**海南大学计算机与网络空间安全学院**

**实 验 报 告**

|  |  |
| --- | --- |
| **评定成绩** | **指导教师** |
|  |  |

**实验课程：** 网络协议与分析

**实验名称：**Mac幀、IP包抓包分析、IP分片分析、ARP及ARP欺骗

1. 实验目的

1.掌握基本的网络协议分析方法。通过抓包工具，观察Mac幀、IP包格式；

2.掌握基本的网络协议分析方法，通过抓包工具，观察并掌握IP分片机制；

3.掌握ARP协议工作原理和格式；

4.掌握常见ARP欺骗类型和手段；

5.掌握Sniffer Pro软件的使用；

6.掌握防范ARP地址欺骗的方法和措施

1. 实验任务

1.运行wireshark工具软件，再分别启动浏览器、FTP工具、Telnet工具或Ping等网络命令，试抓包并察看和分析抓包结果。

2.从本机用Ping命令发送一个5000字节的大数据包到局域网的另一台主机，在传输的过程中，开启wireshark软件抓包，查看并分析详细的分片结果。

3.运行ARP命令查询本机ARP缓存表；运用Sniffer Pro软件进行ARP协议截包分析。

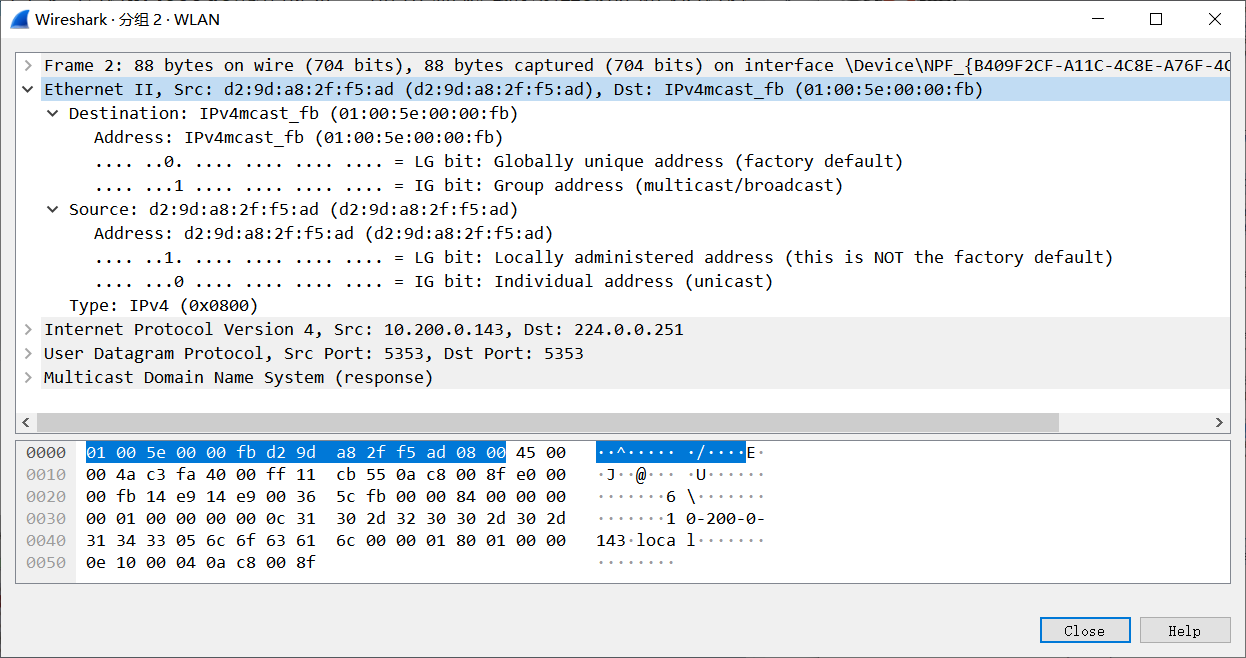
1. 实验环境

计算机网络实验室局域网，安装Windows2000/XP操作系统之PC机。

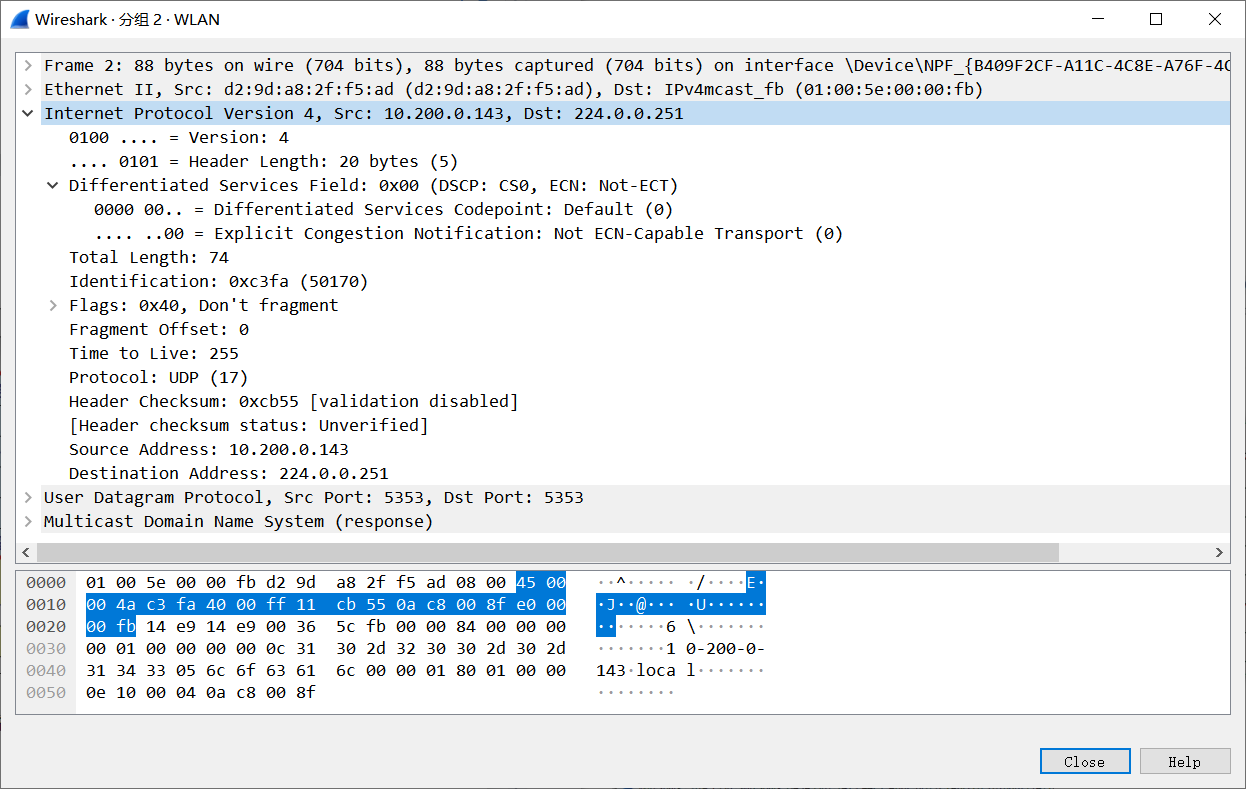
1. 实验内容
2. 运行wireshark工具软件，再分别启动浏览器、FTP工具、Telnet工具或Ping等网络命令，试抓包并察看和分析抓包结果。

数据链路层：

14个字节：源mac地址6字节、目标mac地址6字节、协议标记 type 16位2个字节

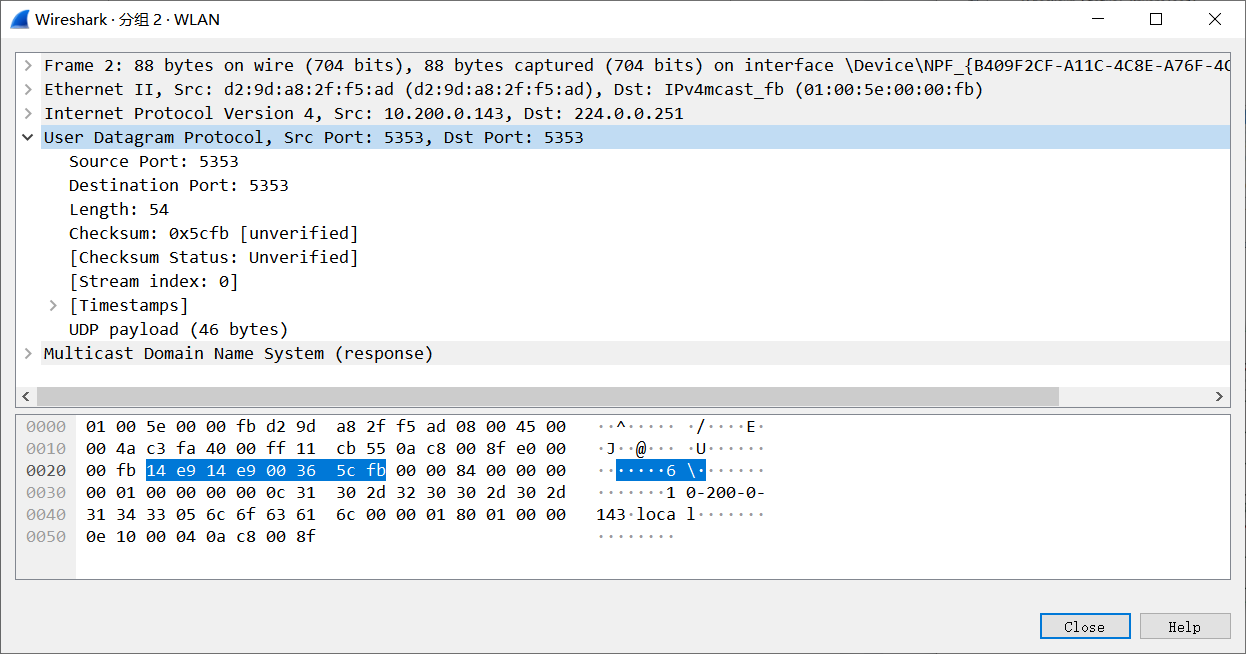


IP数据报：

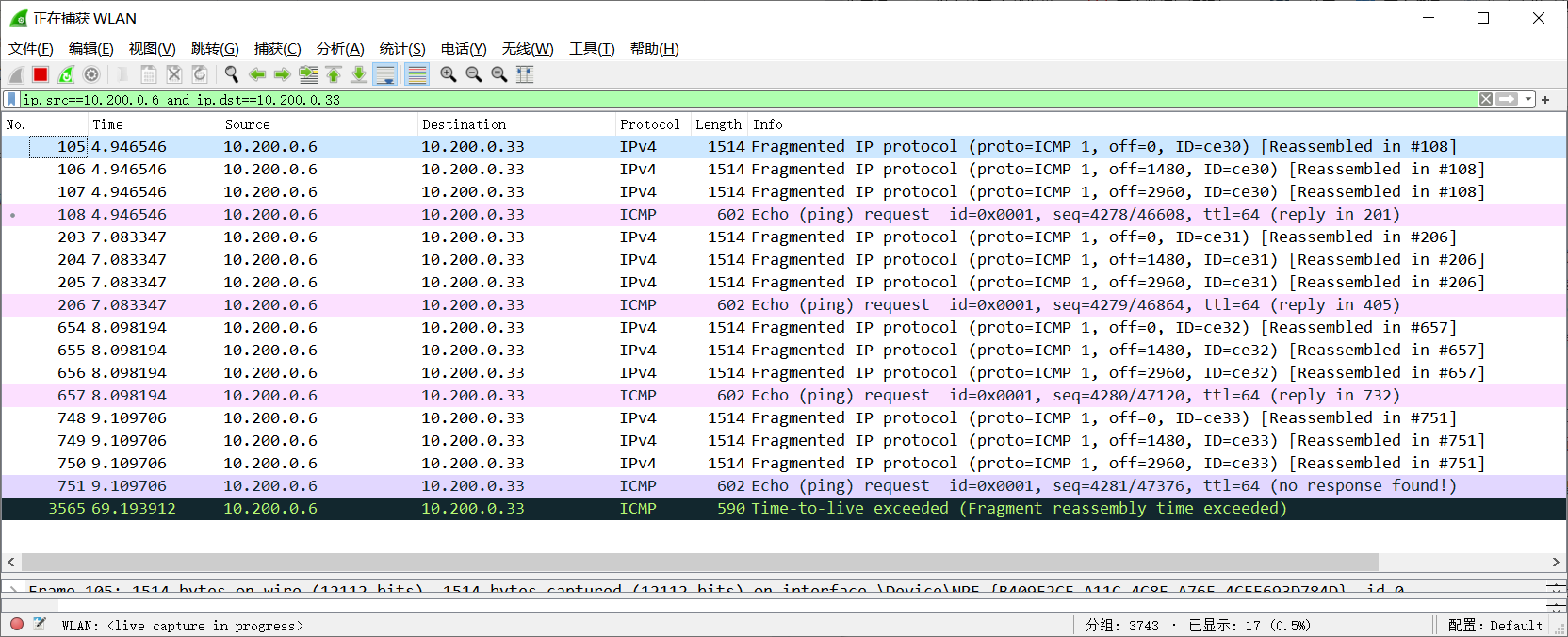
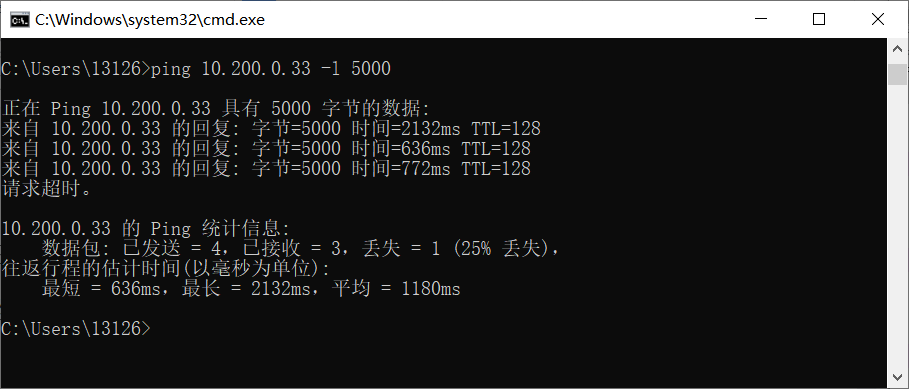


UDP数据包：

源端口Source Port：2字节、目的端口Destination Port：2字节、长度Length：2字节、检验和Checksum：2字节。



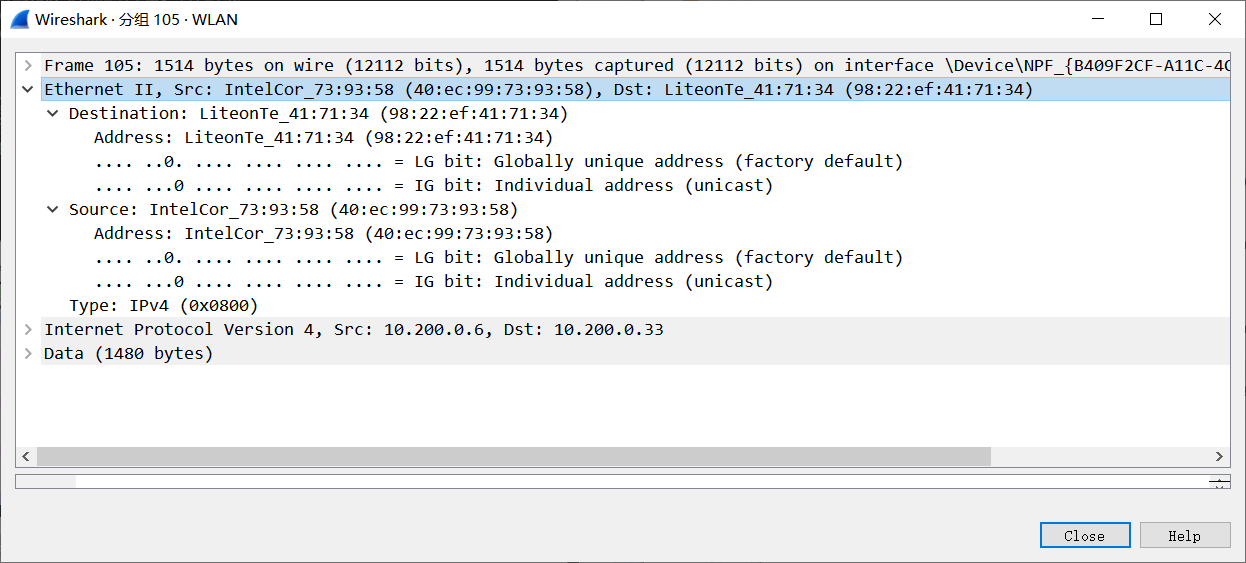
1. 从本机用Ping命令发送一个5000字节的大数据包到局域网的另一台主机，在传输的过程中，开启wireshark软件抓包，查看并分析详细的分片结果。



Ipv4

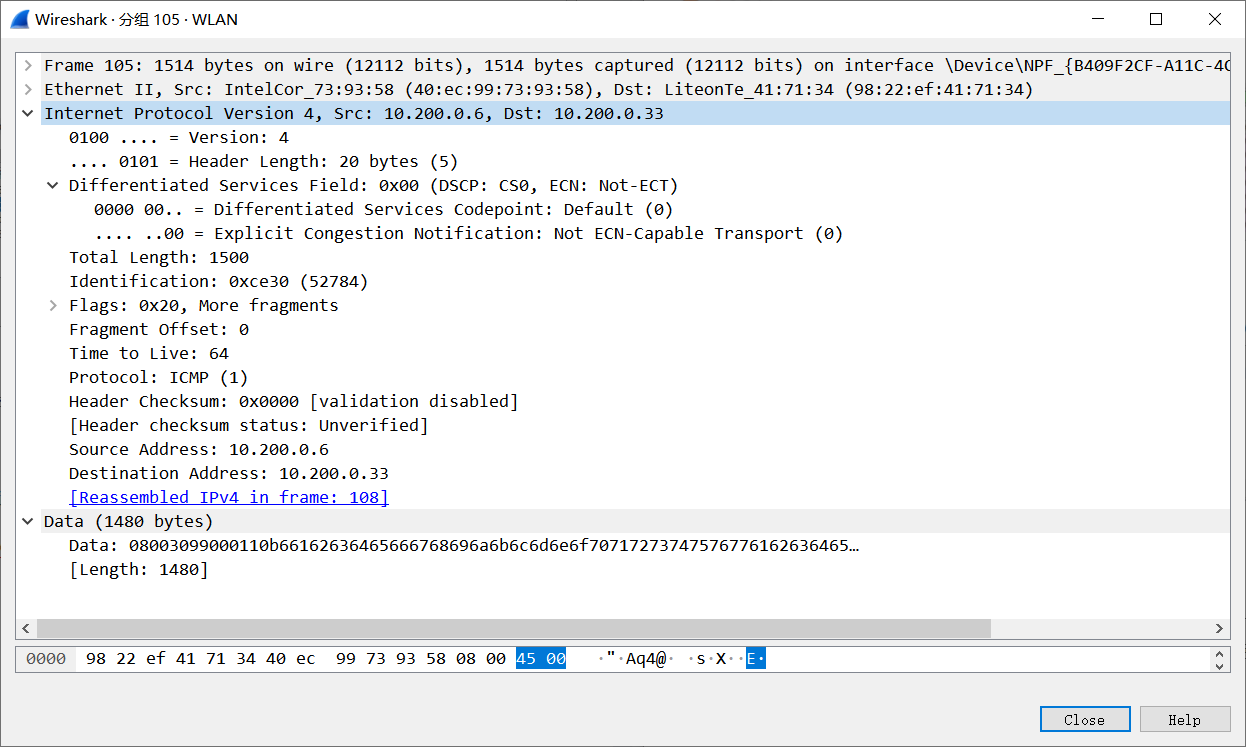
数据链路层：

目的mac地址：6字节、源mac地址：6字节、上层协议类型：ipv4，2字节



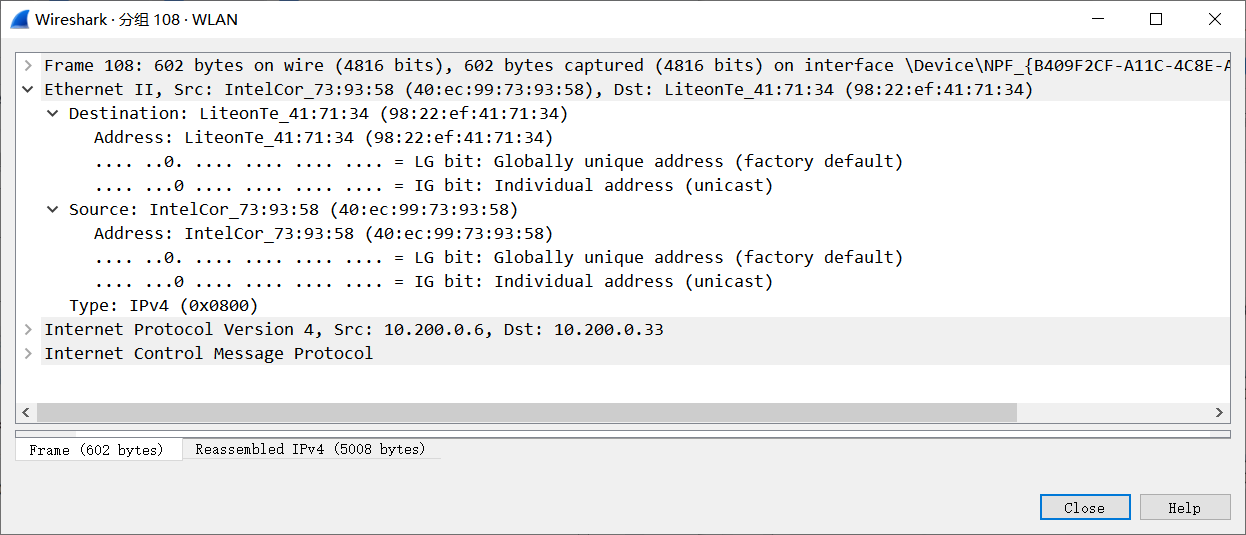
IP数据报：

数据报总长20字节；数据1480字节

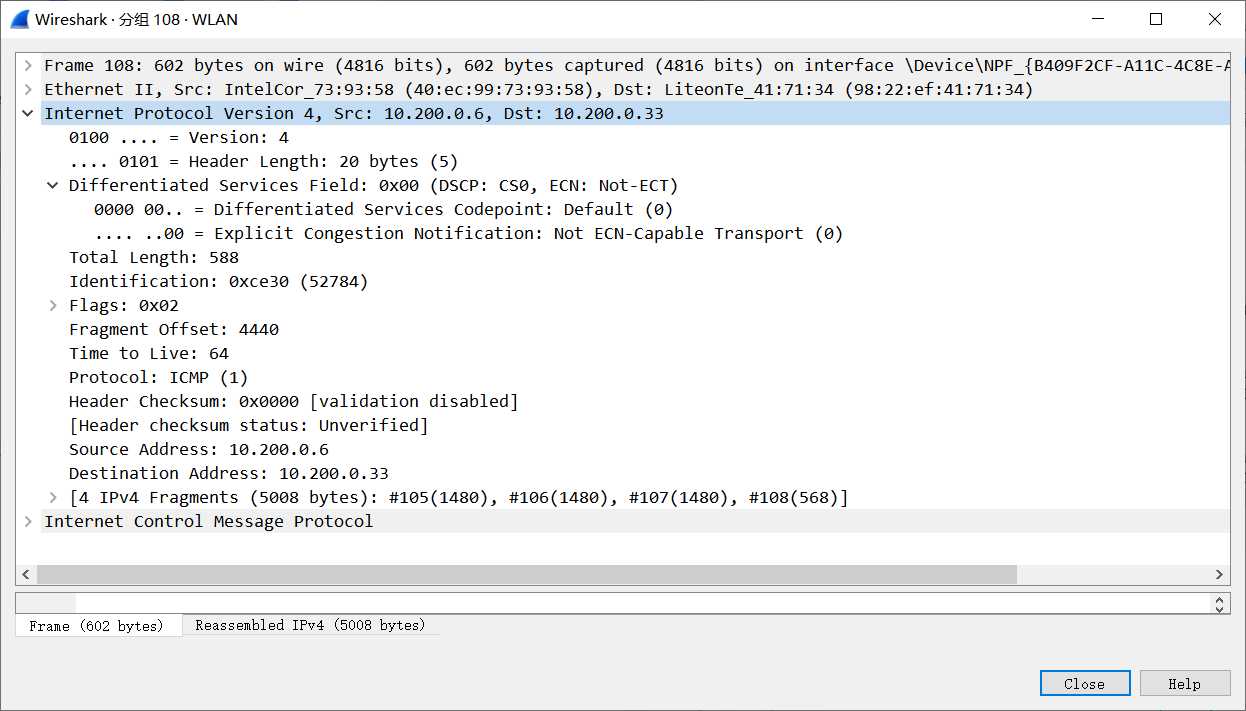


Icmp

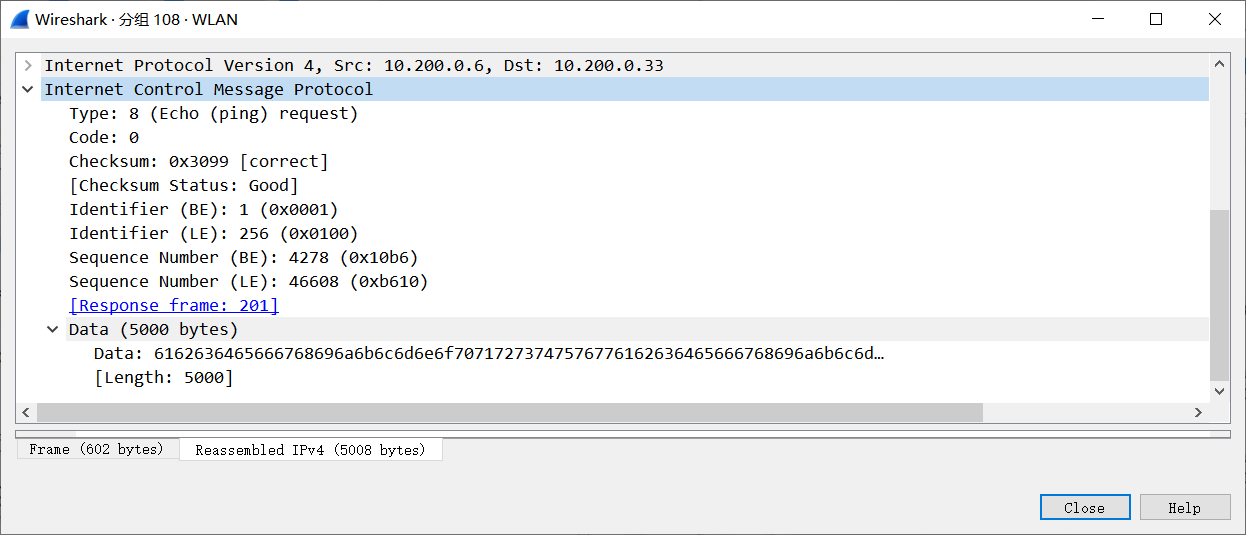
数据链路层：

目的mac地址：6字节、源mac地址：6字节、上层协议类型：ipv4，2字节

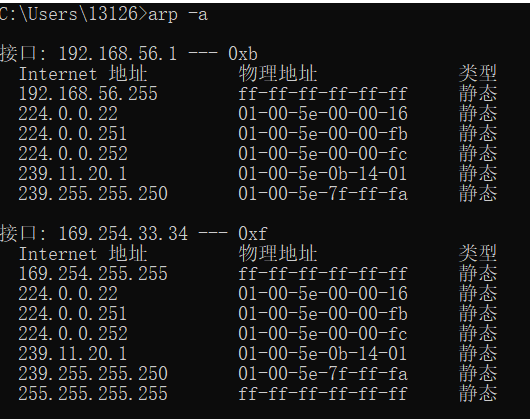
IP数据报：

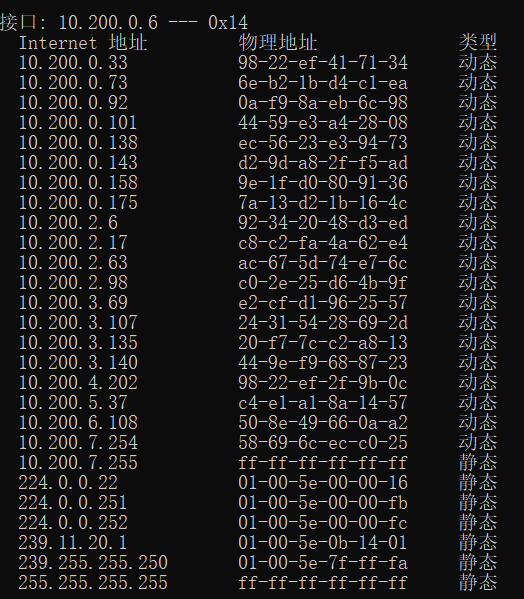


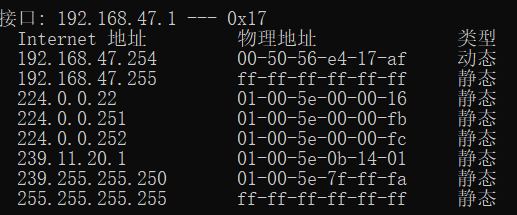
Icmp：type值为8，代码段为0，检验和为0x3099，数据长度为5000字节



3.运行ARP命令查询本机ARP缓存表；运用wireshark软件进行ARP协议截包分析。







arp请求包：

广播地址ff:ff:ff:ff:ff:ff，说明当前数据包会被广播到当前网段中的所有设备上；而这个数据包中以太网的源地址就是本机的MAC地址。Arp的报文格式：

Hardware type ：占2字节，硬件类型，标识链路层协议。

Protocol type： 占2字节，协议类型，标识网络层协。

Hardware size ：占1字节，硬件地址大小，标识MAC地址长度，这里是6个字节（48bit）。

Protocol size： 占1字节，协议地址大小，标识IP地址长度，这里是4个字节（32bit）。

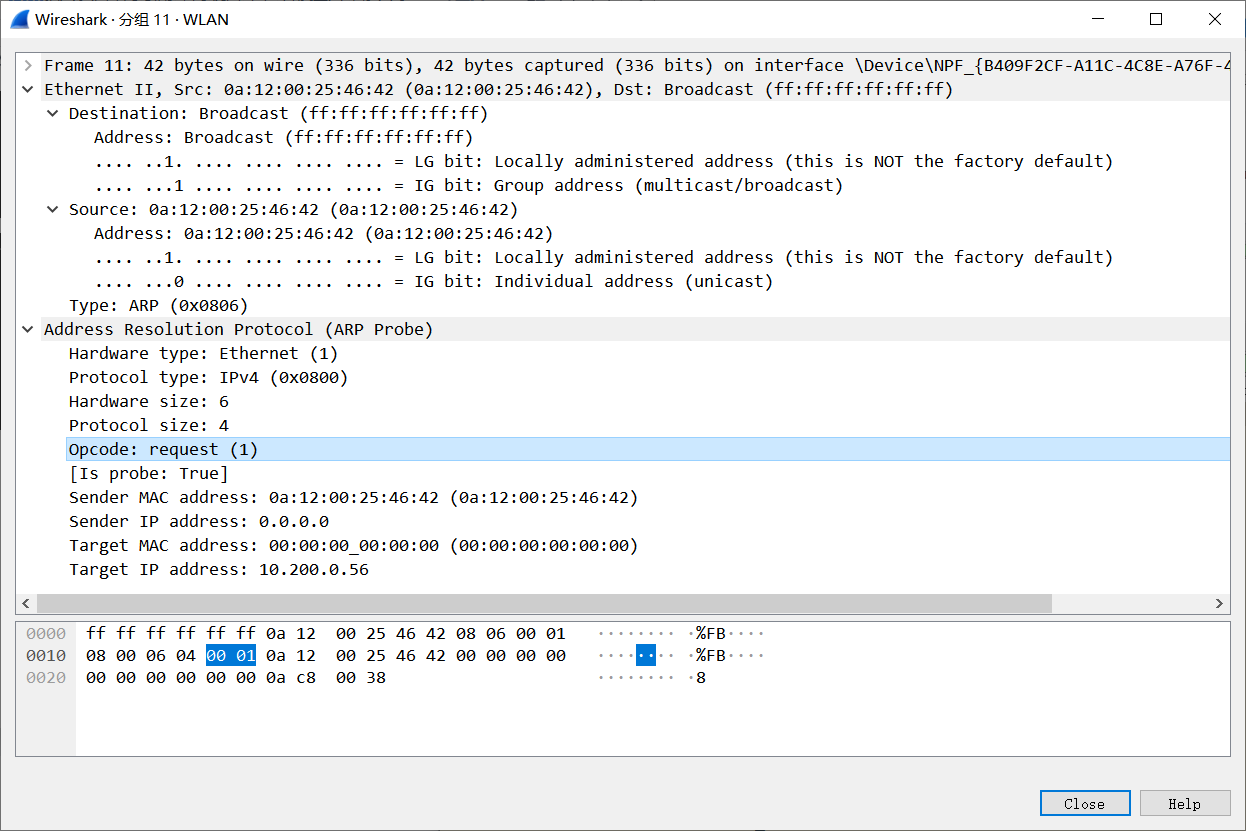
Opcode： 占2字节，操作代码，标识ARP数据包类型，1表示请求，2表示回应。

Sender MAC address ：占6字节，发送者MAC。

Sender IP address ：占4字节，发送者IP。

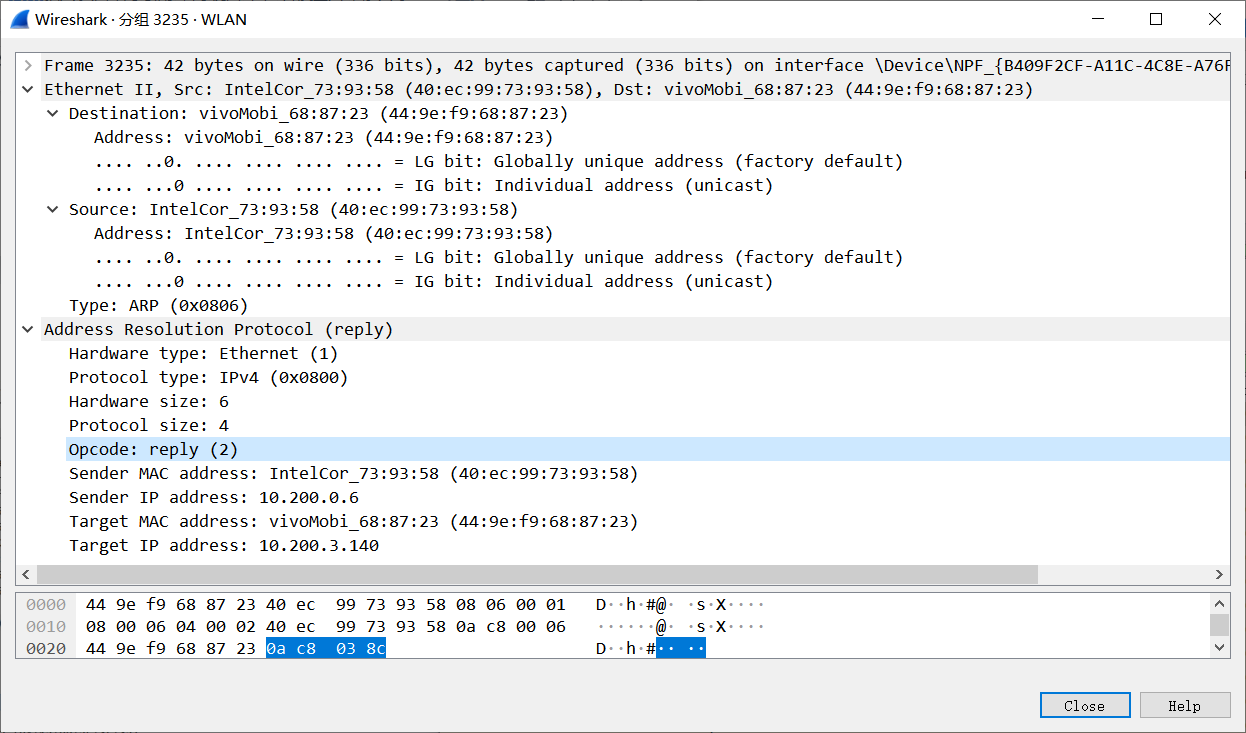
Target MAC address ：占6字节，目标MAC，此处全0表示在请求。

Target IP address： 占4字节，目标IP。



arp响应包：

此时以太网头部帧头部分的目的MAC地址为发送ARP协议地址解析请求的MAC地址，而源MAC地址为被解析的主机MAC地址



**五、实验总结**

通过本次实验，我理解并掌握了IP分片机制，IP分片是网络上传输 IP报文的一种技术手段。IP协议在传输数据包时，将数据报文分为若干分片进行传输，并在目标系统中进行重组。理解了TCP/IP协议定义了一个在因特网上传输的包,称为IP数据报，这是一个与硬件无关的虚拟包,由首部和数据两部分组成，首部的前一部分是固定长度，共 20 字节，是所有IP数据报必须具有的，在首部的固定部分的后面是一些可选字段，其长度是可变的。掌握了ARP协议工作原理和格式，并能熟悉应用wireshark抓包软件。