

****

软 件 学 院

《计算机网络》实验报告

**题　　目 捕获并分析帧和IP报文**

**姓　　名 陈奕培**

**学　　号 22920202202879**

**班　　级 计网2班**

**实验时间 2022/4/1**

**2022 年 4 月 1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，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：win11

IDE：VS2019

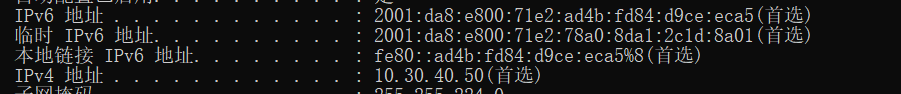
编程语言：C++

# 实验结果

**-2.查询本机IP地址和MAC地址**

打开cmd终端，运行ipconfig/all指令

IP地址：

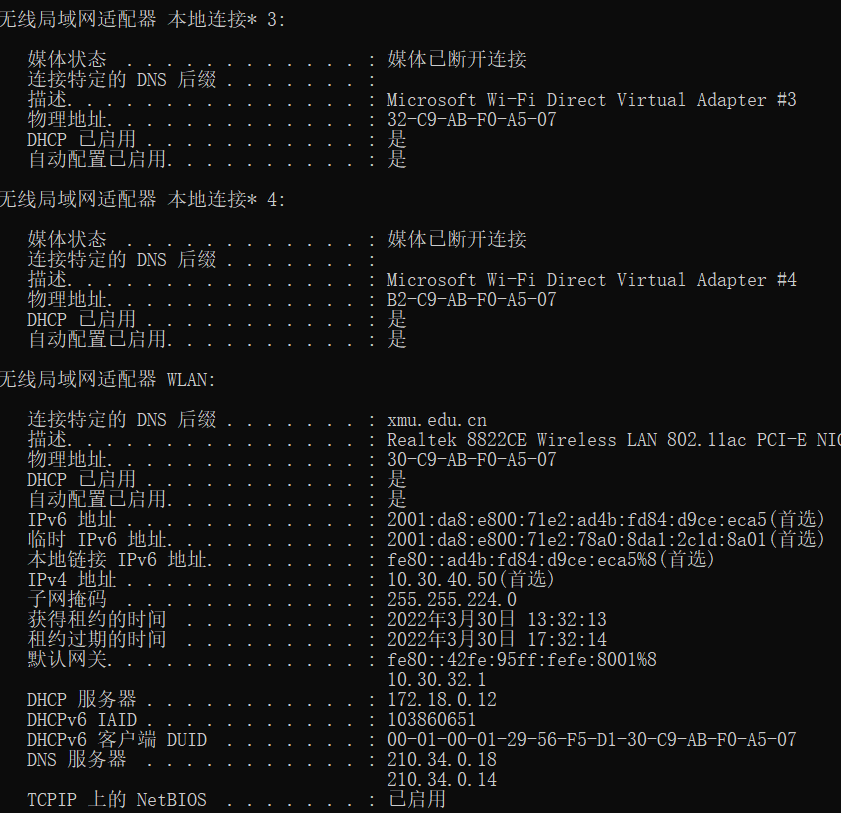


MAC地址：

本地连接\*3：32-C9-AB-F0-A5-07

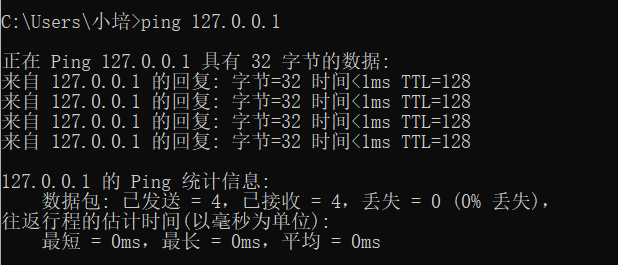
本地连接\*4：B2-C9-AB-F0-A5-07

WLAN：30-C9-AB-F0-A5-07

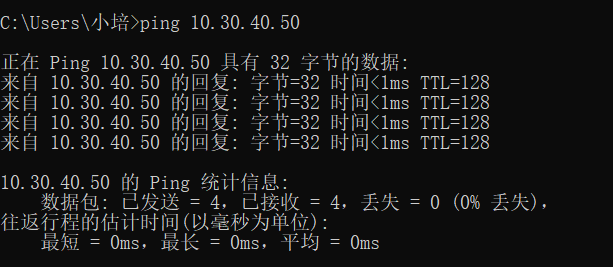


**-1.查看与某个IP是否连通**

Ping 127.0.0.1

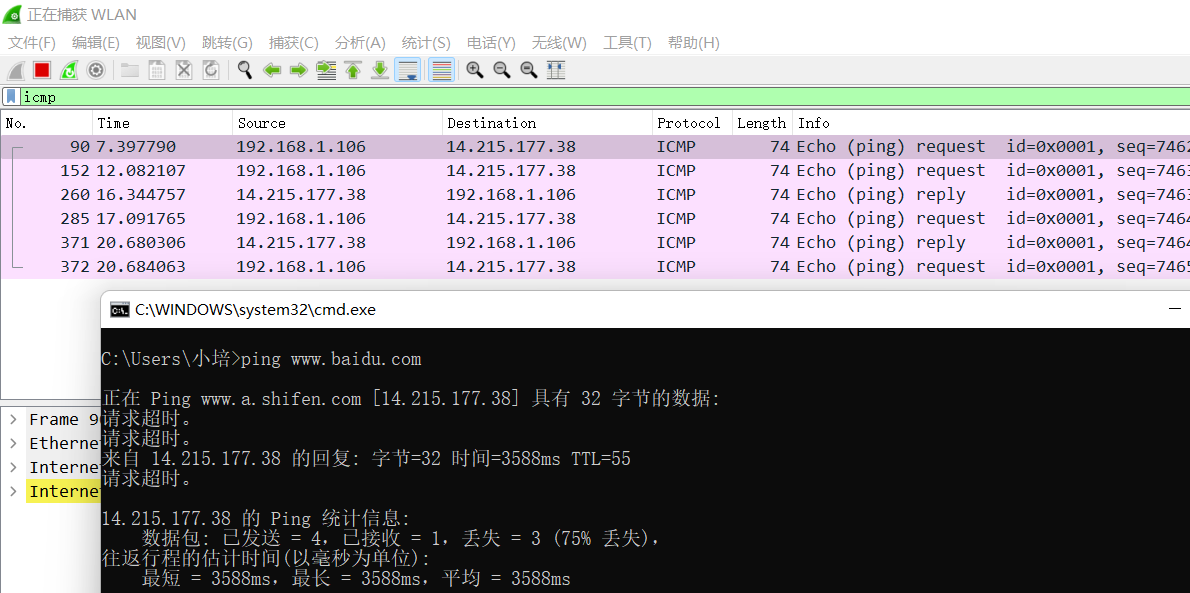


Ping 10.30.40.50（本机）

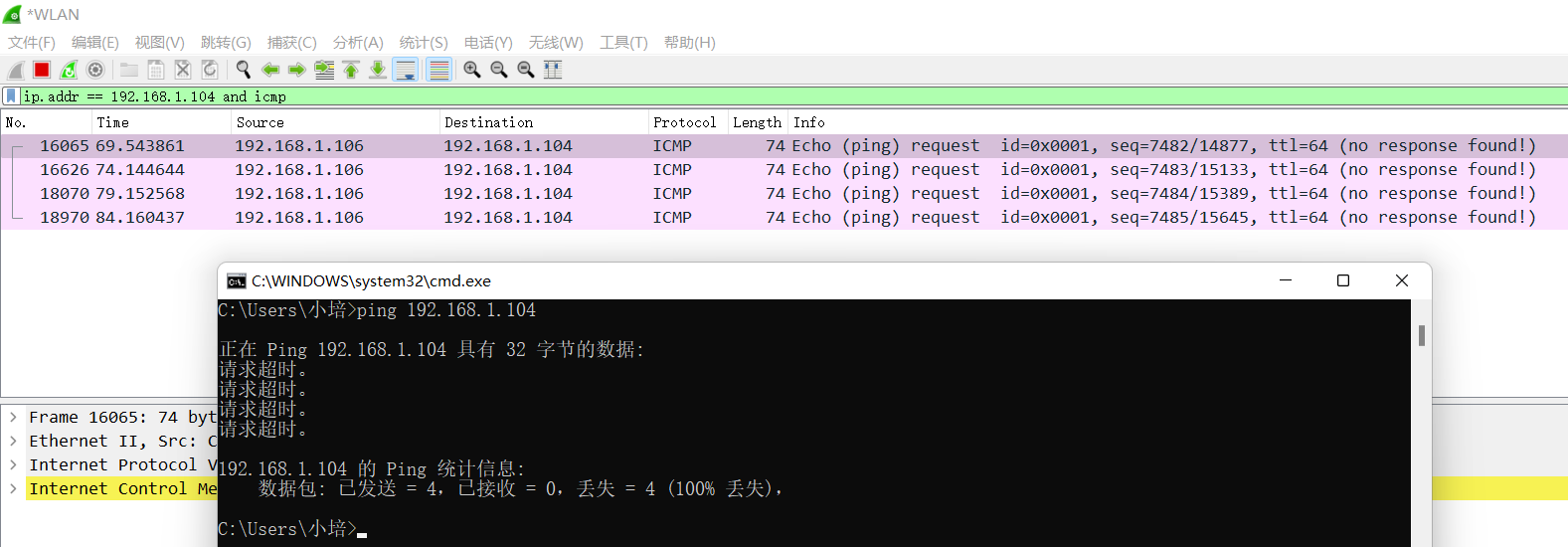


0. 熟悉 Wireshark 的使用

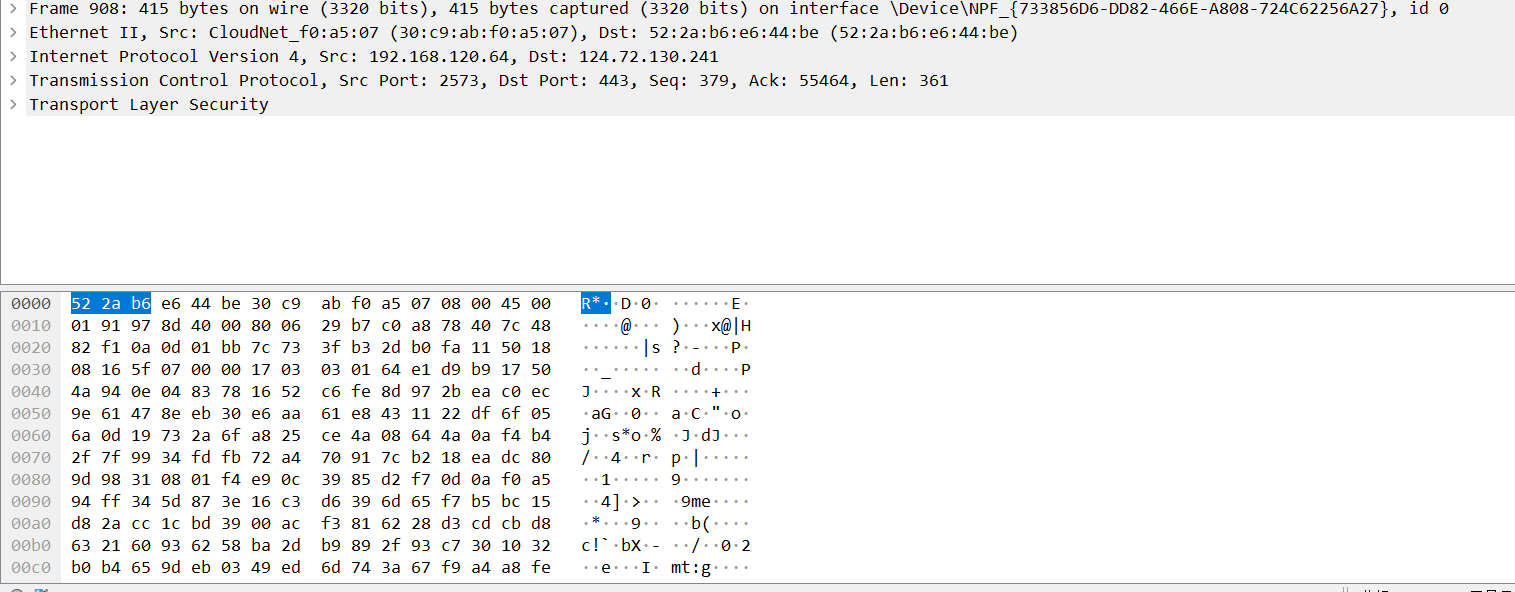
抓取ICMP协议数据包



Ping 192.168.1.104，并抓取错误信息



单击查看某一条



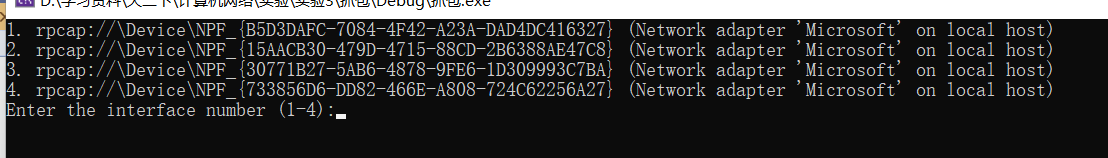
1.配置环境，打印网卡

安装WinPacp

解压出WpdPack文件夹，将include和lib中的文件加入vs的vc文件夹中

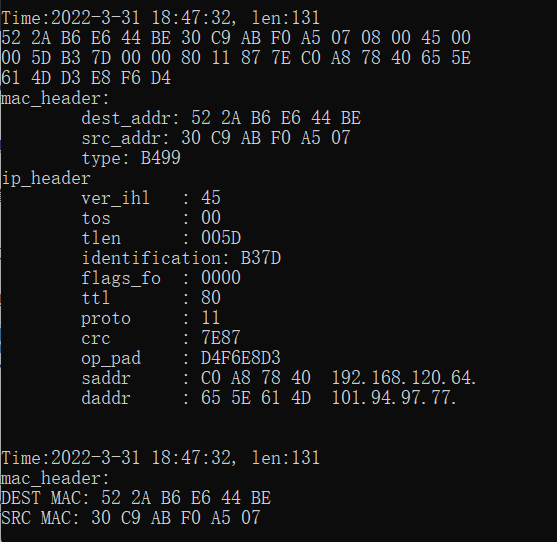
新建C++项目，在设置里面配置静态链接

运行代码并打印



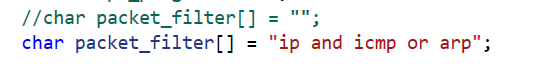
2.捕获帧，并解析出目的MAC、源MAC

详细消息and简约消息

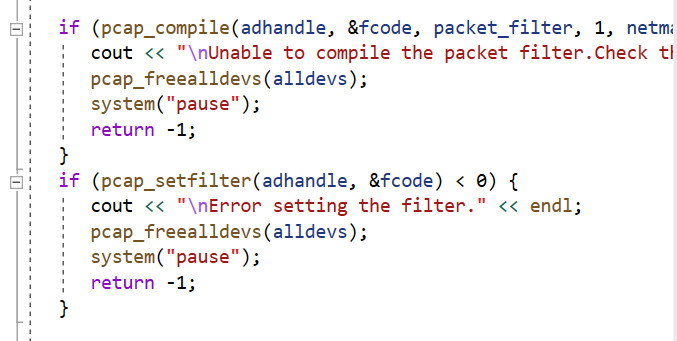


3.过滤出特定类型的数据包

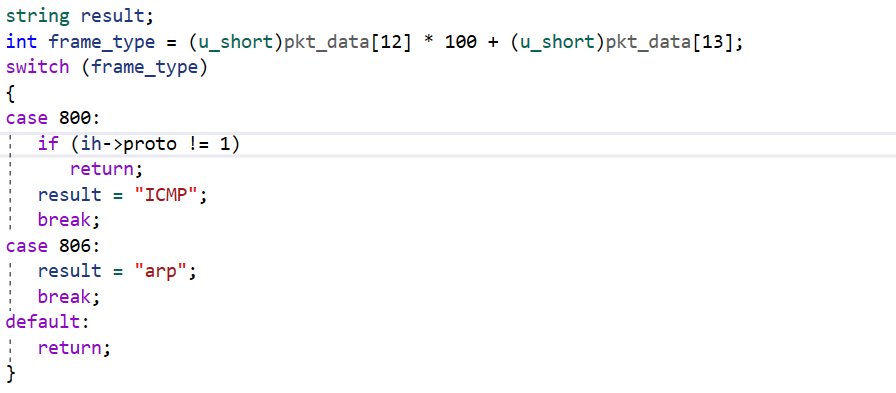
设置过滤类型的数组



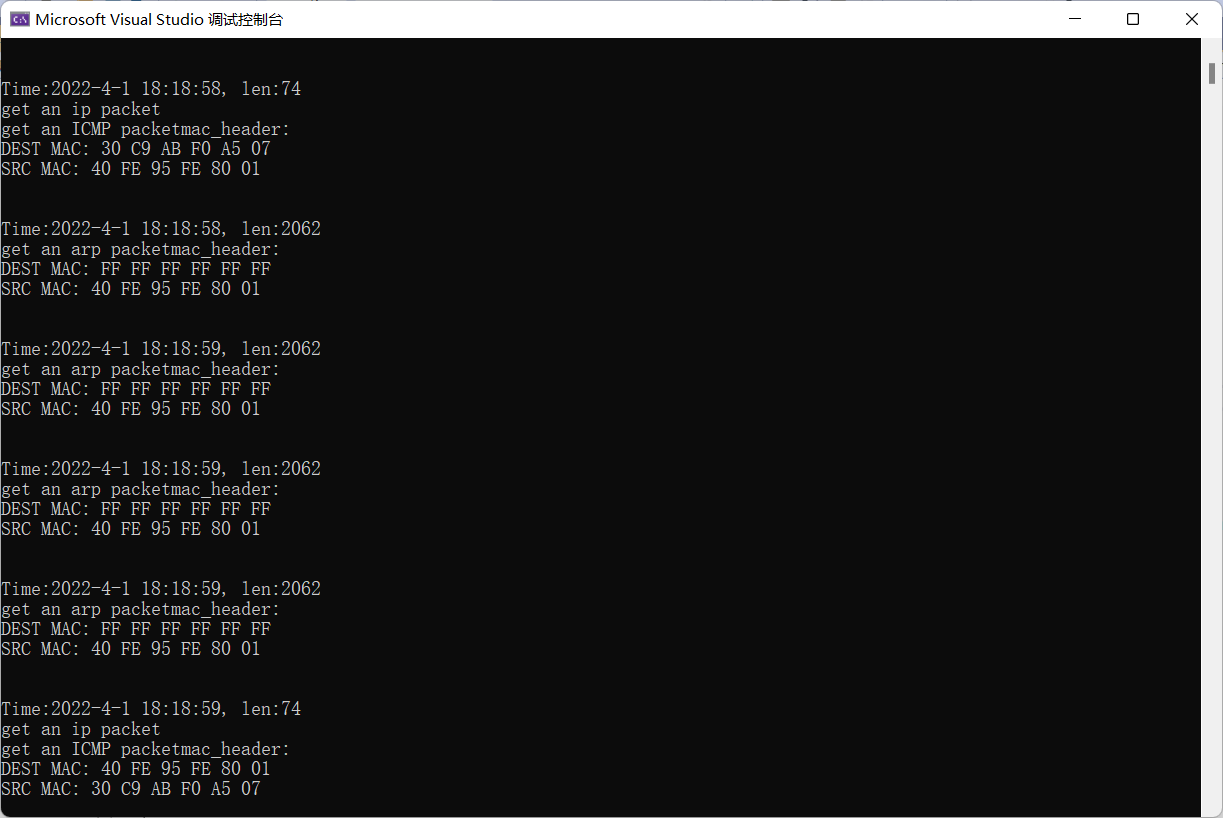
设置过滤



因为设置了ICMP和ARP一起，在后面又加了一层判断，只有当帧类型为0800，且IP协议类型是1，或者帧类型是0806的时候才能输出，也可以直接用这个语句，不用上面的过滤器进行判断

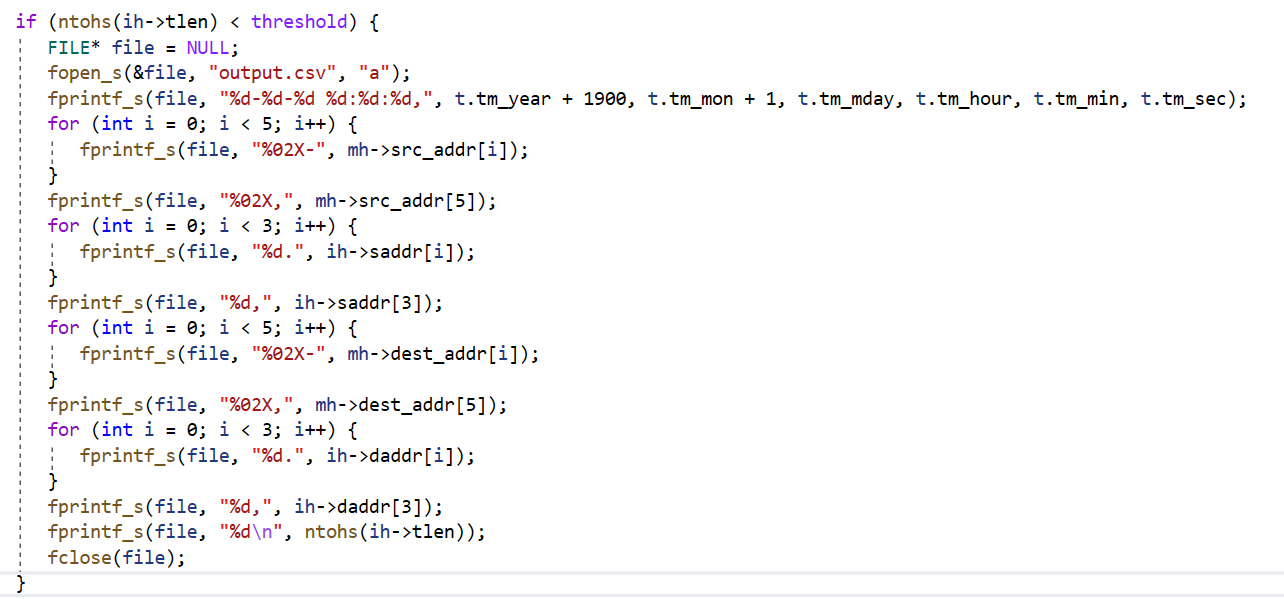


运行结果

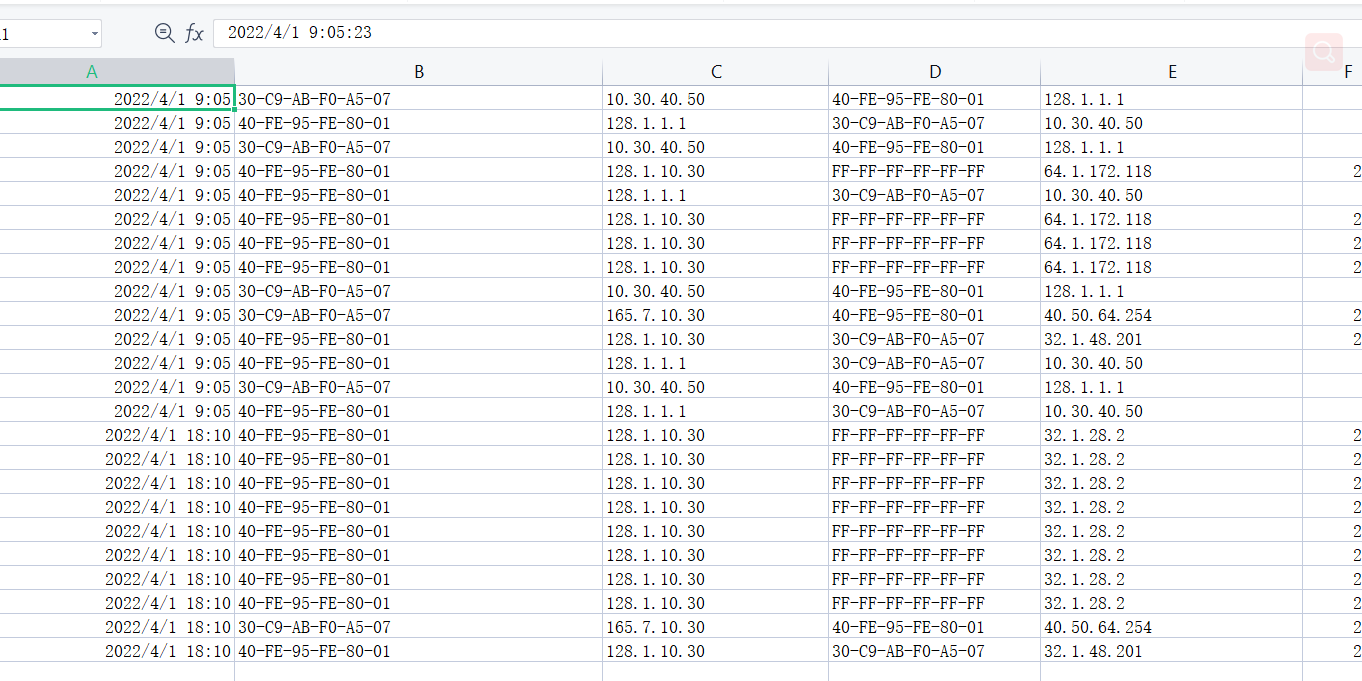


4.保存到csv

将数据保存到out. csv文件当中



运行结果



# 实验总结

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；

学会了查询主机IP，已经ping的使用

学会了wire shark的使用