

****

**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2023级2班**

**姓　　名 苏一涵**

**学　　号 36720232204041**

**实验时间 2025年3月21日**

**2025年2月15日**

**填写说明**

1. 本文件为Word模板文件，建议使用Microsoft Word 2024打开，在可填写的区域中如实填写；
2. 填表时勿改变字体字号，保持排版工整，打印为PDF文件提交；
3. 文件总大小尽量控制在1MB以下，最大勿超过5MB；
4. 在实验课结束14天内，按实验报告提交到我校课程网站的指定位置，源代码等主要材料上传在公开的代码托管平台上。
5. 鼓励同学之间探讨，鼓励合理使用人工智能平台，提升效率，但不应滥用相关资源，如抄袭代码和代写作业。

# 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。

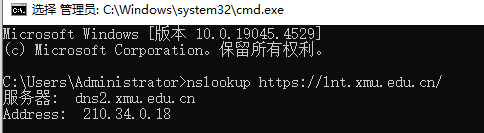
# 实验环境

操作系统：win11

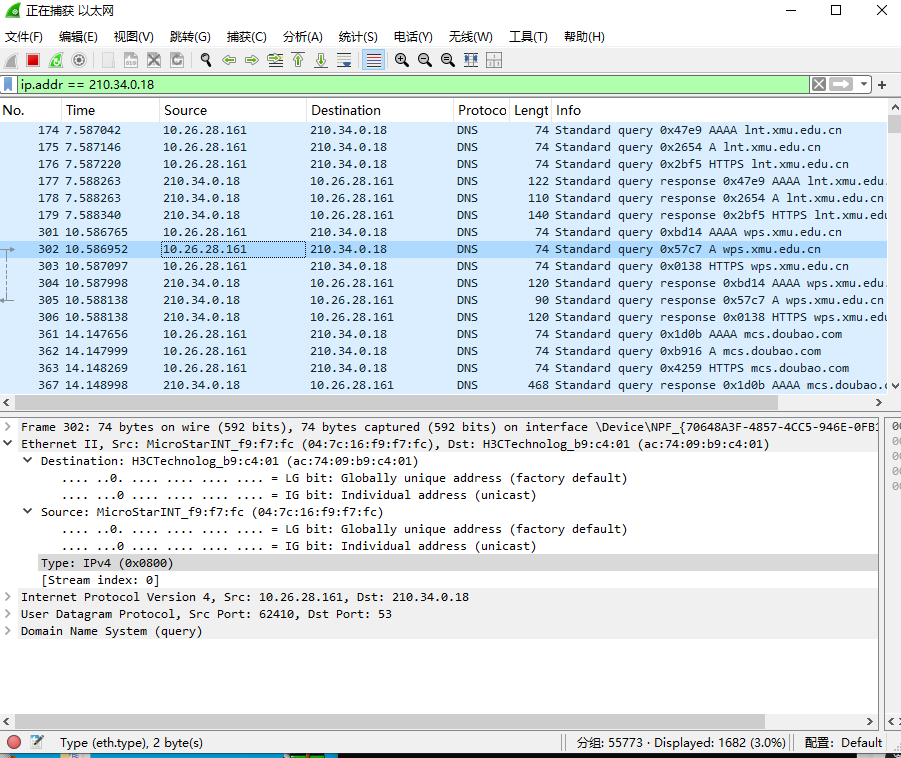
编程语言：C/C++

# 实验结果

1.用Wireshark侦听软件网络上的数据流并观察数据格式：

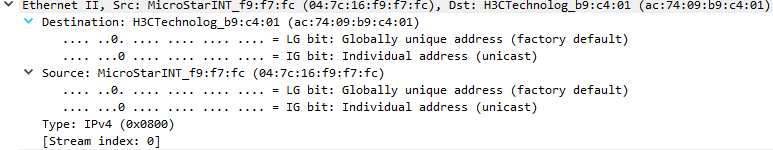


用学校的服务qi地址开始抓包：

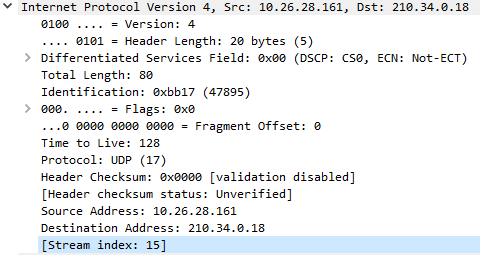


(1)验证协议层次嵌套：

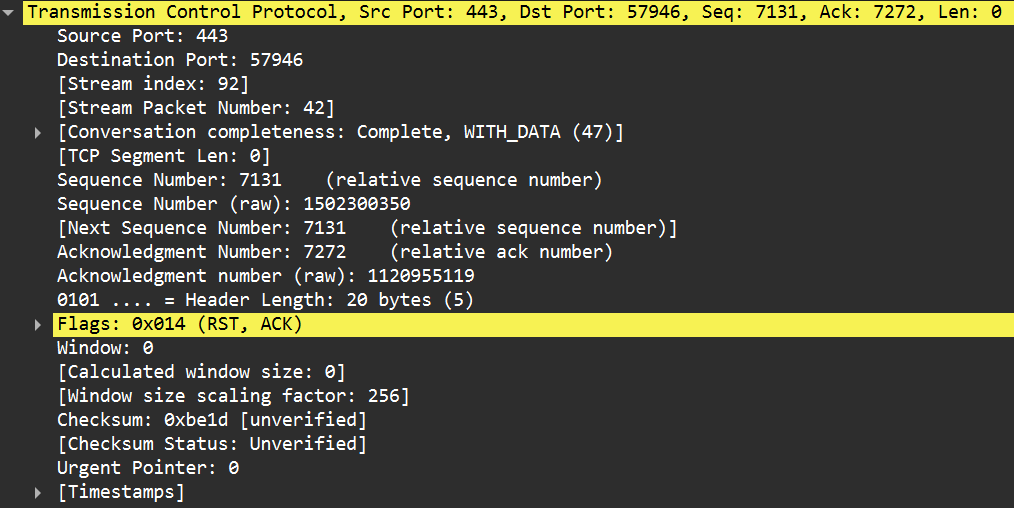
数据链路层/帧格式：从图可以看到源MAC地址(source)和目标MAC地址(destination)



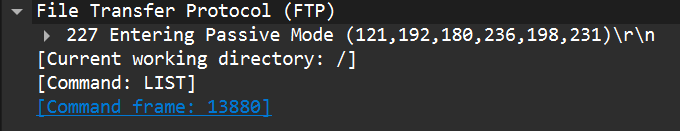
网络层/IP报文格式：可以看到是IP v4，源IP地址为：10.26.28.161，目的IP地址为：210.34.0.18

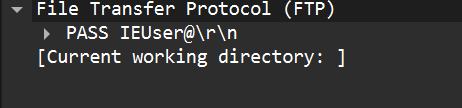


传输层/TCP段格式：可以看到TCP头部的端口、序列号、标志位等如下



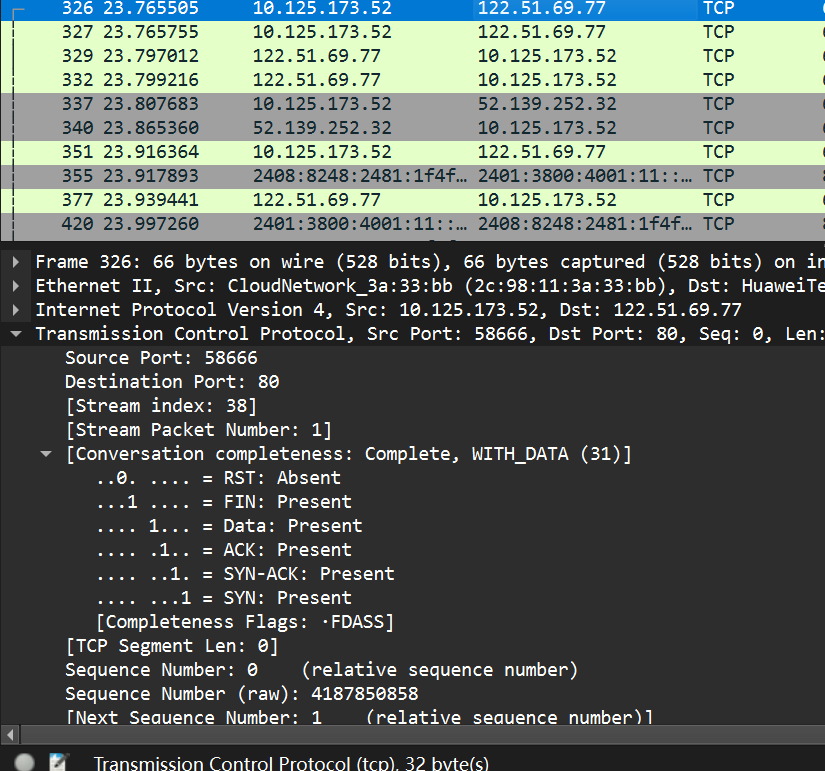
应用层/FTP协议：



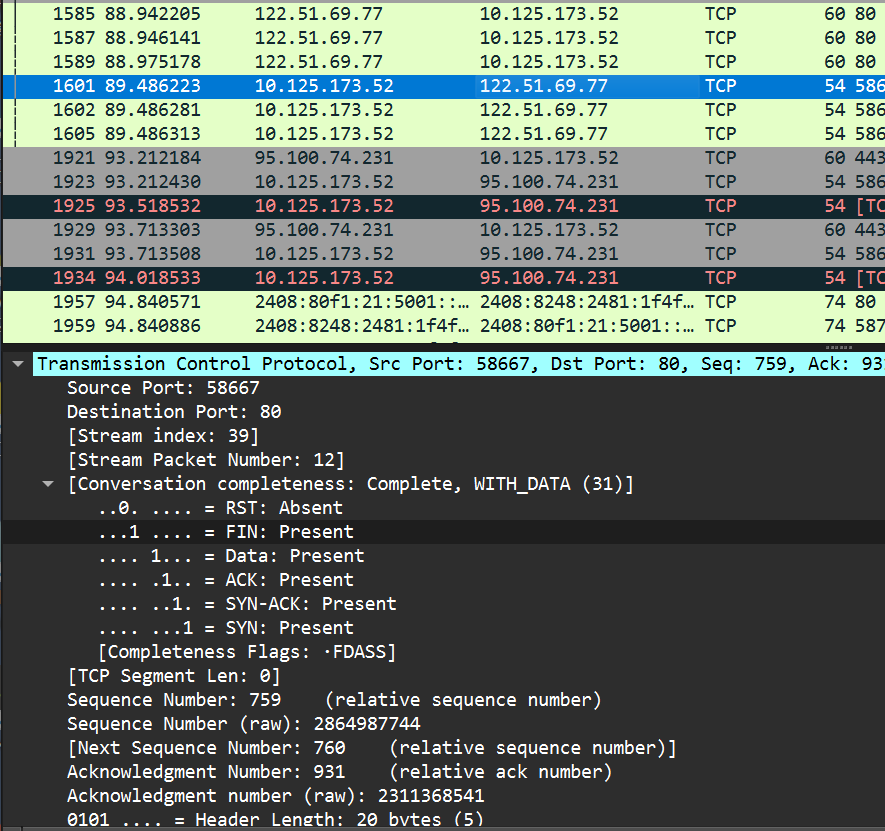


2.用侦听解析软件观察 TCP 机制:

连接建立，客户端SYN标志位为1，SYN=1, ACK=1



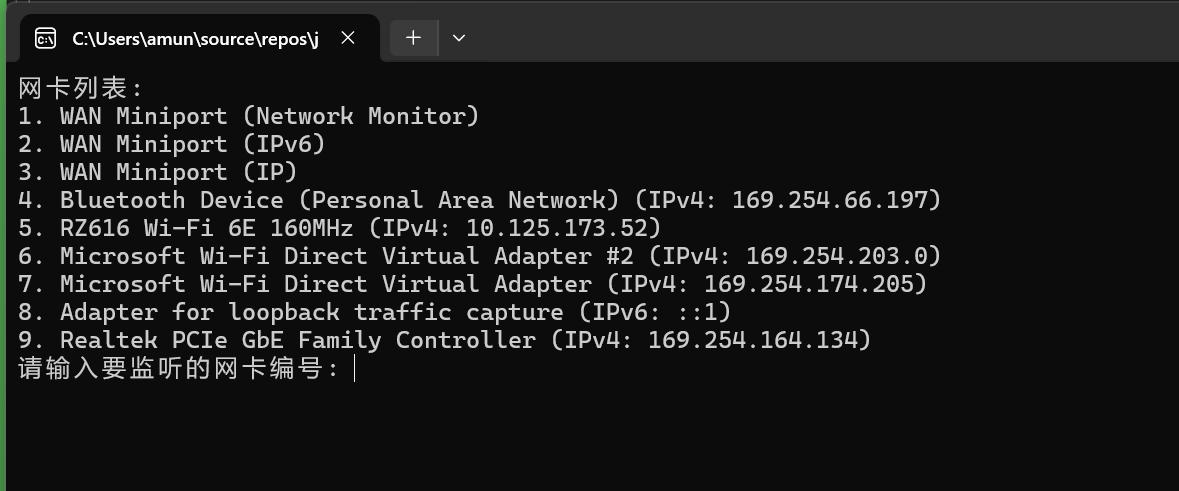
接收端回执：

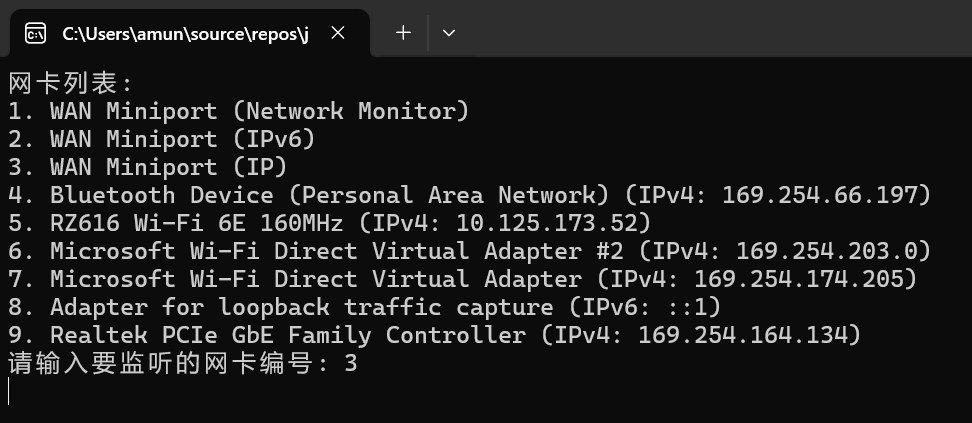


三次握手、四次挥手建立和断开连接。

3.用 Libpcap 或 WinPcap 库侦听网络数据:

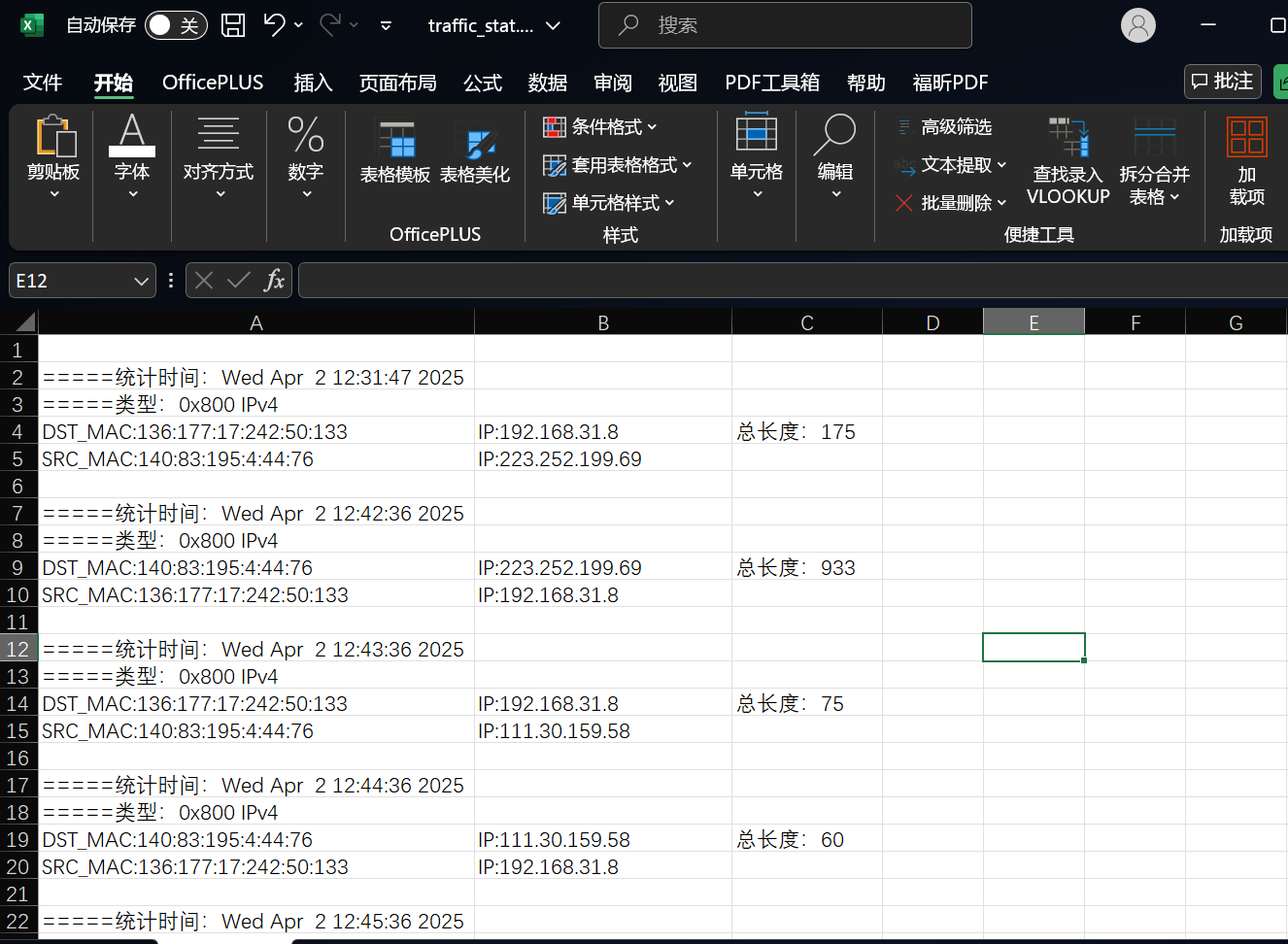
首先在控制台上打印出网卡列表以供选择：



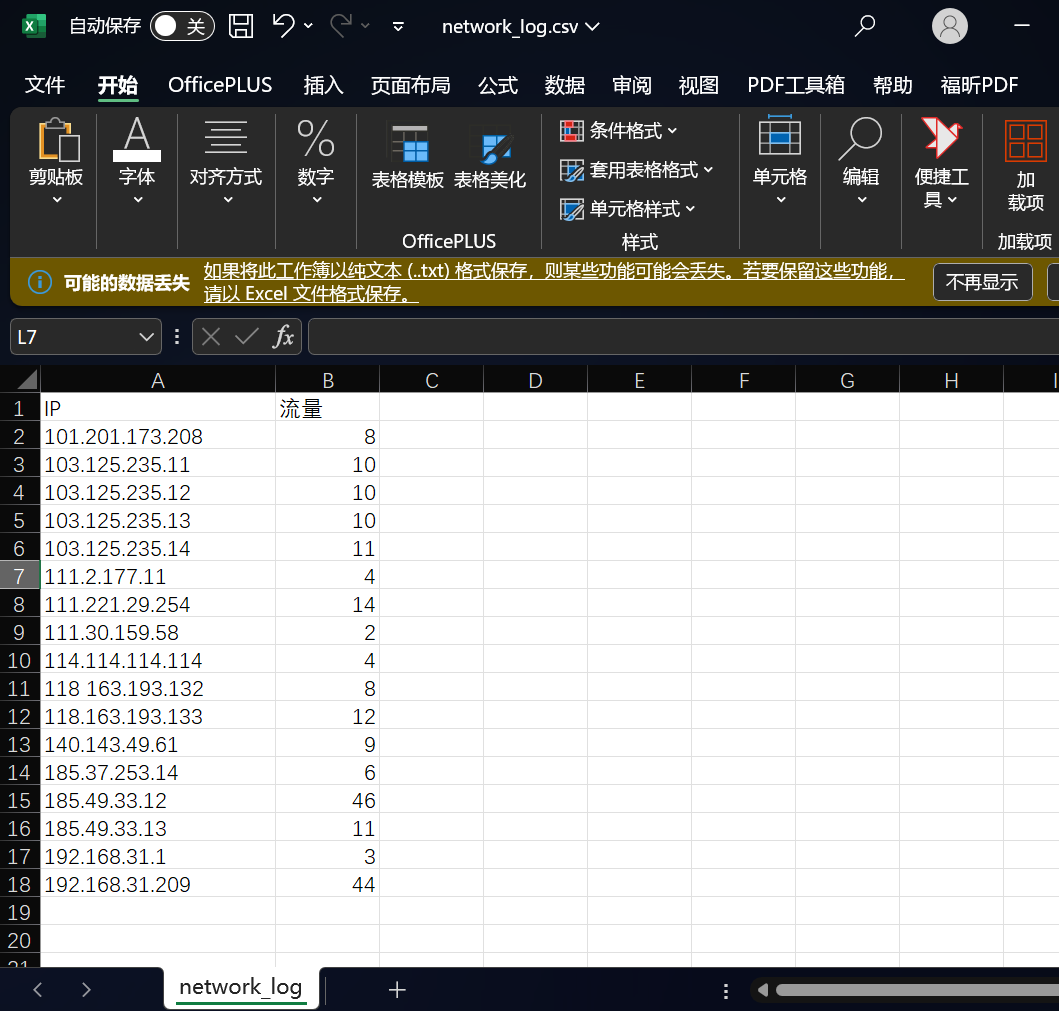


这里直接选择ipv4进行抓取。

得到抓取日志以及流量统计如下：

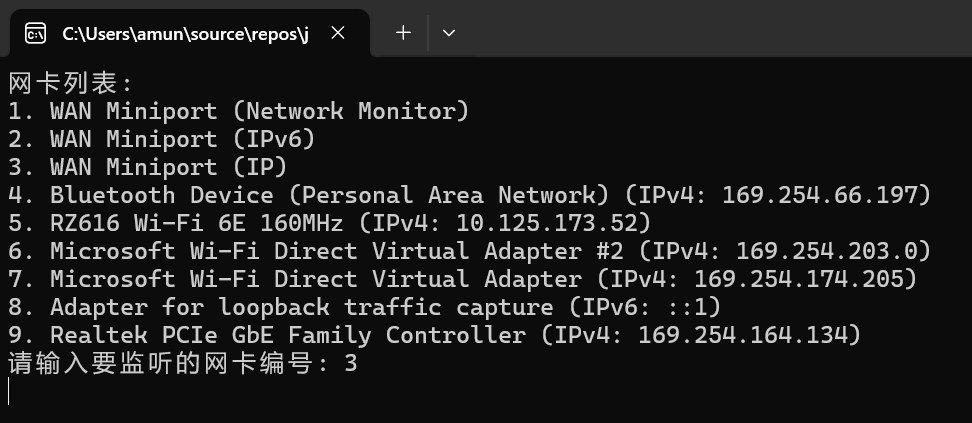


流量统计如下：



4.解析侦听到的网络数据

同3过程运行程序选择网卡开始监听：



打开日志文件查看结果：



# 实验代码

本次实验的代码已上传于以下代码仓库：https://gitee.com/Soyaha/computer-network/tree/master/%E5%AE%9E%E9%AA%8C%E4%B8%89%20%E5%9F%BA%E4%BA%8EPCAP%E5%BA%93%E4%BE%A6%E5%90%AC%E5%B9%B6%E5%88%86%E6%9E%90%E7%BD%91%E7%BB%9C%E6%B5%81%E9%87%8F。

# 课后思考题

无

# 实验总结

本实验通过实战操作，加深了对网络协议栈的理解，并为后续研究网络入侵检测、流量分析等方向奠定了基础。同时，通过代码实现与调试，提升了对底层网络编程和数据解析能力的掌握。