

****

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：宋泽涛**

**学　　号：25120222201292**

**班　　级：2022级网络2班**

**实验时间：2024/4/7**

**2024 年 4 月 7 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。

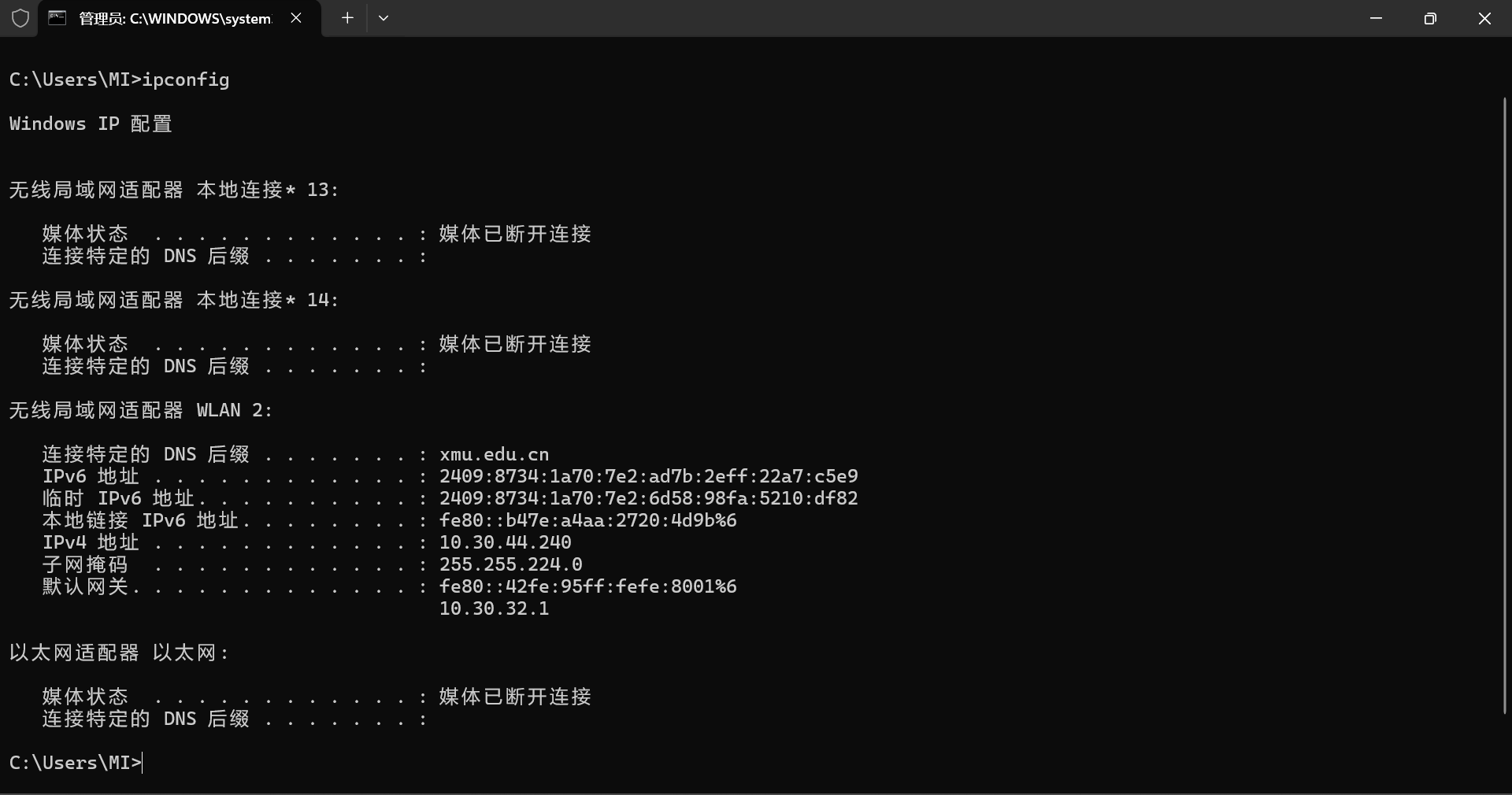
# 实验环境

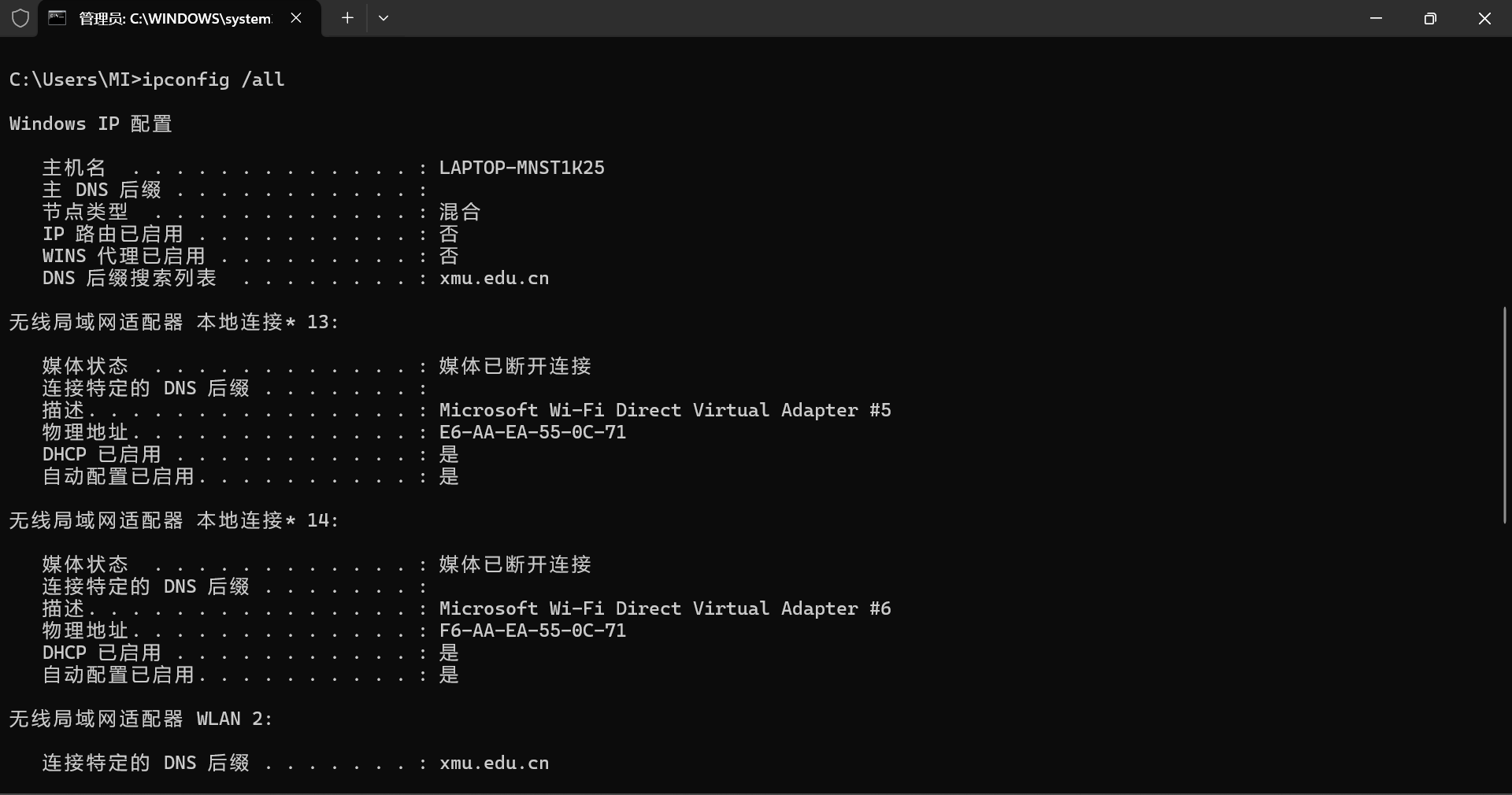
操作系统：Win11

编程语言：C/C++

# 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



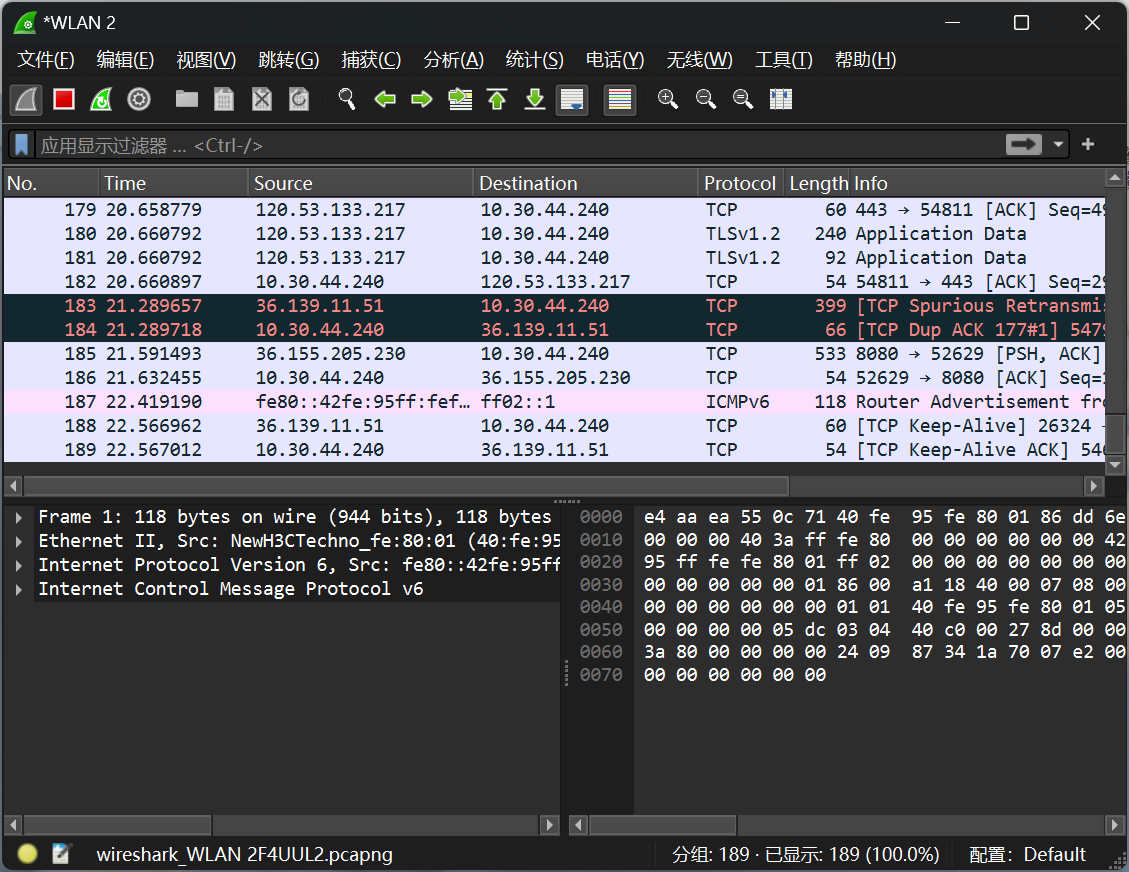


1. 使用 Windows 自带的“命令提示符”或“PowerShell” 完 成“本机与具有某个 IP的主机是否连通”的检测

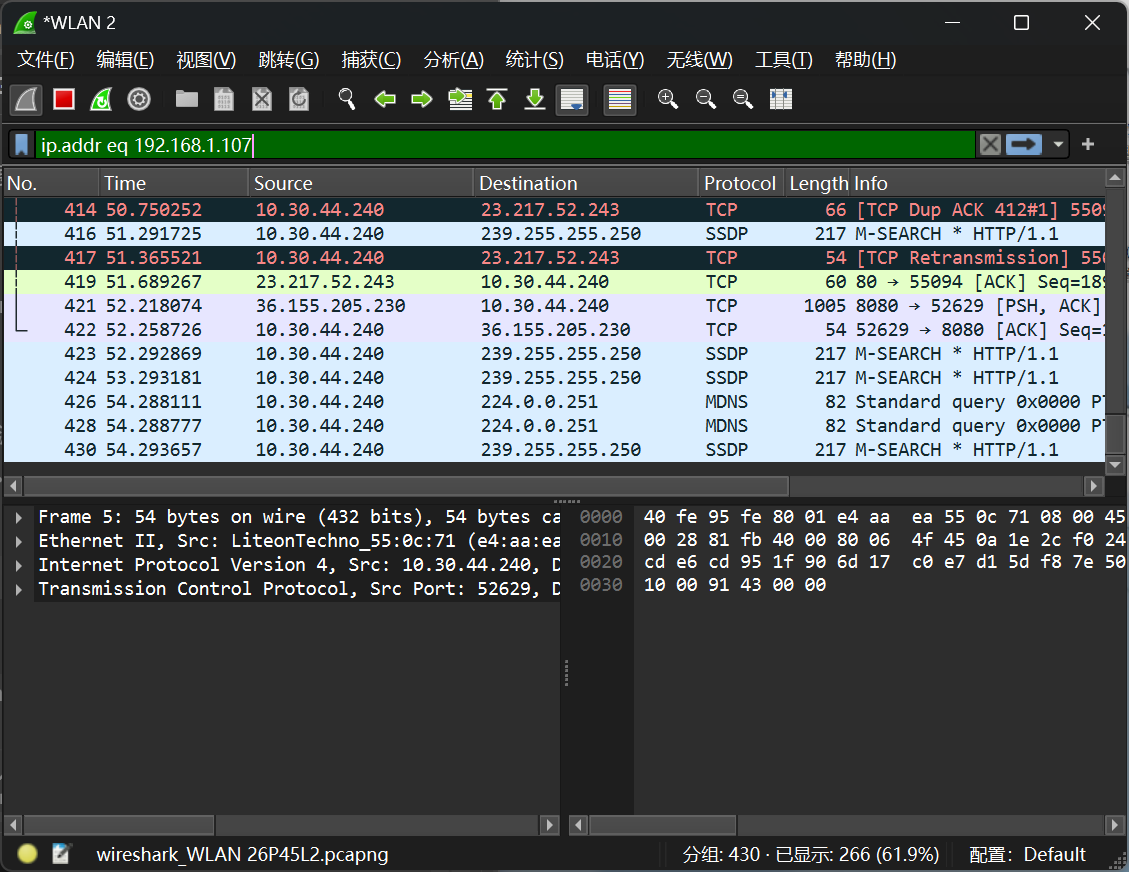


1. 熟悉 Wireshark 的使用，会设置过滤条件，如过滤出指定 IP的数据帧

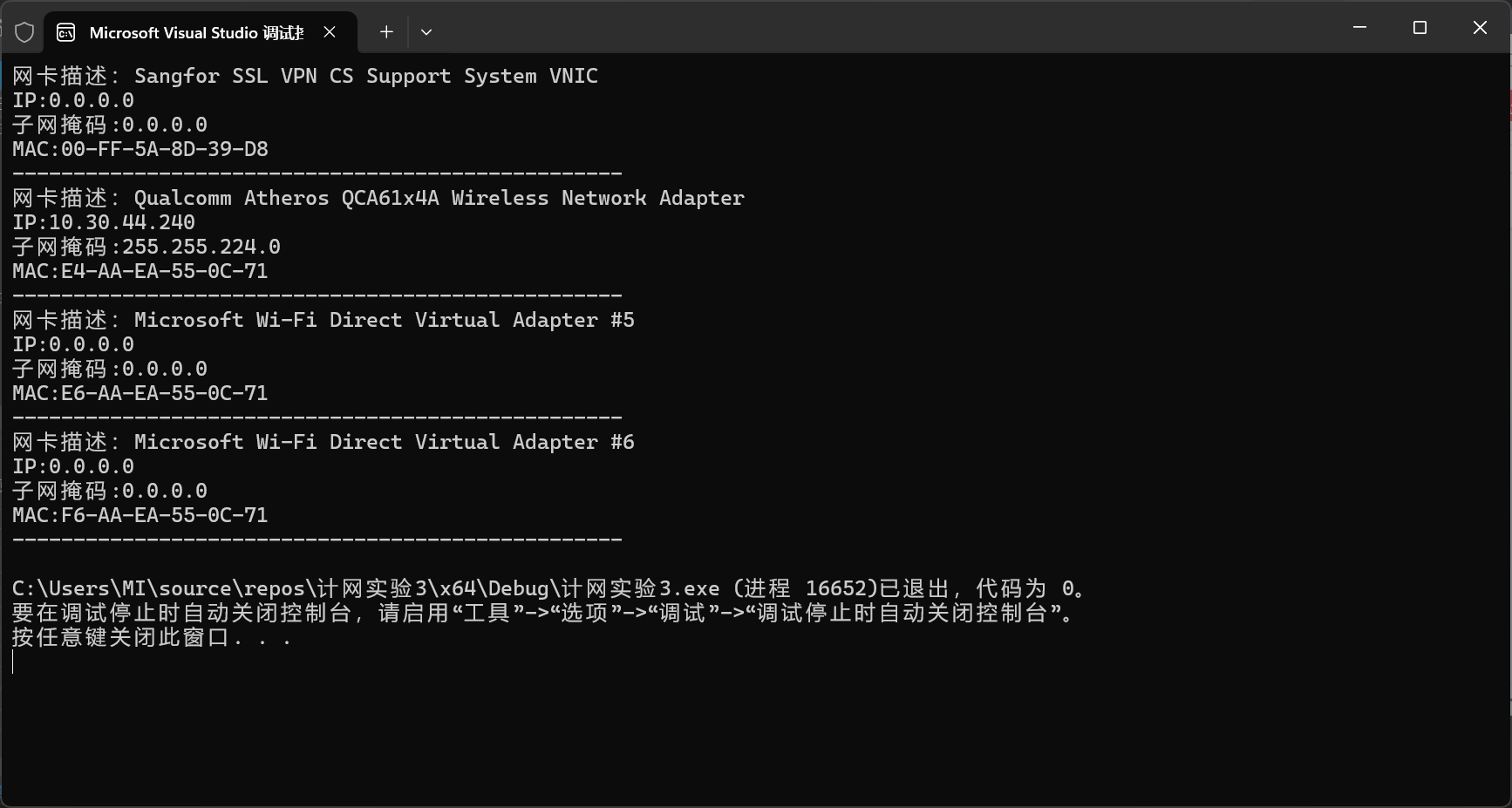
**过滤前结果如下**

****

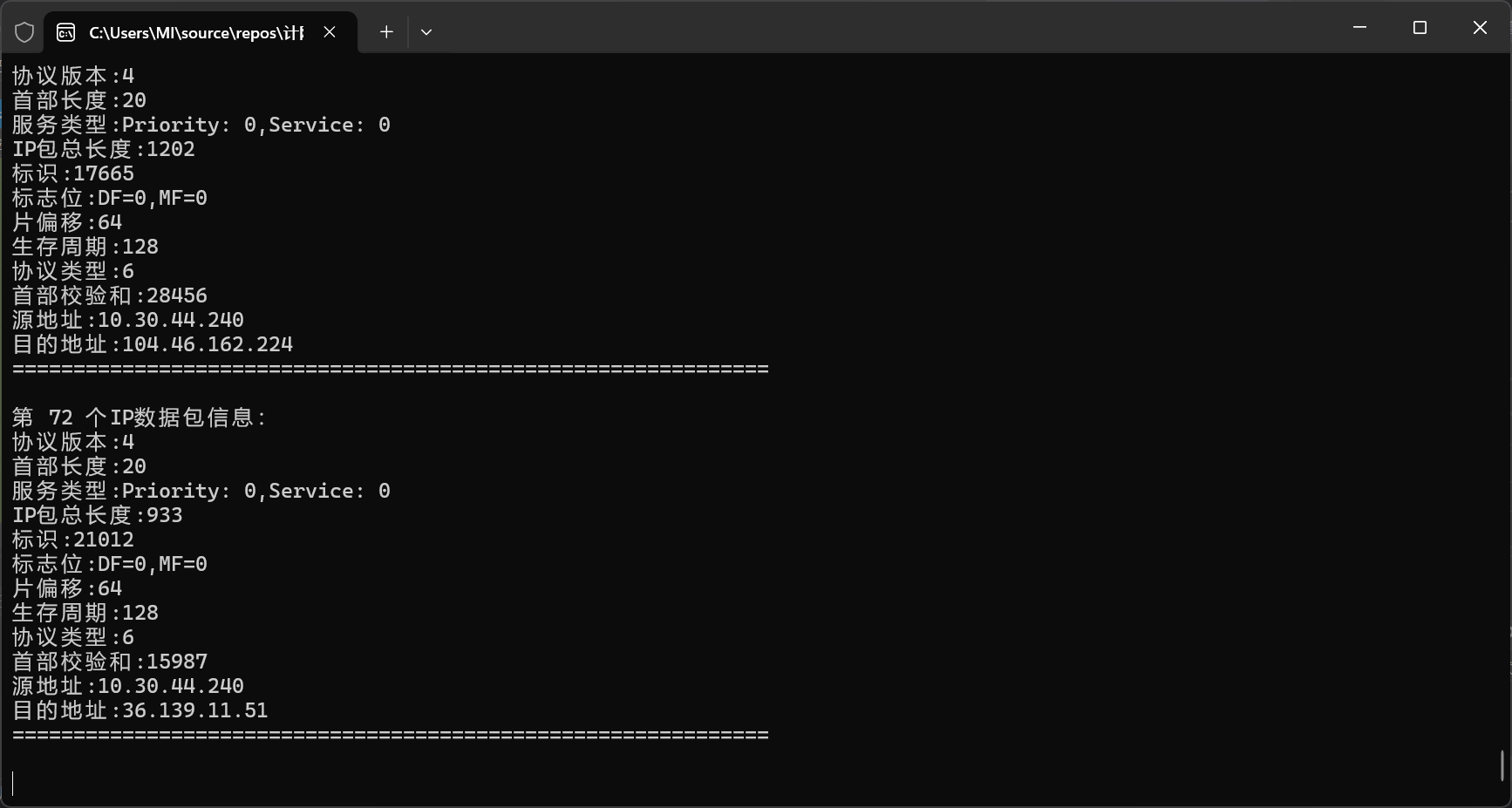
**过滤后结果如下**

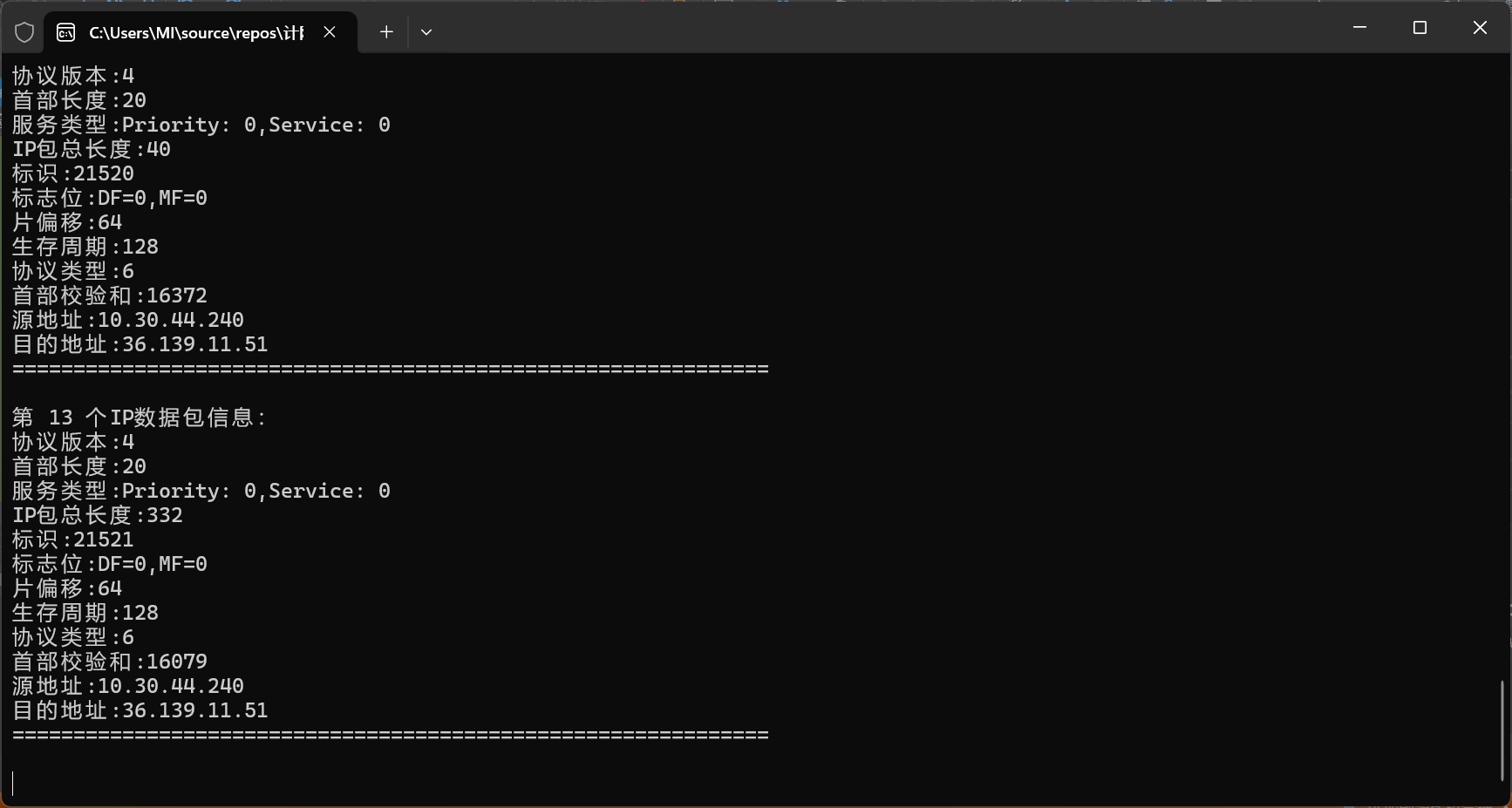
****

1. 配置好实验环境，在控制台打印出网卡设备列表



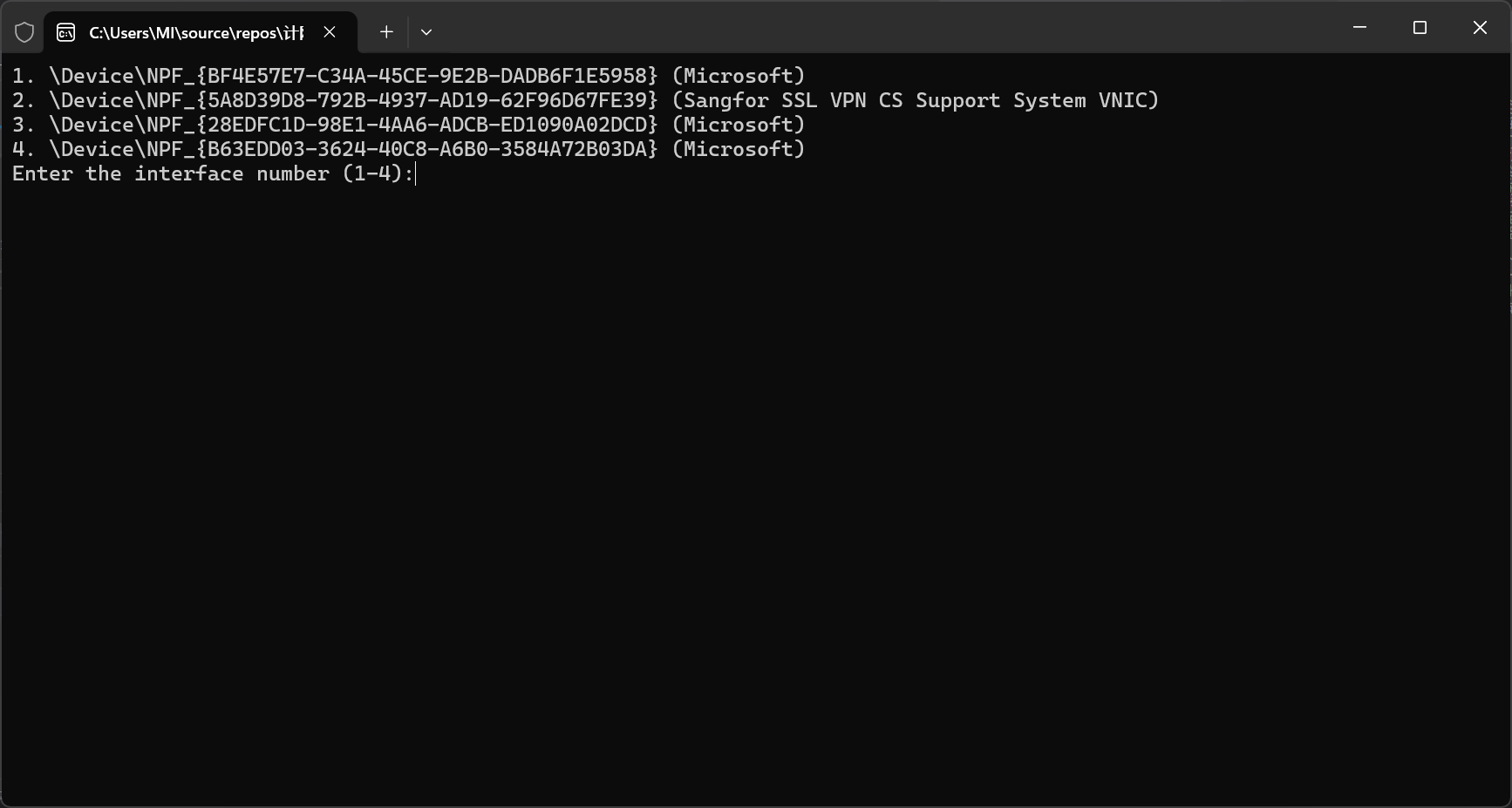
1. 捕获到以太网帧，并能 够 解 析 出 目 的MAC、源 MAC





1. 能够过滤出特定类型的数据包，指定类型的为 ARP，ICMP等

**选择需要监听的网卡**

****

**监听结果如下**

****

# 实验总结

1. 理解以太网帧：通过本实验，我对捕获和分析以太网帧进行了实际操作。通过这个过程，我深入了解了常见数据包的结构和格式，例如 ARP、ICMP 和 IP 协议；
2. 过滤捕获的帧：我学会了根据指定的条件过滤捕获的帧，如目标 IP 地址、源 IP 地址和协议类型。通过应用过滤器，我能够集中精力分析特定类型的网络流量，有助于深入分析网络行为;
3. WinPCAP 使用：本实验涉及使用 WinPCAP，在 Windows 平台上进行数据包捕获和分析。通过实际应用，我熟悉了 WinPCAP 的功能，可以捕获和解析网络数据包.