1.实验名称+个人信息

实验二 刘铭涵 37220232203751

2.实验目的

学习捕获和分析网络数据包

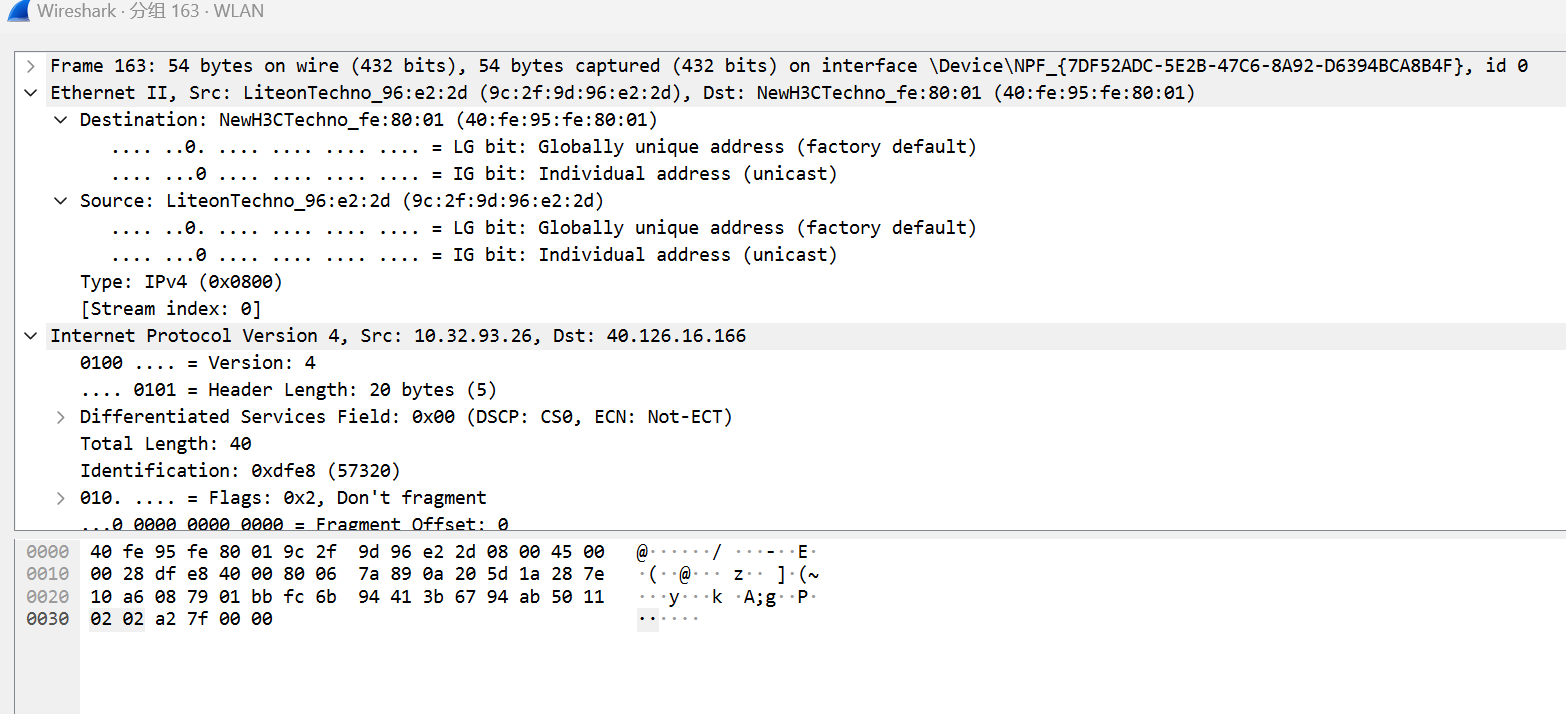
掌握以太网MAC帧、802.11数据帧和IPv4/IPv6数据包的构成，了解各字段的含义

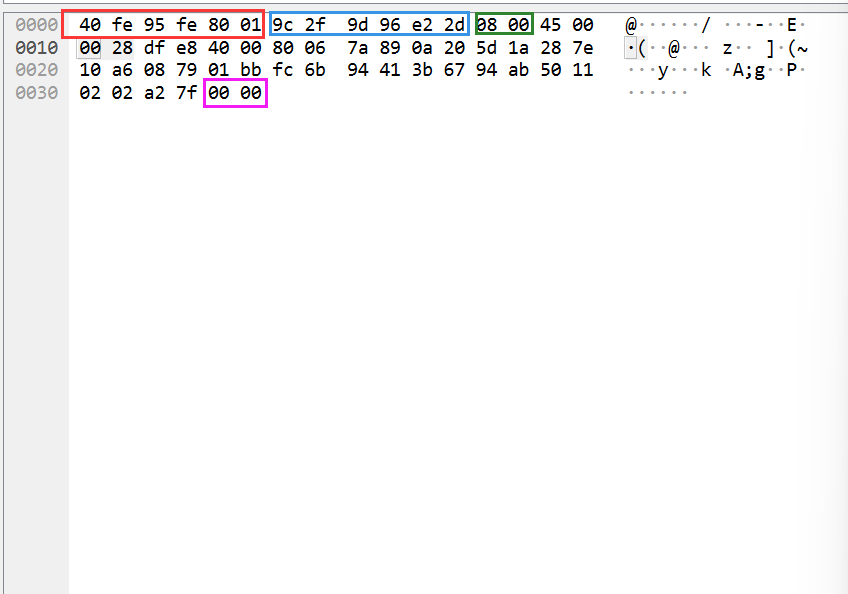
掌握ICMP协议，ping和tracert指令的工作原理

掌握ARP协议的请求/响应机理

3.实验内容/步骤，结果和分析

1.1 观察MAC帧格式





红色是目的地址

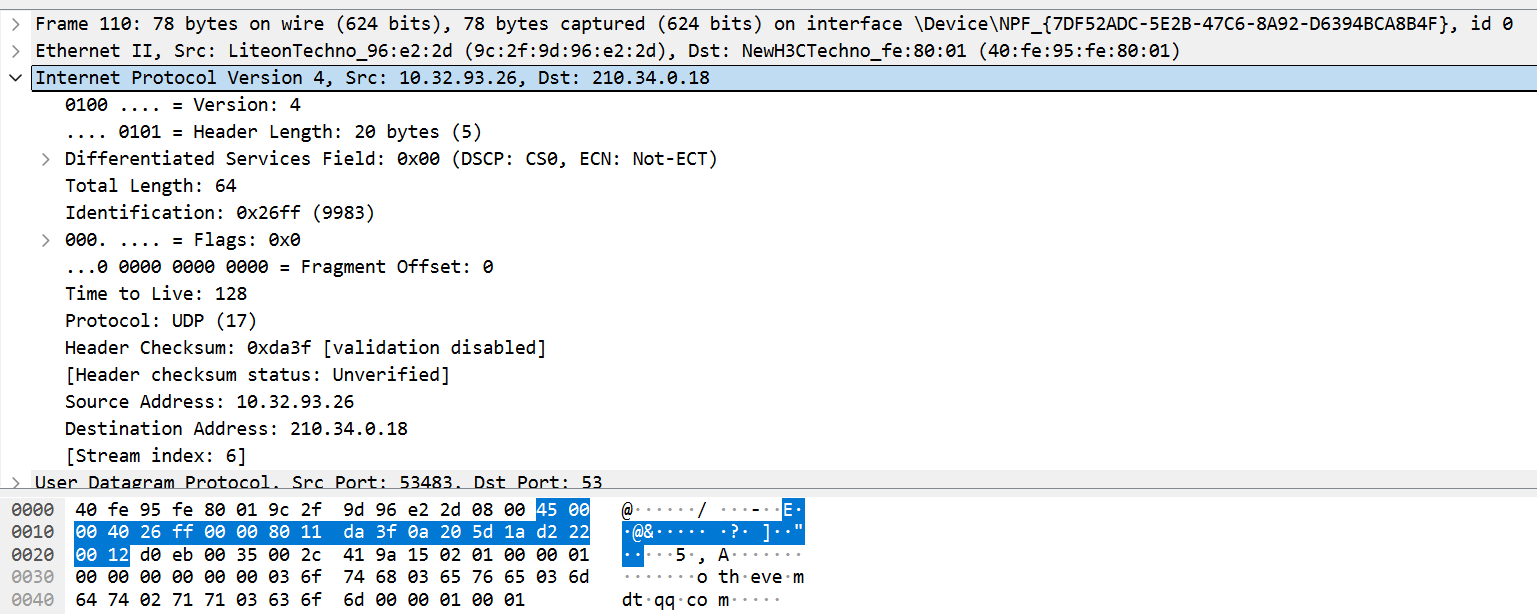
蓝色是源地址

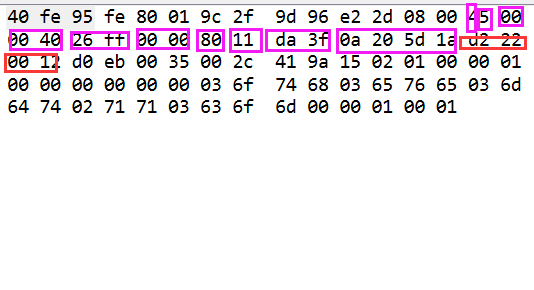
绿色是类型

紫色是FCS

其他部分是数据

1.2 观察IP数据报的首部结构

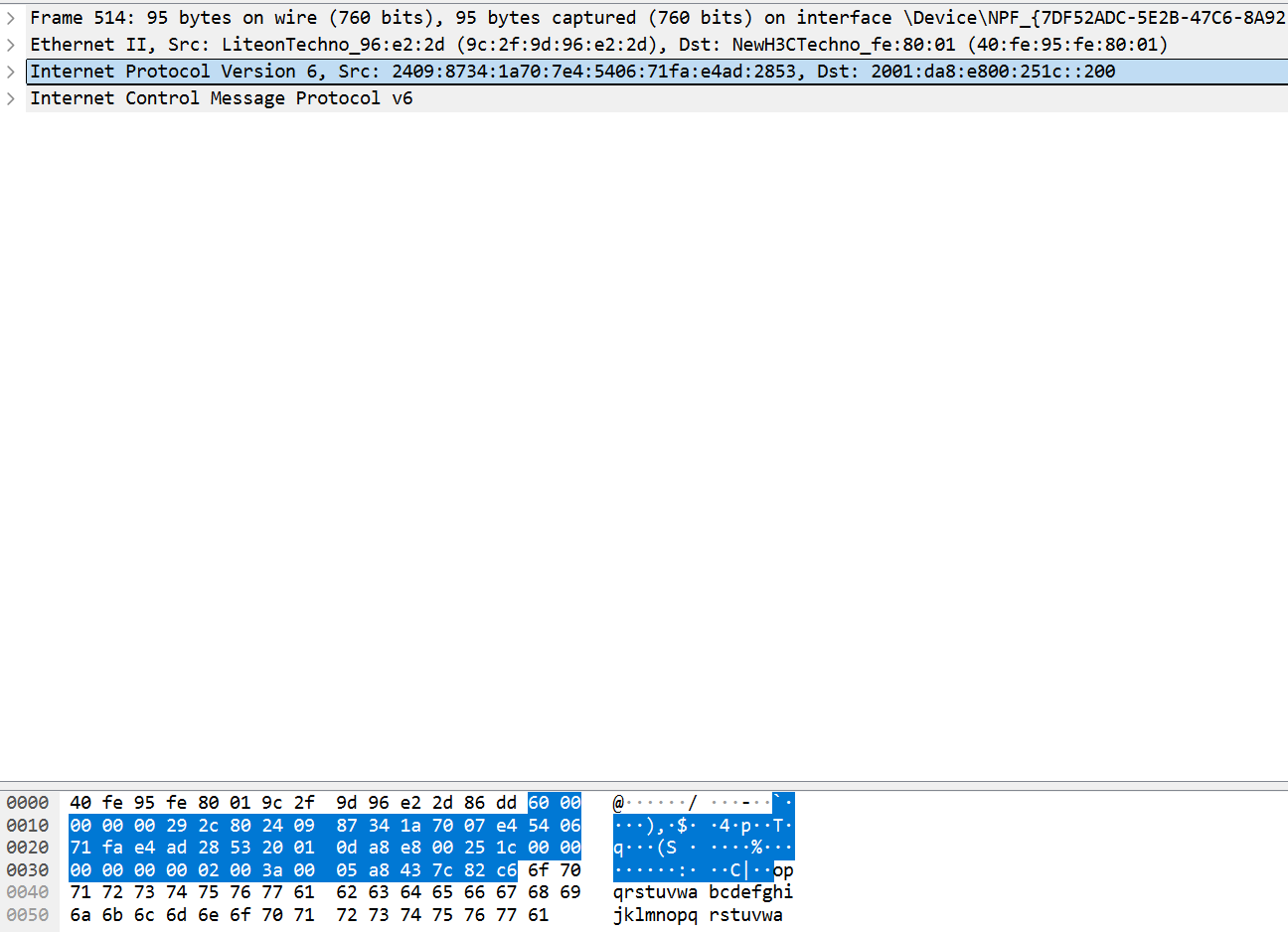




（红色部分连在一起）

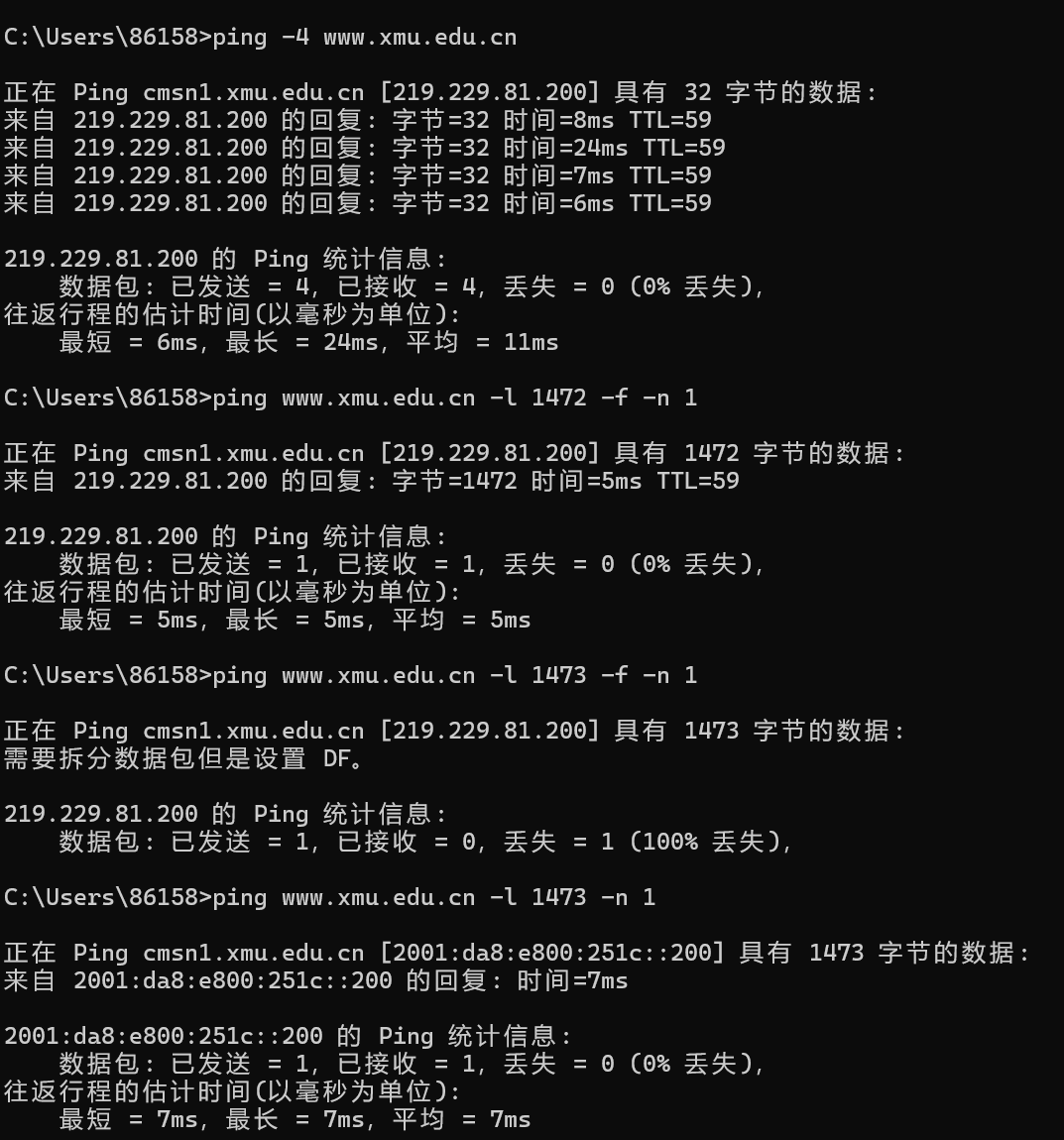
按照分割，从前往后分别是版本，首部长度，TOS，总长度，标识，（标志位与片偏移），TTL，协议，首部校验和，源IP地址，目的IP地址

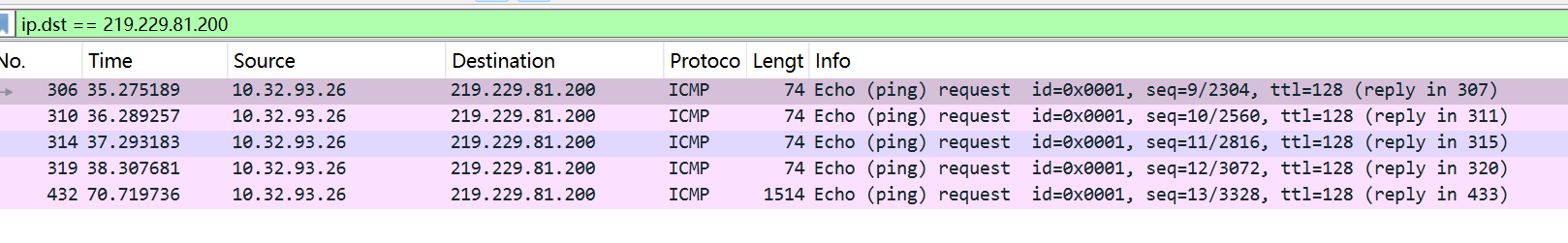
以下是IPv6数据报

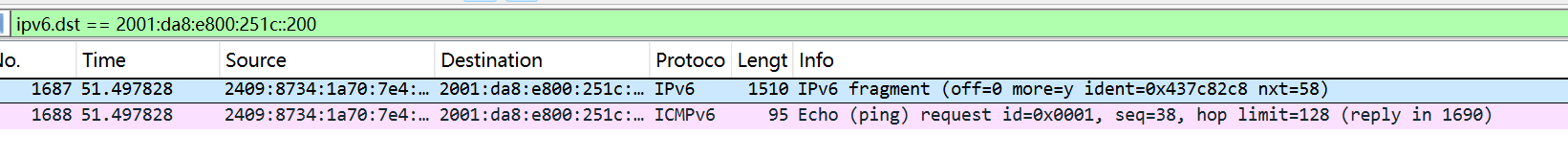


IPv4数据报与IPv6数据报长度不一样

1.3







验证了发送的字节数量

(c)的数据包全部丢失，其他没有。

1. 这个命令会尝试使用IPv4地址来ping
2. 此命令尝试发送一个大小为1472字节的数据包（不包括ICMP头），并且要求数据包不分段。

结果没有丢包。

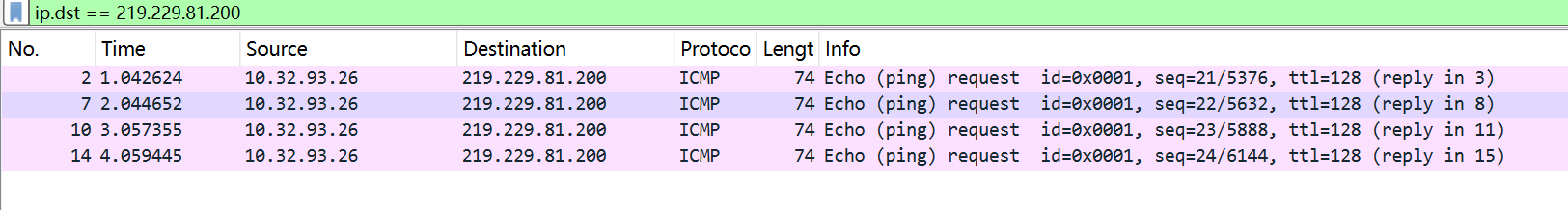
1. 类似于命令(b)，但数据包大小增加到1473字节。‘

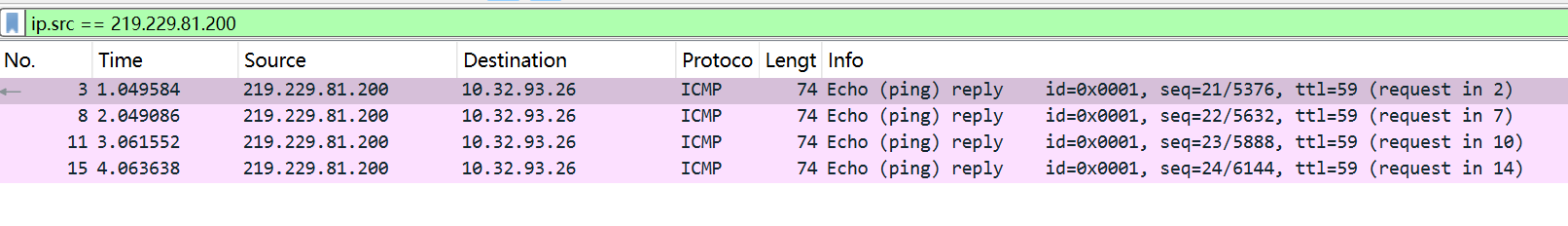
由于数据包比命令(b)中的稍大，如果路径上的MTU小于或等于1472字节，会遇到数据包太大而无法通过某个网络设备。

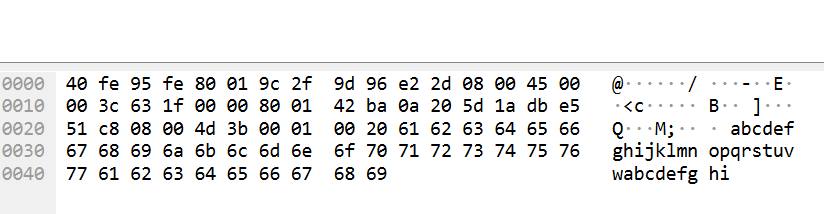
实际运行时，全部丢包。

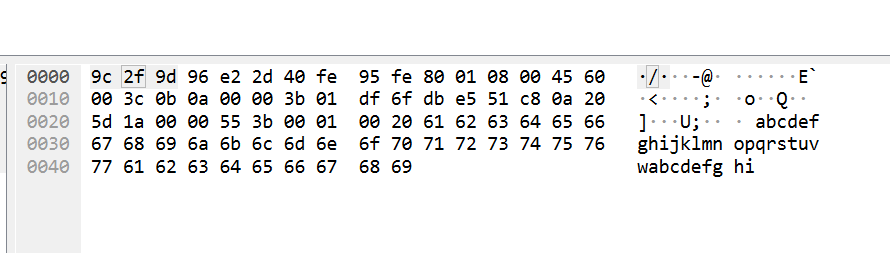
1. 此命令与命令(c)相似，但缺少-f参数。数据包在传输过程中可能会被分割成较小的片段，以适应路径上任何较小的MTU。

1.4





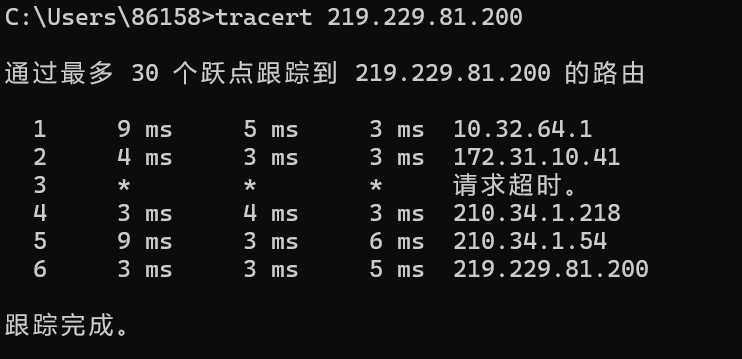


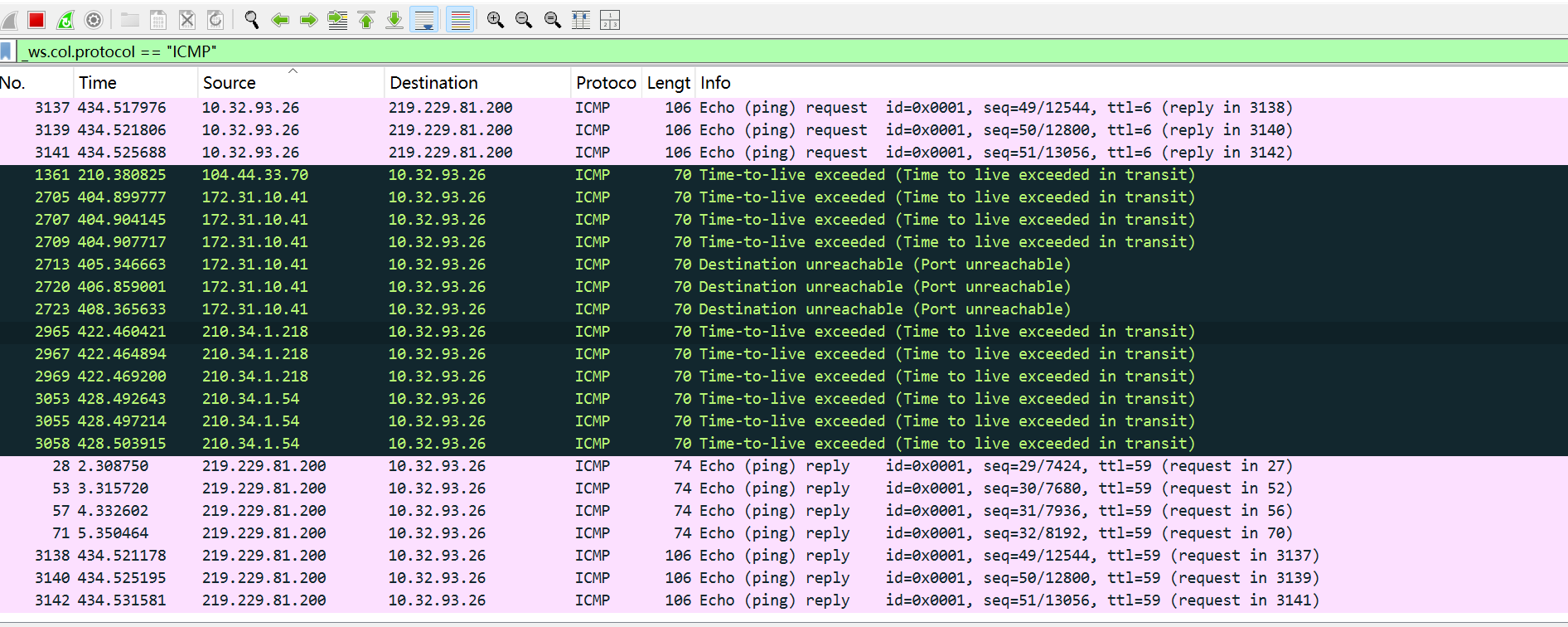


执行一次ping命令，共有4个ICMP请求帧和回应帧

对应IP头部的变化：源地址，目的地址互换，类型一样。

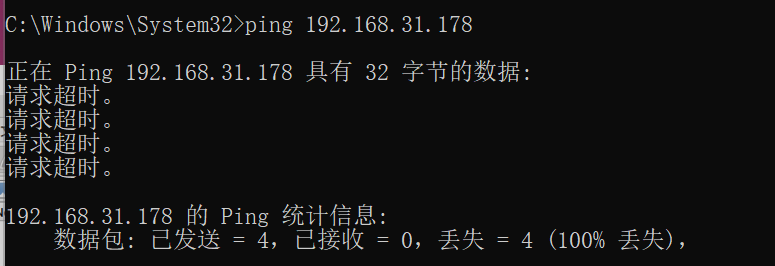
1.5

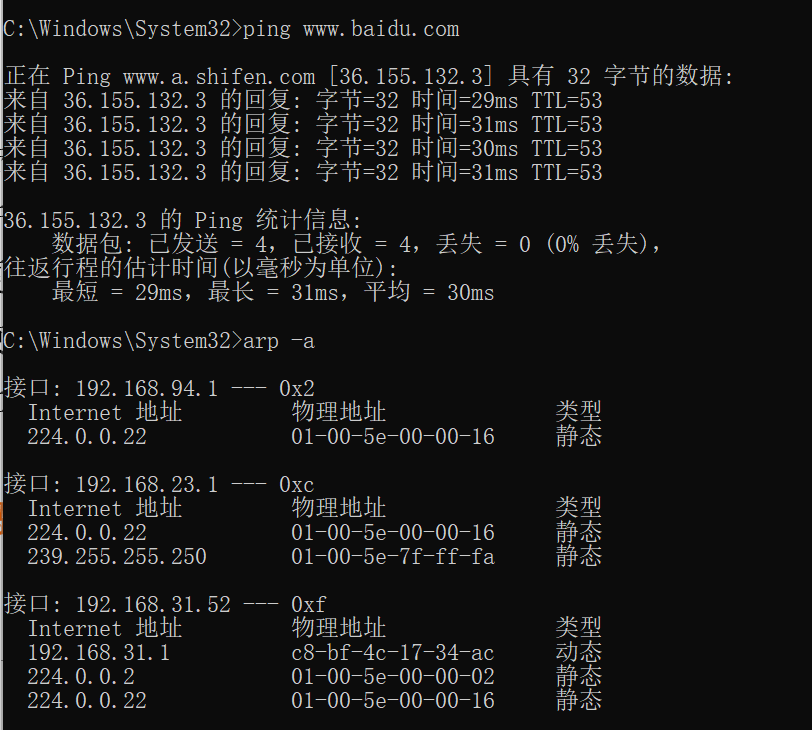


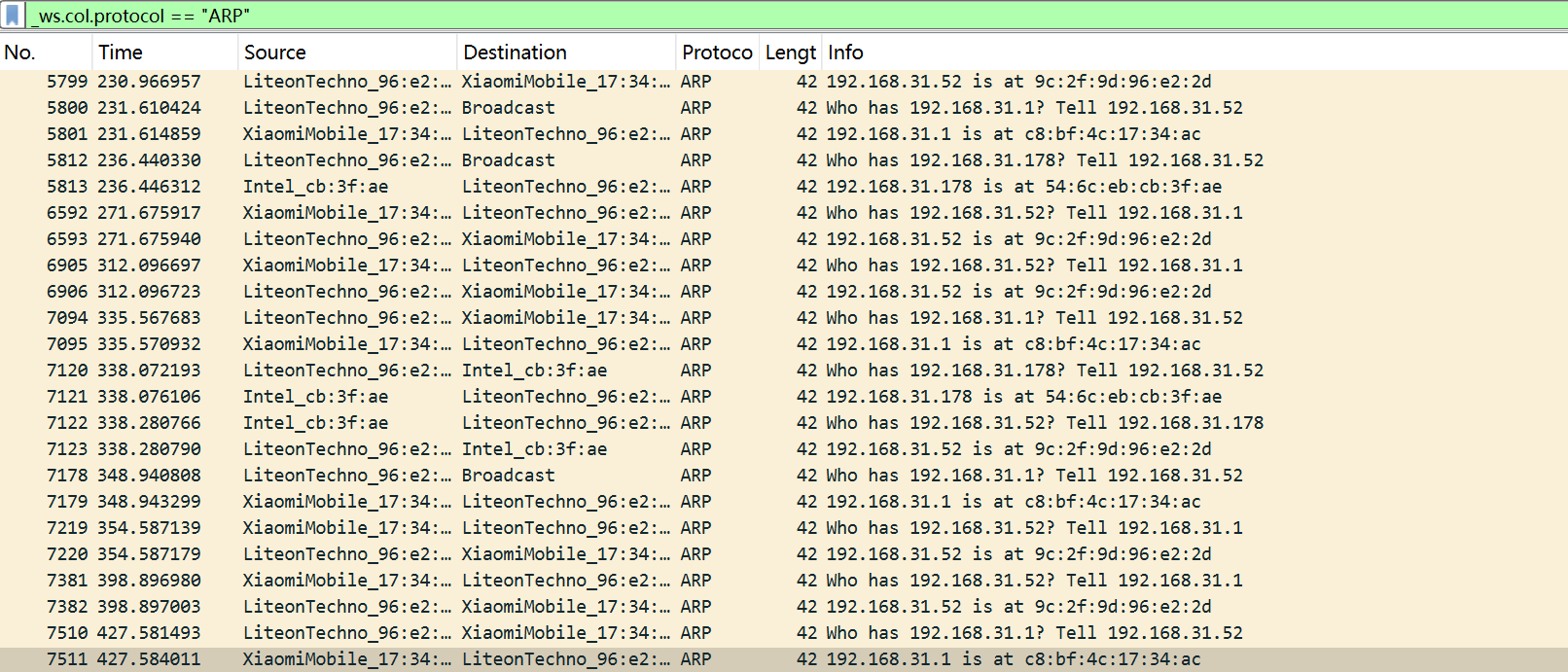


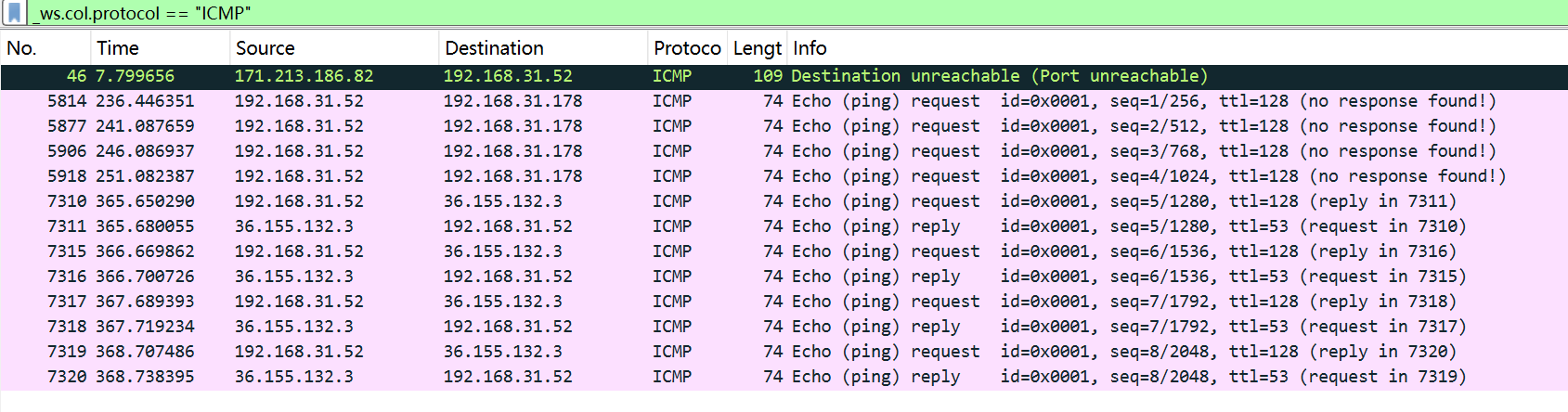
这个工具通过发送一系列Internet控制消息协议（ICMP）回声请求消息（或有时使用其他IP协议的数据包，如UDP或TCP，当ICMP被阻止时）到目标地址，并逐渐增加每个数据包的生存时间（TTL）值来工作。

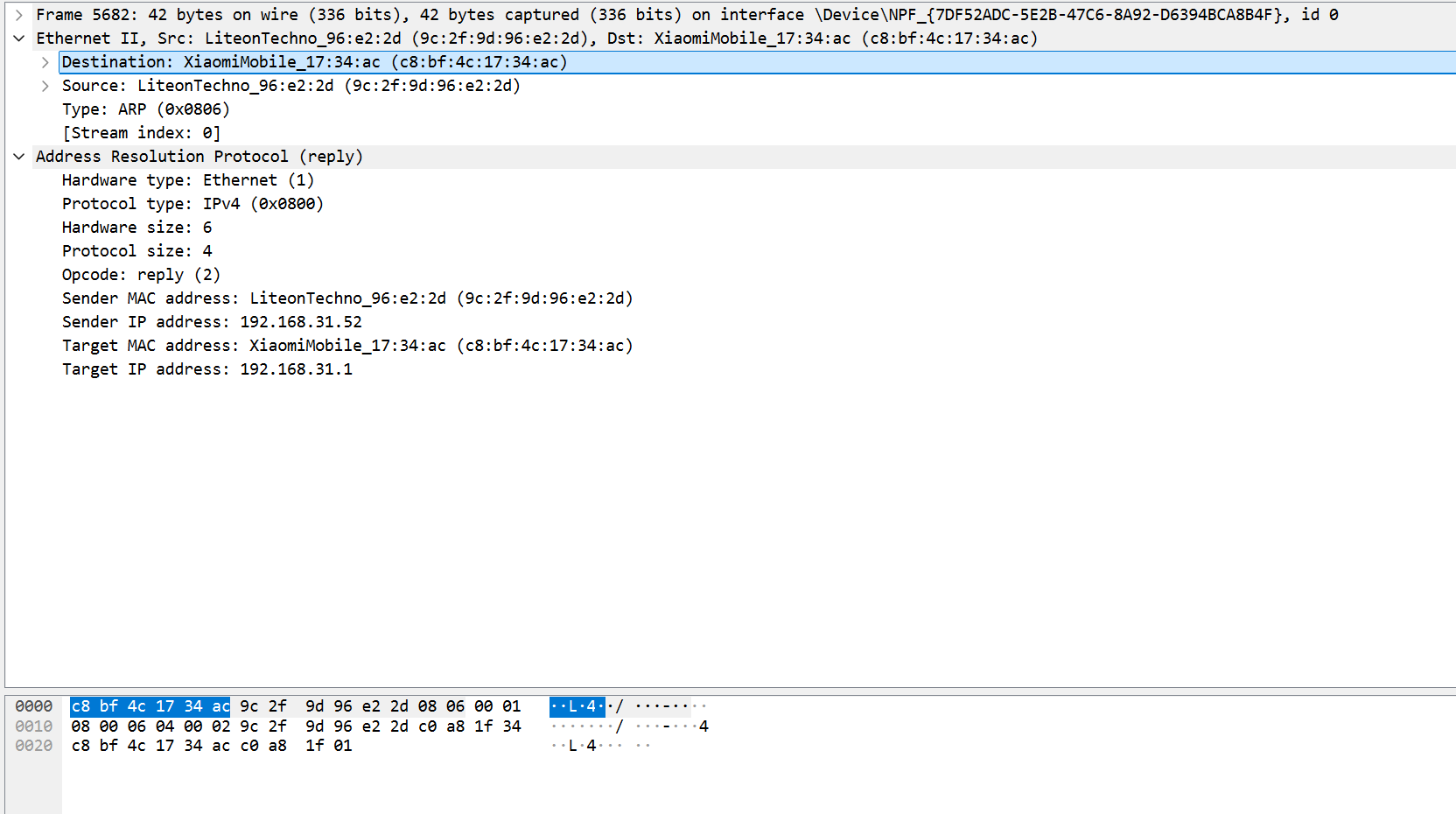
1.6









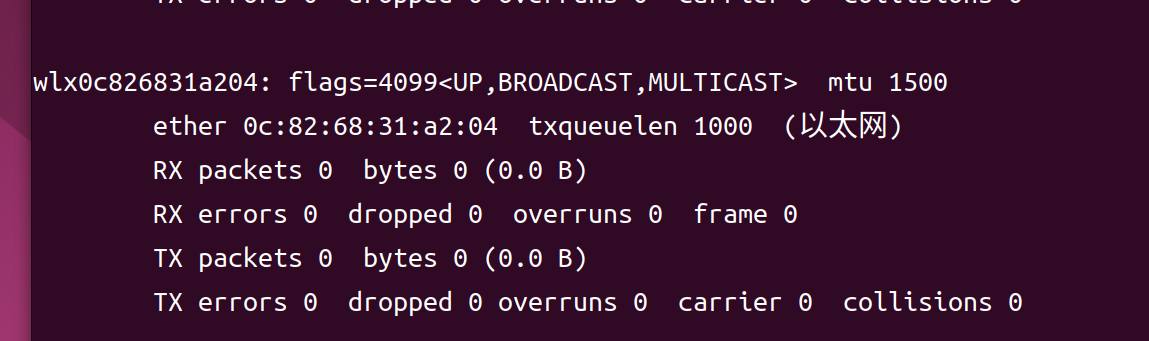


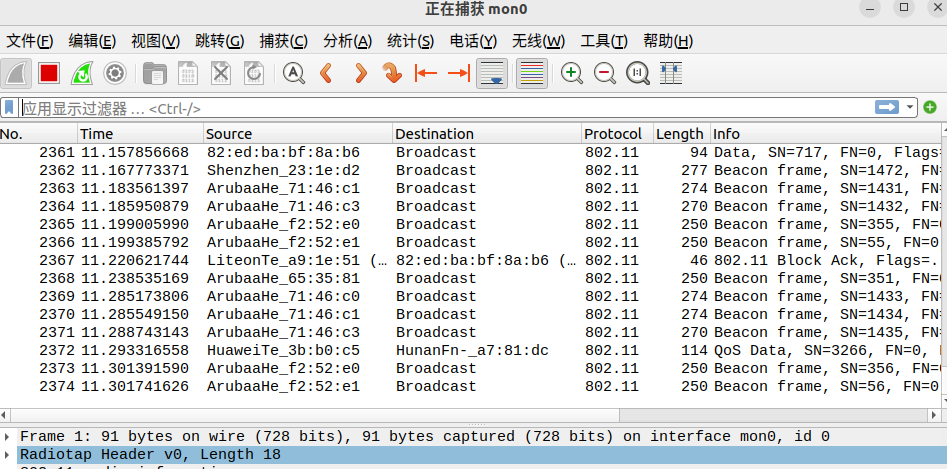
字段和含义在右边的info

解释：点击对应字段，蓝色对应的部分就是对应内容

局域网内的ARP请求是直接在局域网内广播的，而局域网外的ARP请求需要通过路由器或网关进行转发，并且可能不会直接使用ARP协议来解析IP地址。在实际应用中，局域网外的主机通常使用路由协议而不是ARP来确定如何将数据包发送到目标网络。

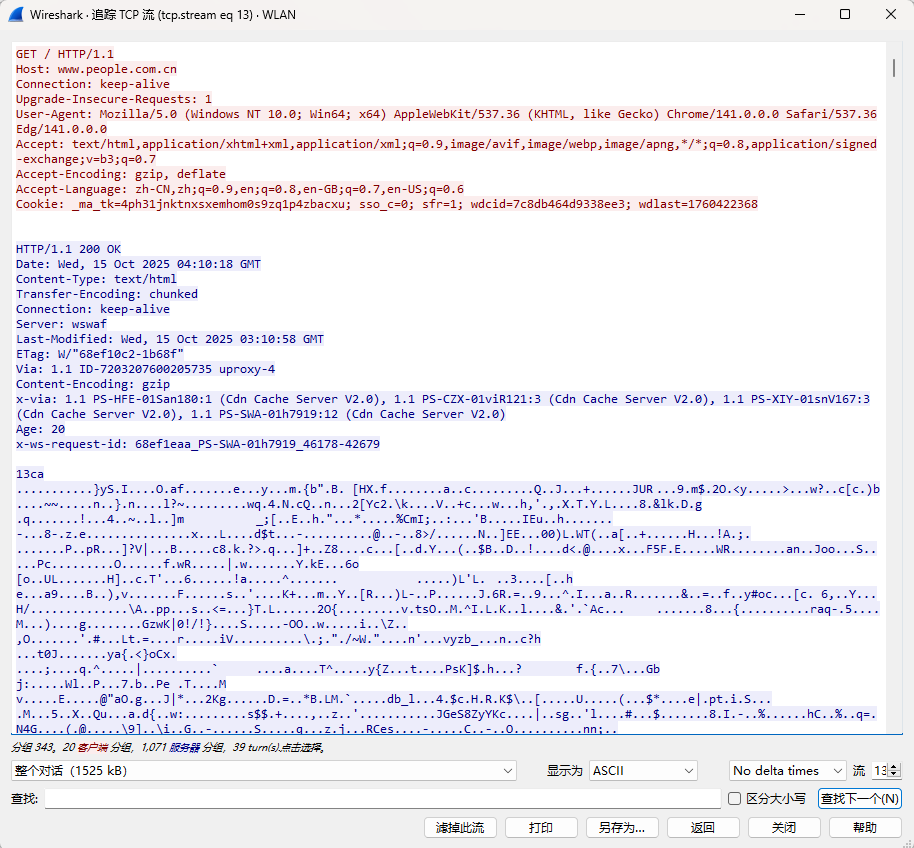
2捕获和分析802.11数据





3.1 数据流追踪

显然红色部分是客户端发送的请求，蓝色部分是服务器返回的响应。



4.实验小结/感想

通过本次实验，我深入理解了网络数据包的基本捕获与分析方法，掌握以太网MAC帧、802.11数据帧以及IPv4/IPv6数据包的构成细节，明确各字段的具体含义。同时，我熟练掌握了ICMP协议及其在应用中的两个重要指令——ping和tracert的工作原理，以及ARP协议的请求/响应机制。本次实验我深刻体会到网络数据包捕获与分析在网络安全、网络性能优化及故障排除等方面的重要性。掌握了这些技能，我能够更深入地理解网络通信的底层机制，有效地识别和解决网络问题。本次实验是一次宝贵的学习经历，它不仅增强了我的理论知识，还提高了我的实践操作能力。