1. **实验目的：**

1、掌握网络分析工具Wireshark的使用方法；

2、理解以太网的数据帧格式和MAC地址。

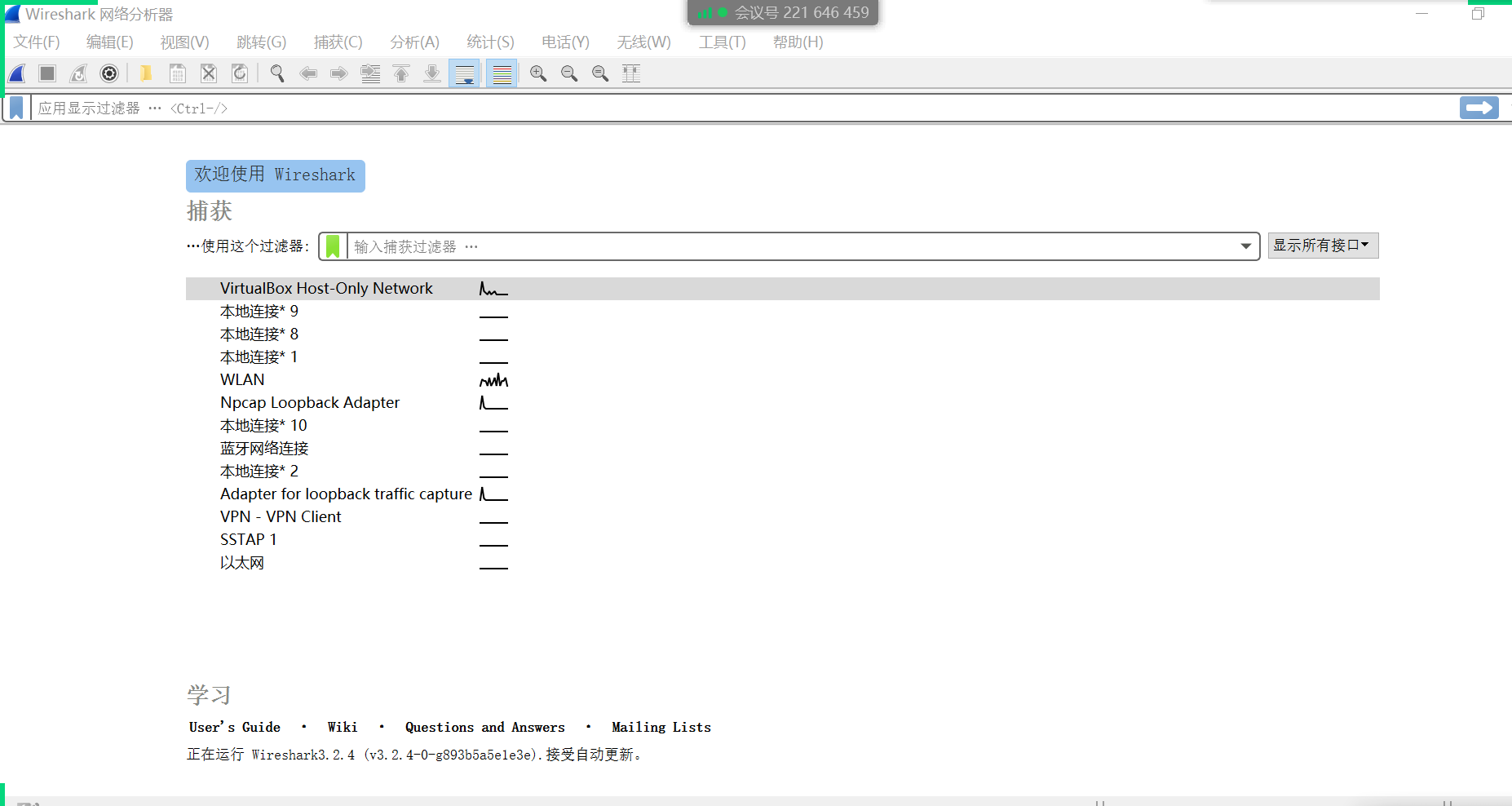
1. **实验配置**

联网计算机；

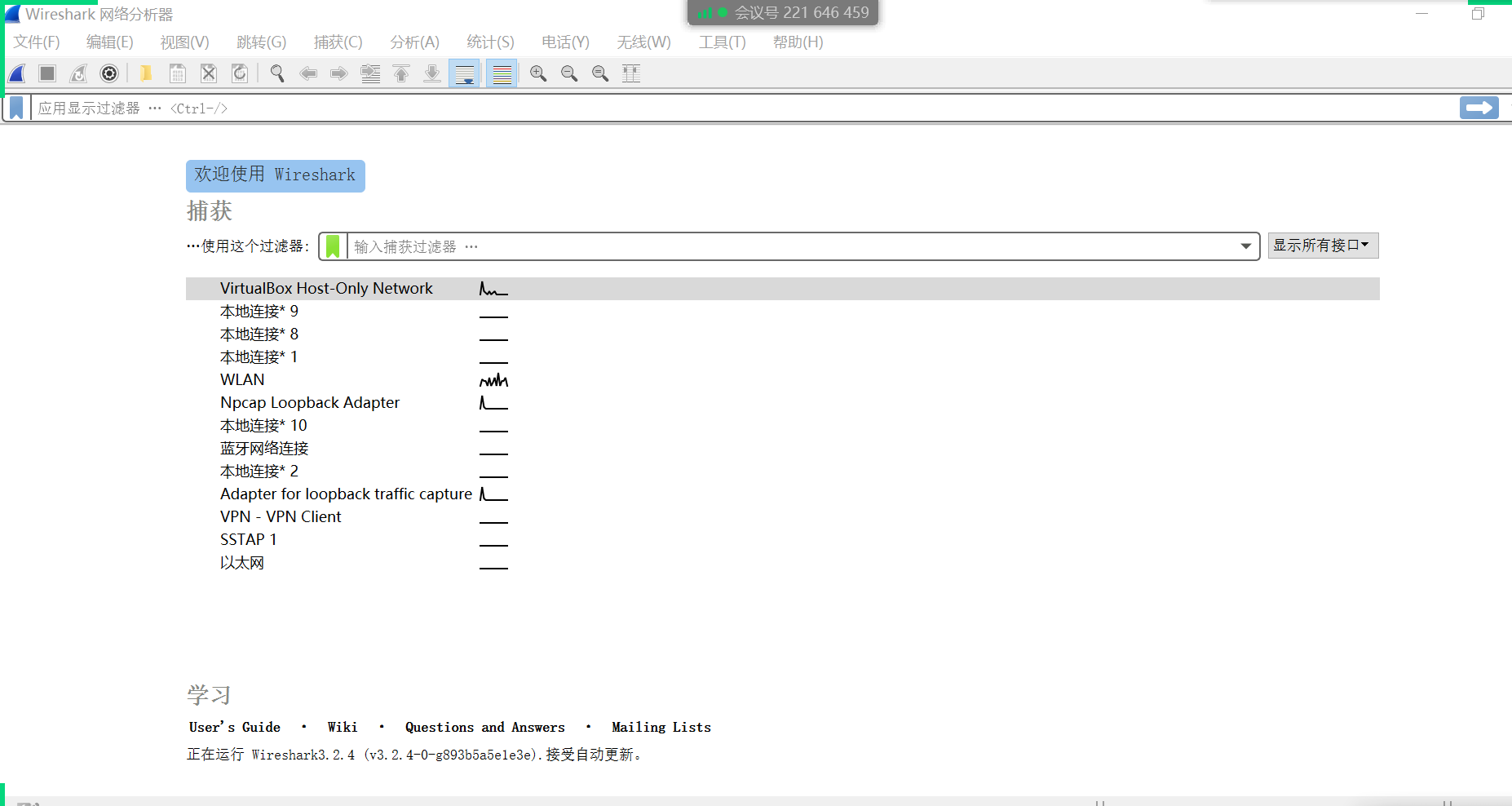
Windows操作系统；

Wireshark。

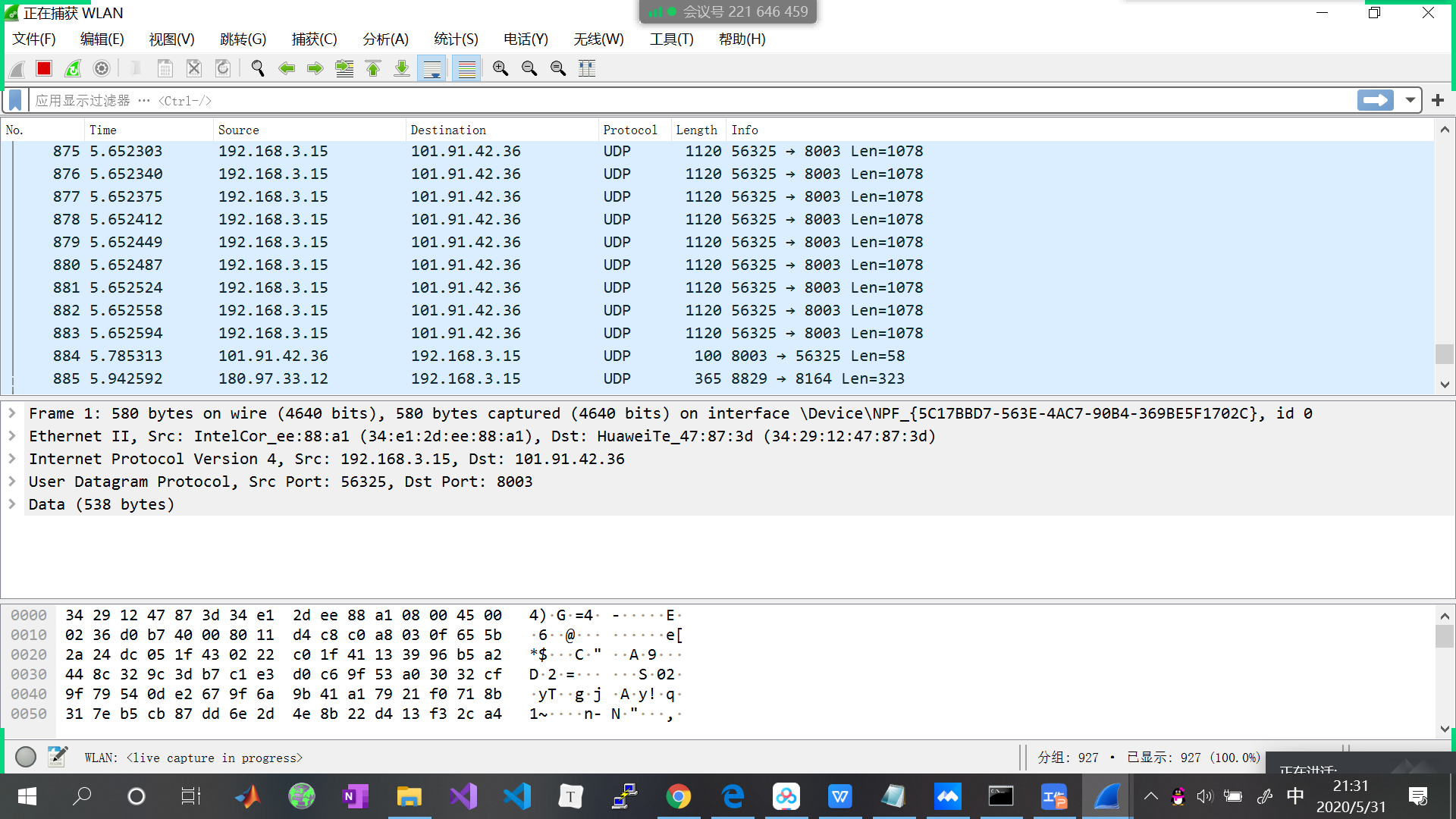
1. **实验步骤：**
2. 启动Wireshark；



1. 设置接口，关闭混杂模式，即关闭Capture packets in promiscuous mode选项；



1. 进行网络操作，操作结束后，停止抓包；



**四、实验报告内容：**

1. **观察Frame信息，写出数据包的捕获时间，这个包与第一个包的相对时间增量，帧序号，数据包的长度，捕获的长度，协议封装层次。**

答：

数据包的捕获时间：May 31, 2020 20:16:57.631133000

与第一个包的相对时间增量：0.000000000

帧序号：1

数据包长度：698 bytes (5584 bits)

捕获长度：698 bytes(5584 bits)

协议封装层次：eth:ethertype:ip:udp:data

1. **找到一个单播帧，分析其首部各字段值，并说明其含义，如发送计算机的MAC地址和接收计算机的MAC地址各是什么，以及类型字段等。**

答：

5`FYS1ZZB4KBZG$ILT}Q27Q

02的2进制为0000 0010，因此为单播帧

02 ac 0d d3 00 00：发送计算机的MAC地址

01 11 c0 ca c0 a8：接收计算机的MAC地址

使用TCP协议传输

1. **找到一个广播帧，源地址和目的地址是什么，数据部分承载的是什么协议的数据包？**

答：

B_999(7O[H8@S3MQE$$EQ2C

末尾为.255，因此为广播帧

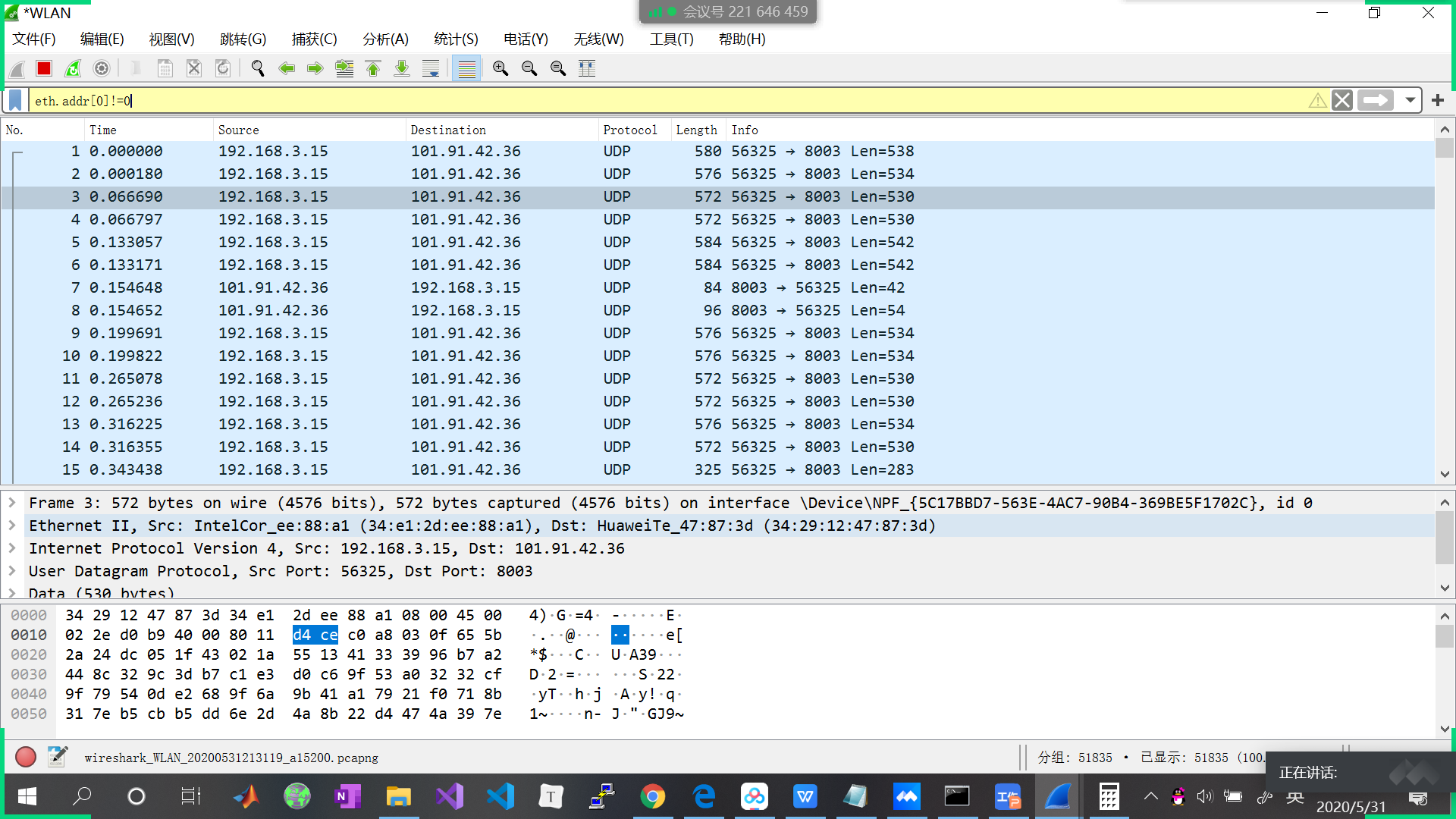
源地址：192.168.3.15

目的地址：192.168.3.255

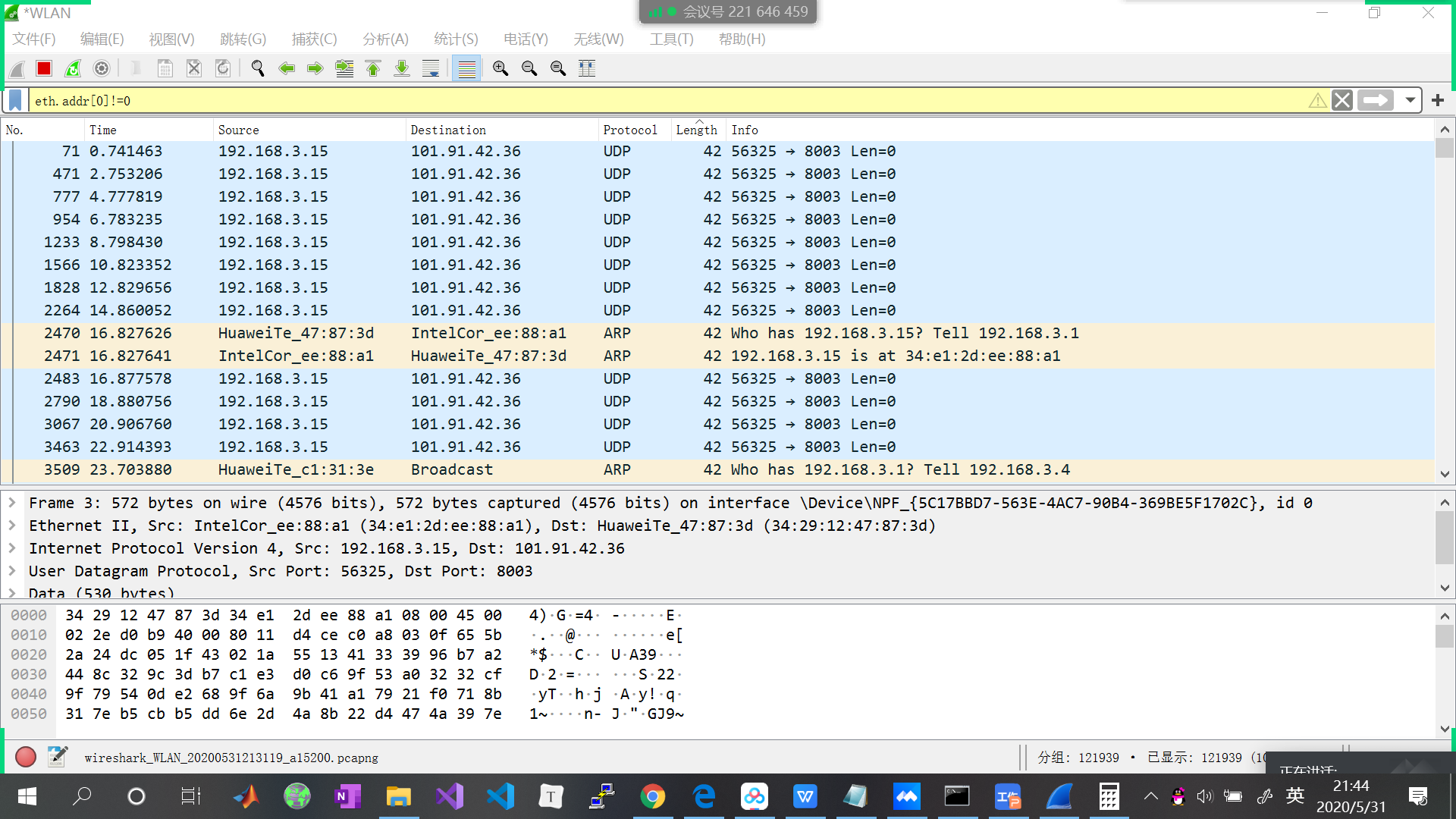
协议：UDP

1. **编写过滤规则找到一个组播帧。**

答：eth.addr[0]!=0



1. **实验中捕获的所有以太网帧，最小帧长是多少？为什么？**



最小帧长是42。

抓包软件抓到的是去掉前导同bai步码、帧开始分界符、FCS之外的数据，wireshark把du8字节的前序和4字节的FCS都给过滤了。wireshark中所显示的zhi报文长度是包含14字节dao以太类回型头,但不计算尾部4字节校验FCS值的.即wireshark报文长度大小：14（以太类型头）答＋20（ip头）＋（实际数据）

1. **在实验中捕获的以太网帧中，除了封装IP数据包，还有别的什么协议的数据包？Type字段的值是多少？**

答：

按照Protocol参数进行筛选，得到：

ARP 0x0806  
BROWSER 0x0800  
DHCP 0x0800  
ICMPv6 0x86dd  
IGMPv3 0x0800  
LLMNR 0x0800  
MDNS 0x86dd  
NBNS 0x0800  
SSDP 0x0800

参考资料：

1. <https://zhidao.baidu.com/question/143894456>
2. <https://blog.csdn.net/zwl1584671413/article/details/80229110>
3. <https://blog.csdn.net/hebbely/article/details/54424823>
4. <https://www.cnblogs.com/linyfeng/p/9496126.html>
5. https://blog.csdn.net/qq\_43655453/article/details/106271650