

****

软 件 学 院

《计算机网络》实验报告

**题　　目 用 WinPCAP 监听并分析以太网的帧**

**姓　　名 陈澄**

**学　　号 32420212202930**

**班　　级 软工三班**

**实验时间 2023.04.07**

**2023 年 04 月 07 日**

# 实验目的

通过捕获并分析以太网帧，分析常见数据包的帧格式，熟悉以太网中常用协议及其报文

格式，如 ARP、ICMP、IP 协议。

学会对捕获到的数据帧按指定的条件进行过滤，为网络流量深入分析做基础。所谓的指定条件可包含：指定的目的 IP 地址、指定的源 IP 地址、指定的协议类型等（参考 Wireshark

的过滤条件），比如当指定协议类型为 IP 时，其它类型的数据帧将被丢弃，仅留下 IP 数据 帧。

# 实验环境

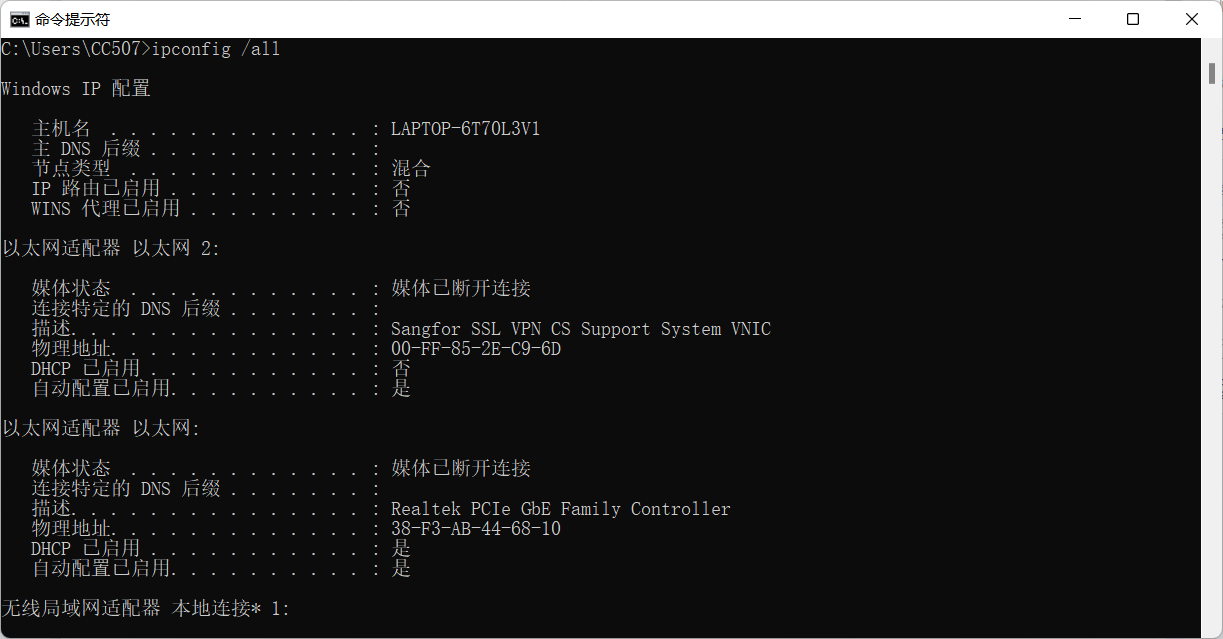
操作系统：Windows10

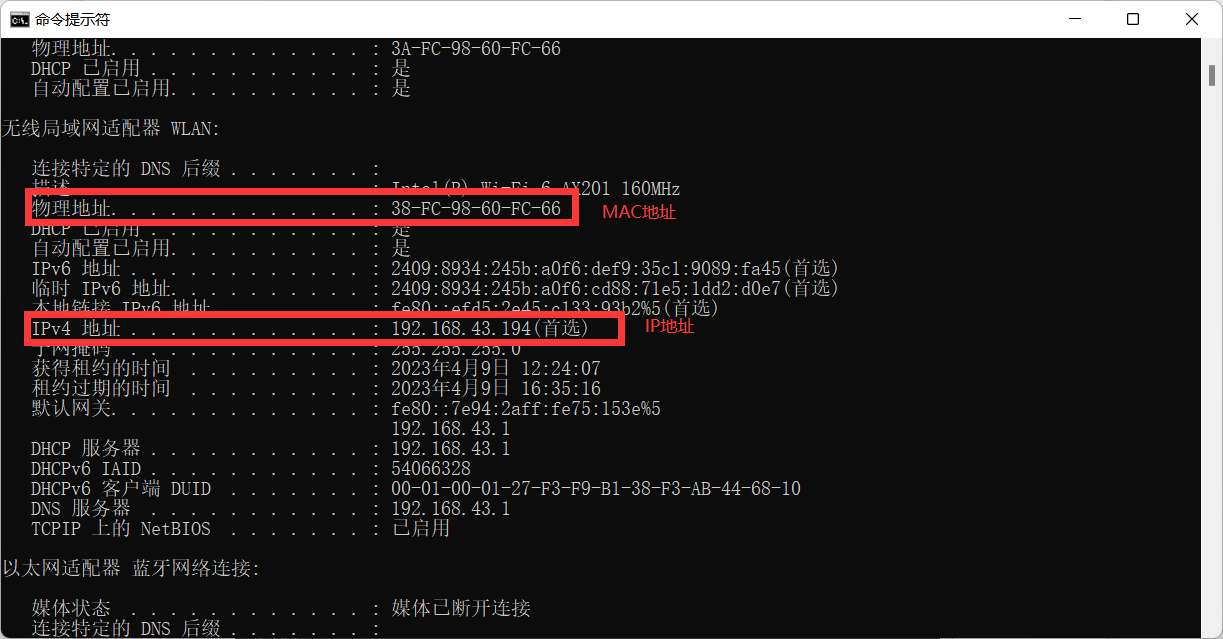
编程语言：C++

IDE：VS2020

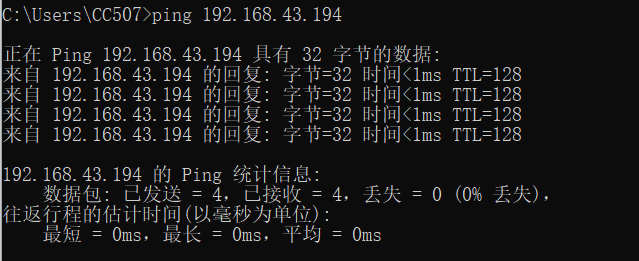
# 实验结果

1.使用 Windows 自带 的“命令提示符”或 “PowerShell”完成本 机 IP、MAC 地址等 信息的查询工作

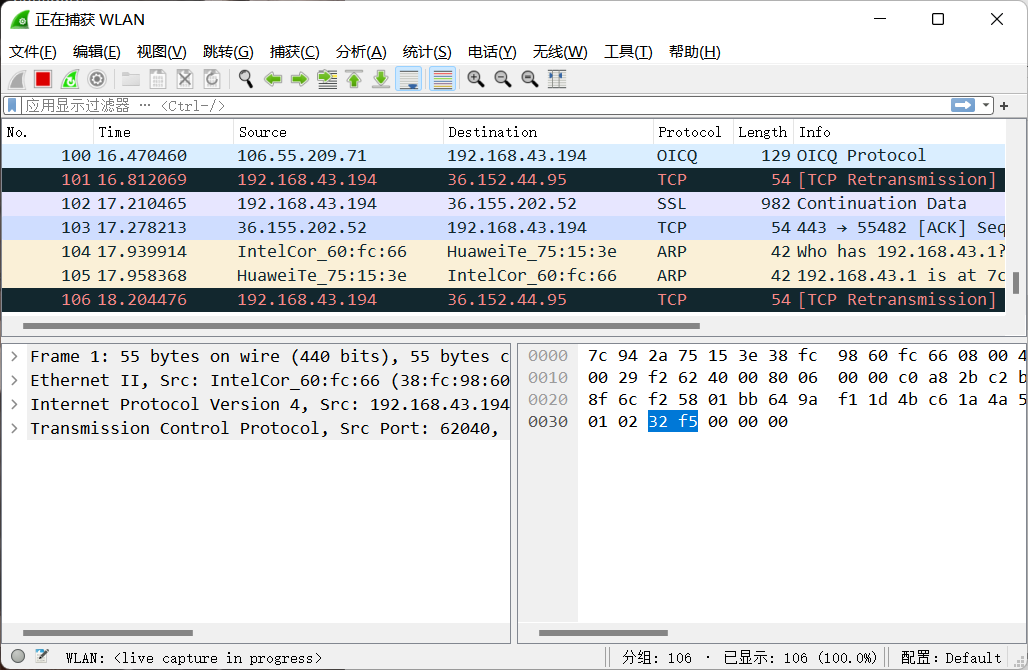




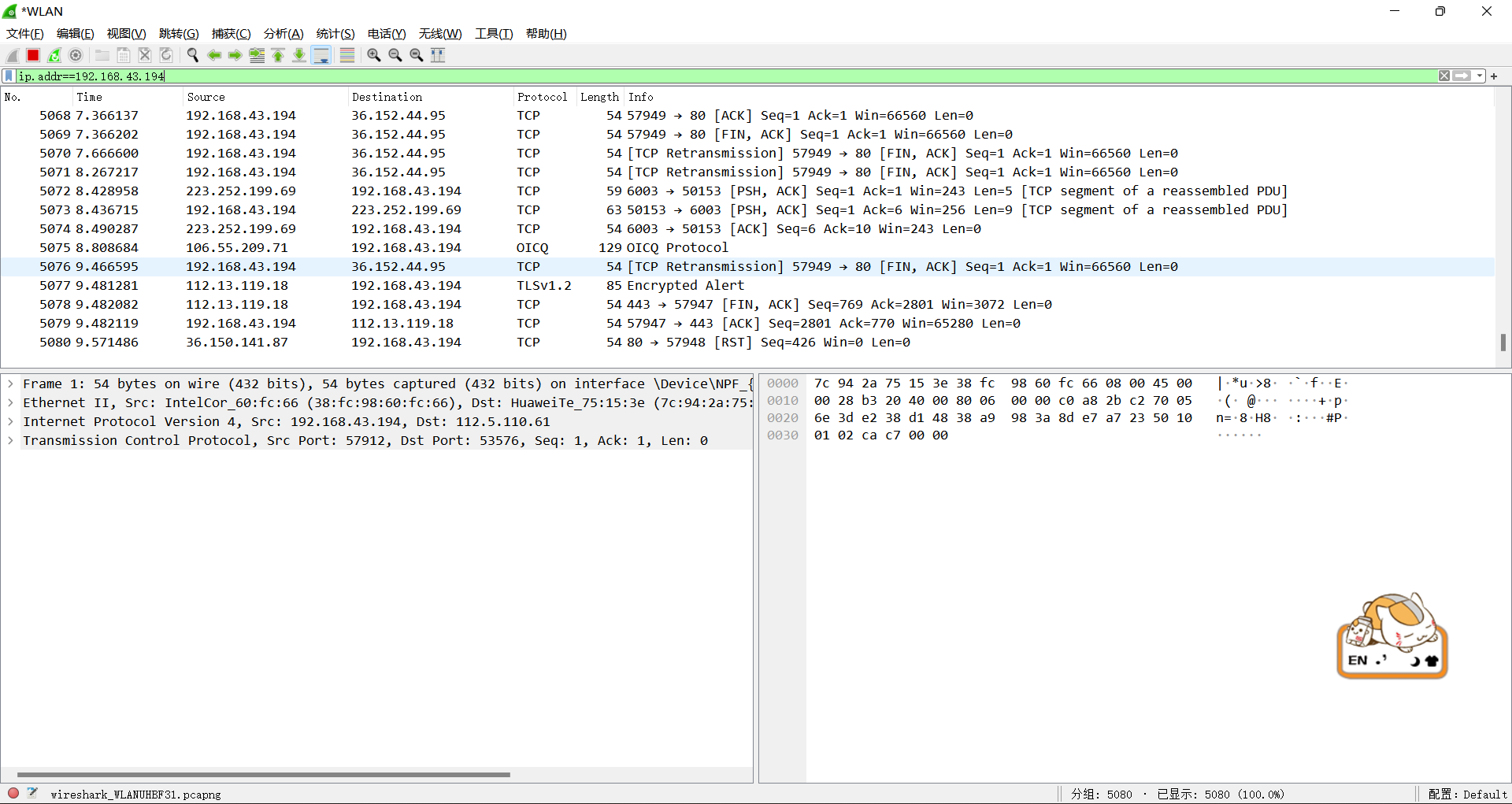
1. 使用 Windows 自带的“命令提示符”或 “PowerShell” 完成“本机与具有某个 IP 的主机是否连通”的检测



1. 熟悉 Wireshark 的使用，会设置过滤条件，如过滤出指定 IP的数据帧

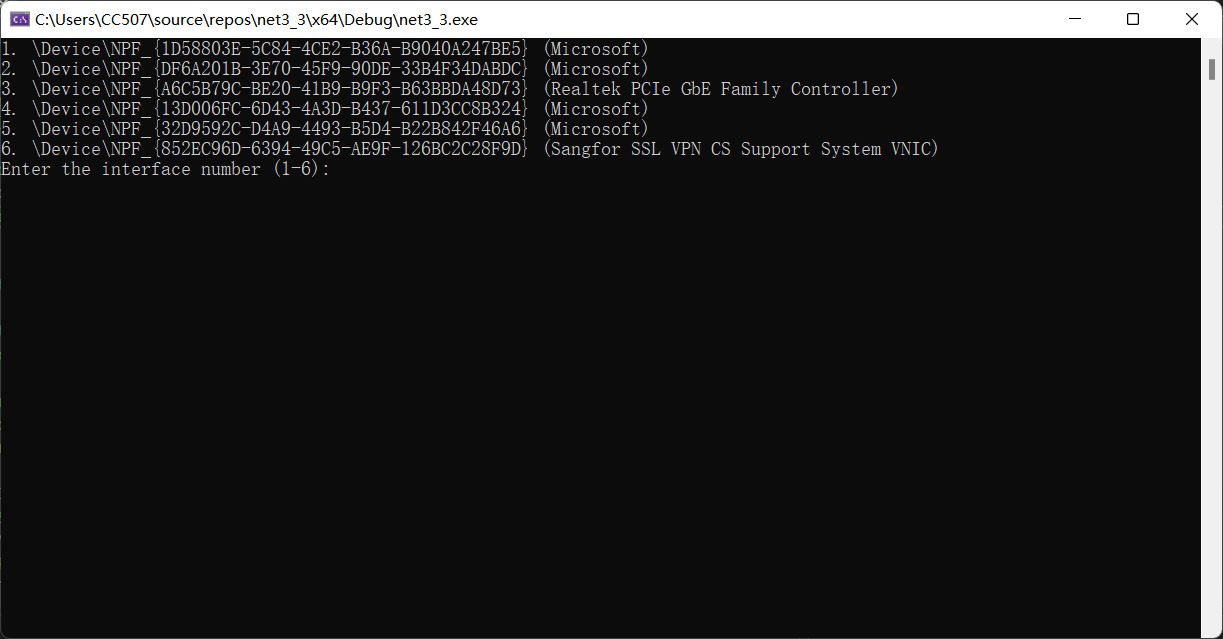


得出源IP地址为192.168.43.194的数据包

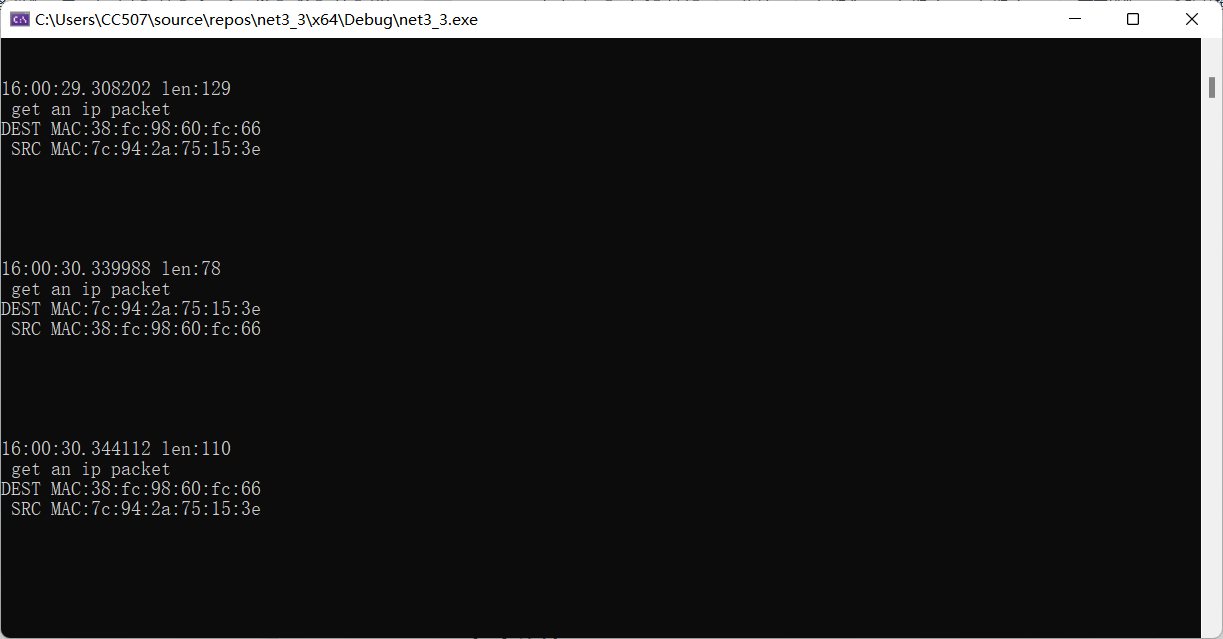


1. 配置好实验环境，在控制台打印出网卡设备列表，捕获到以太网帧，并能 够 解 析 出 目 的MAC、源 MAC

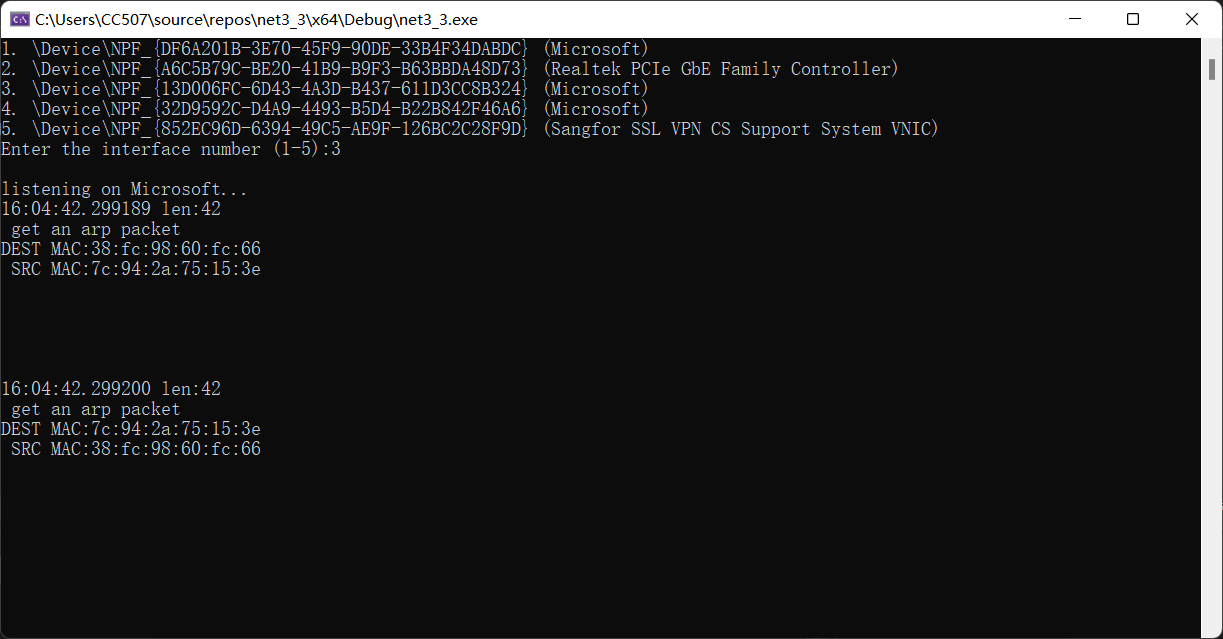
网卡设备列表



捕获到以太网帧，并能 够 解 析 出 目 的MAC、源 MAC，图中DESC为目的MAC，SRC为源MAC

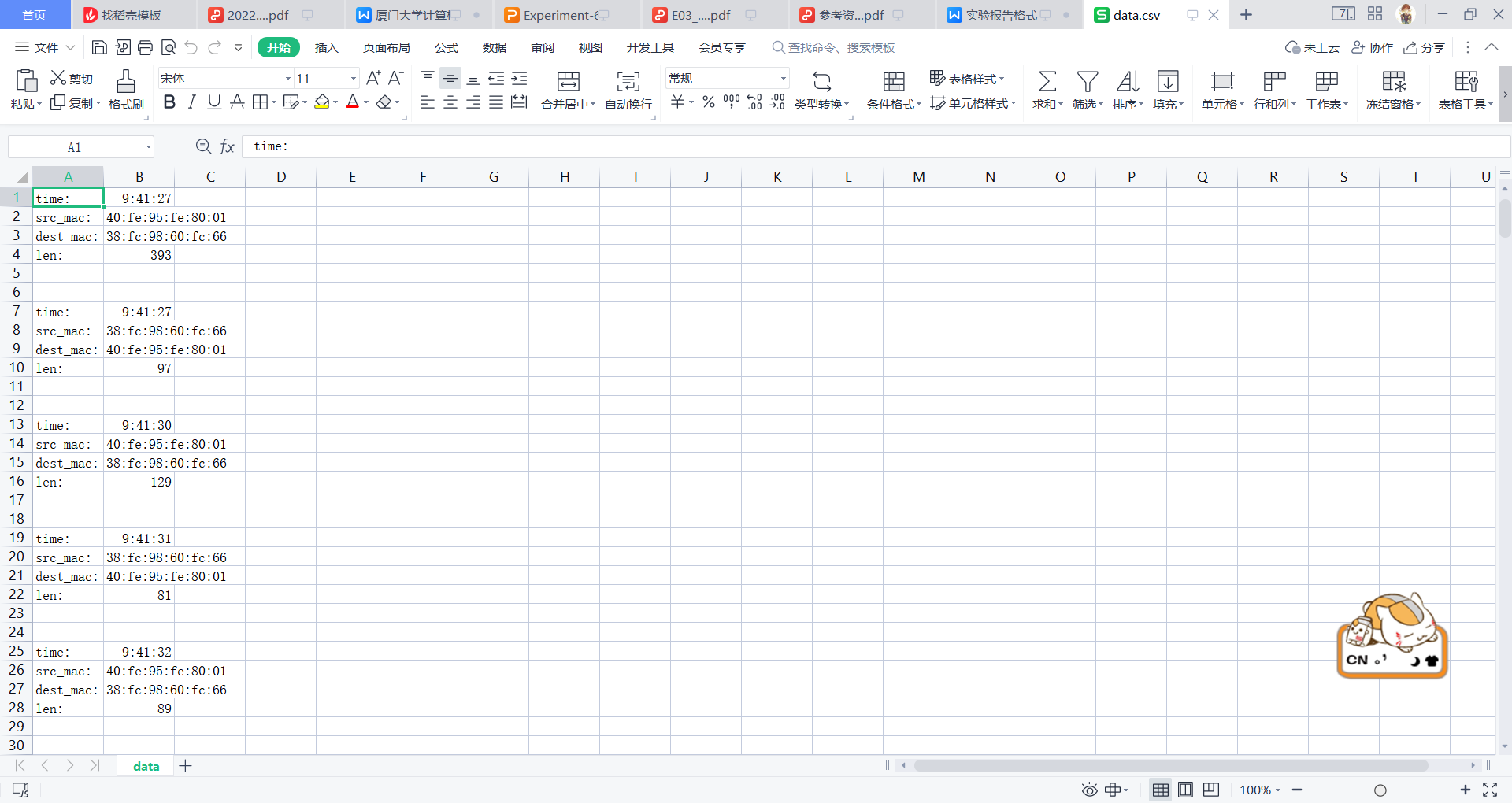


1. 能够过滤出特定类型的数据包，指定类型的为 ARP，ICMP 等



6.能够将捕获到的帧保存到 CSV 文件中，包含：时间、源MAC、源IP、目标 MAC、目标 IP、帧长度（以逗号间隔）





# 4实验总结

学会了通过使用WinPCAP去监视传输协议、数据包大小和流量，并对数据包进行详细的分析和解码。

学会了在Wireshark中设置捕获过滤器，以便只捕获发送到特定MAC地址的帧。

学会了使用pcap库和其下的函数进行变成实现以太网帧的捕获，并解析其长度，目的地址，源地址。以及学会了如何对其类型进行筛选，以及对捕获结果的保存。