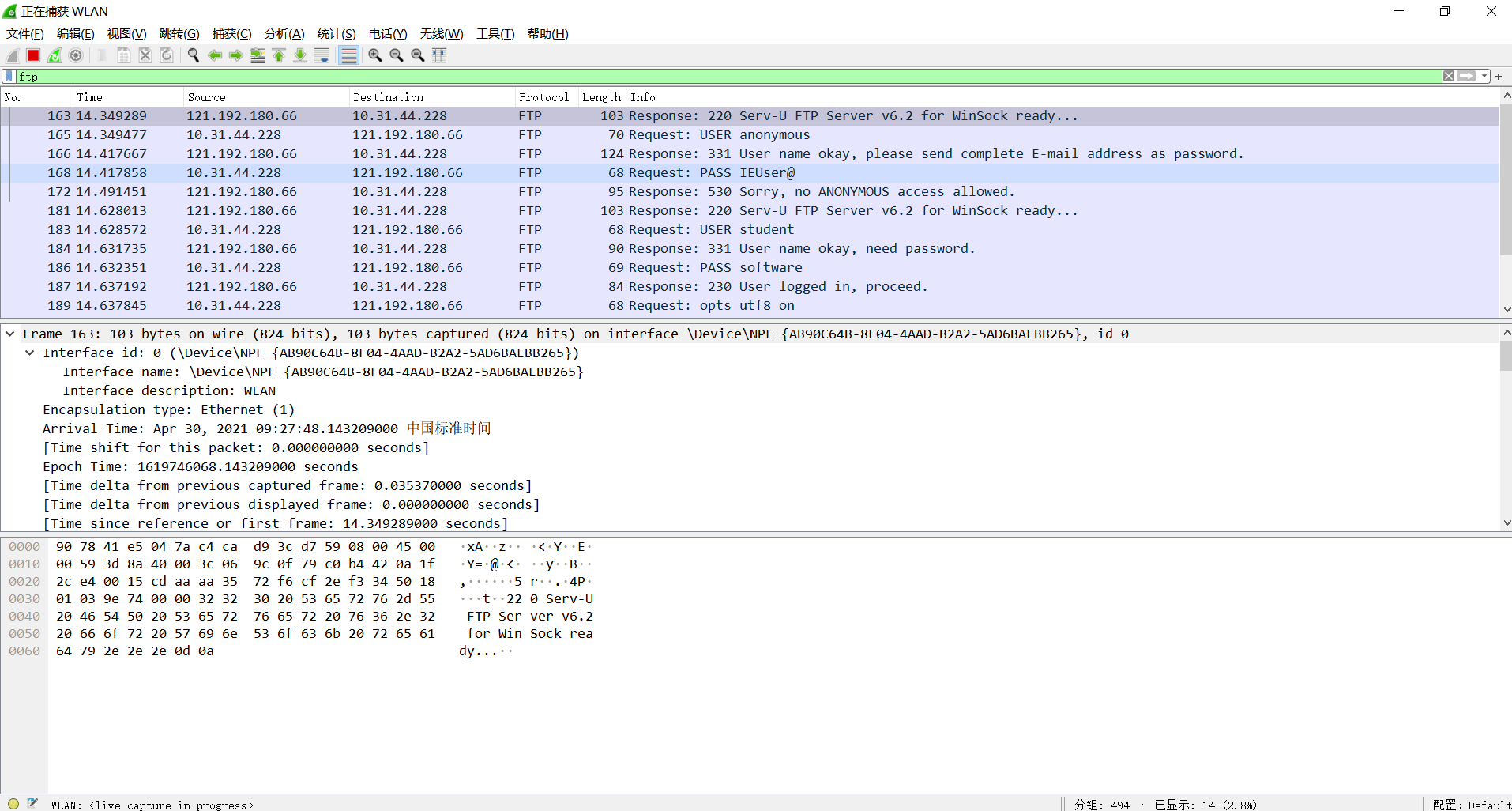
查看具体内容（16进制表示，winpacp也可以进行类似操作）



四次挥手



进入ftp（这里使用了学院的ftp，很抱歉占用相关资源，可以看到530、230等回应）



# 实验代码

本次实验的代码已上传于以下代码仓库：https://github.com/leipipi

# 实验总结

本次实验使用wireshark和winpacp配合，观察了网络流量，并加深了对以太网帧、 IP 报文、 TCP段和 FTP 命令的格式的理解 ，真实看到了TCP三次握手和四次挥手的过程，以及登入ftp的整个传输过程，最后，初步了解了网络编程的一些相关操作。