# 信息安全课程实验二

## 1、实验目的

学习虚拟机安装、版本控制Git软件、收发包、抓包软件使用及初步具备协议分析能力；

## 2、实验工具

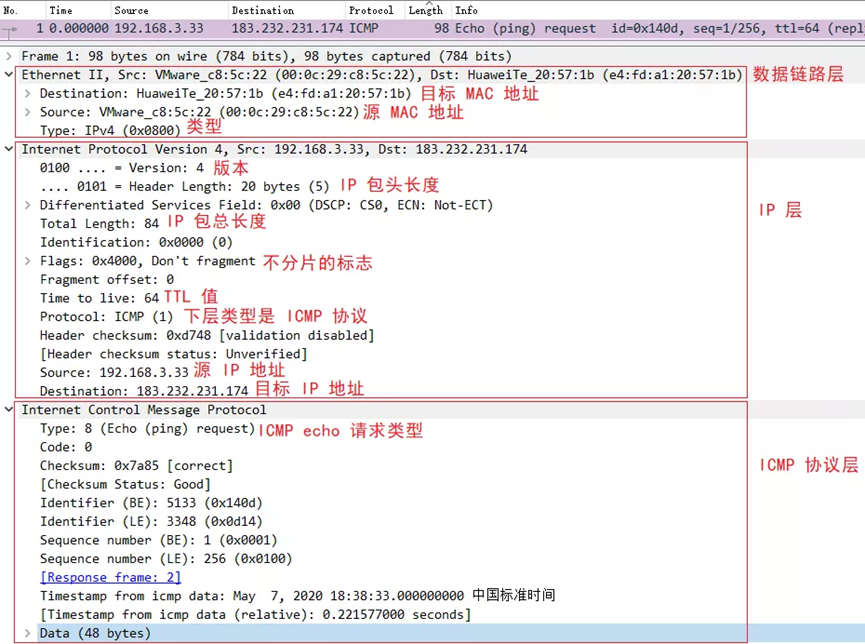
Centos6以上系统、GitHub、科来数据包生成器/科来数据包播放器软件（pktbuilder\_x64/pktplayer\_x64）、Wireshark

## 3、实验内容

A 采用科来数据包生成器生成三种ARP协议数据包（请求、应答、免费(Gratuitous ARP)三种形式的ARP包；

B 并采用科来数据包播放器软件将三种伪造数据包向攻击目标机发送，检验三种形式的ARP包是否具备断网攻击能力（采用ARP命令查看攻击前后的目标机ARP缓存表是否发生变化并截图说明）

C 整个攻击过程采用Wireshark进行抓包，并参考如下图对三种ARP协议进行协议分析和标注，同时对应攻击数据包导出以pcap包格式保存；



D 针对ARP攻击，如何进行防护，请提出自己的意见和建议

3.1 ARP请求包的生成及发送

如图3.1所示，发送ARP请求包的格式

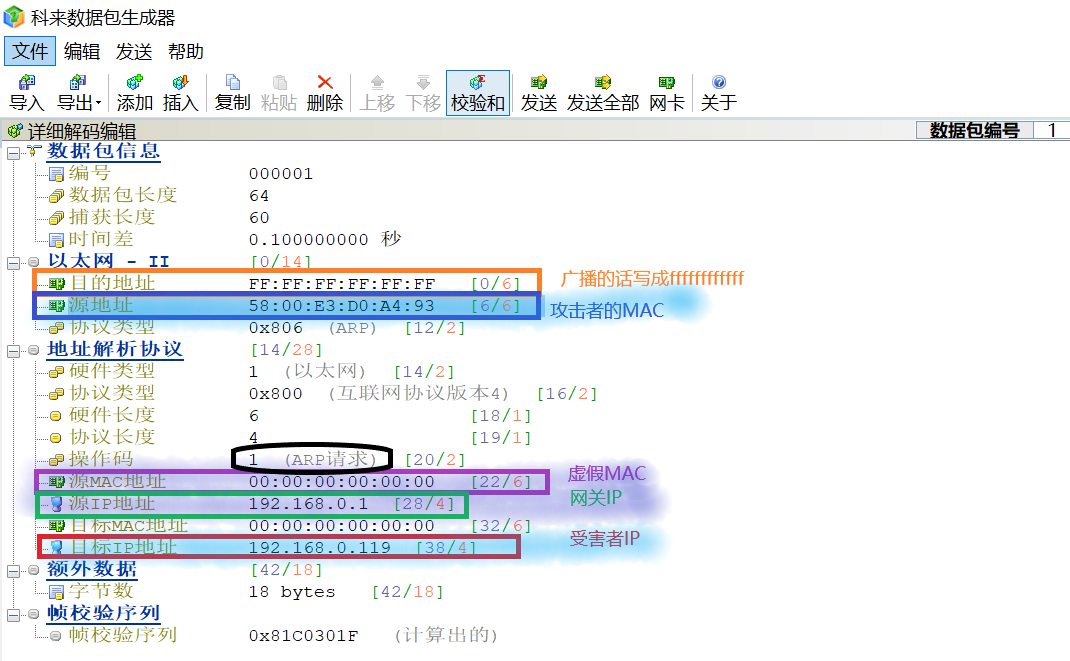


图3.1 ARP请求包的发送

发送数据前的arp缓存表

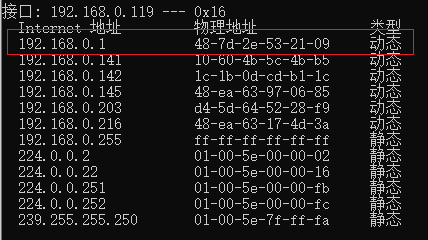


图3.2发送arp请求包前的缓存表

发送ARP请求包后的arp缓存表

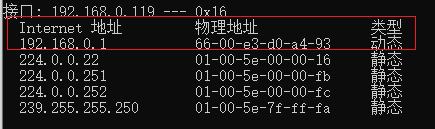


图3.3发送arp请求包后的缓存表

电脑显示已经断网；并对所发送的数据包进行抓取，可以得到以下数据

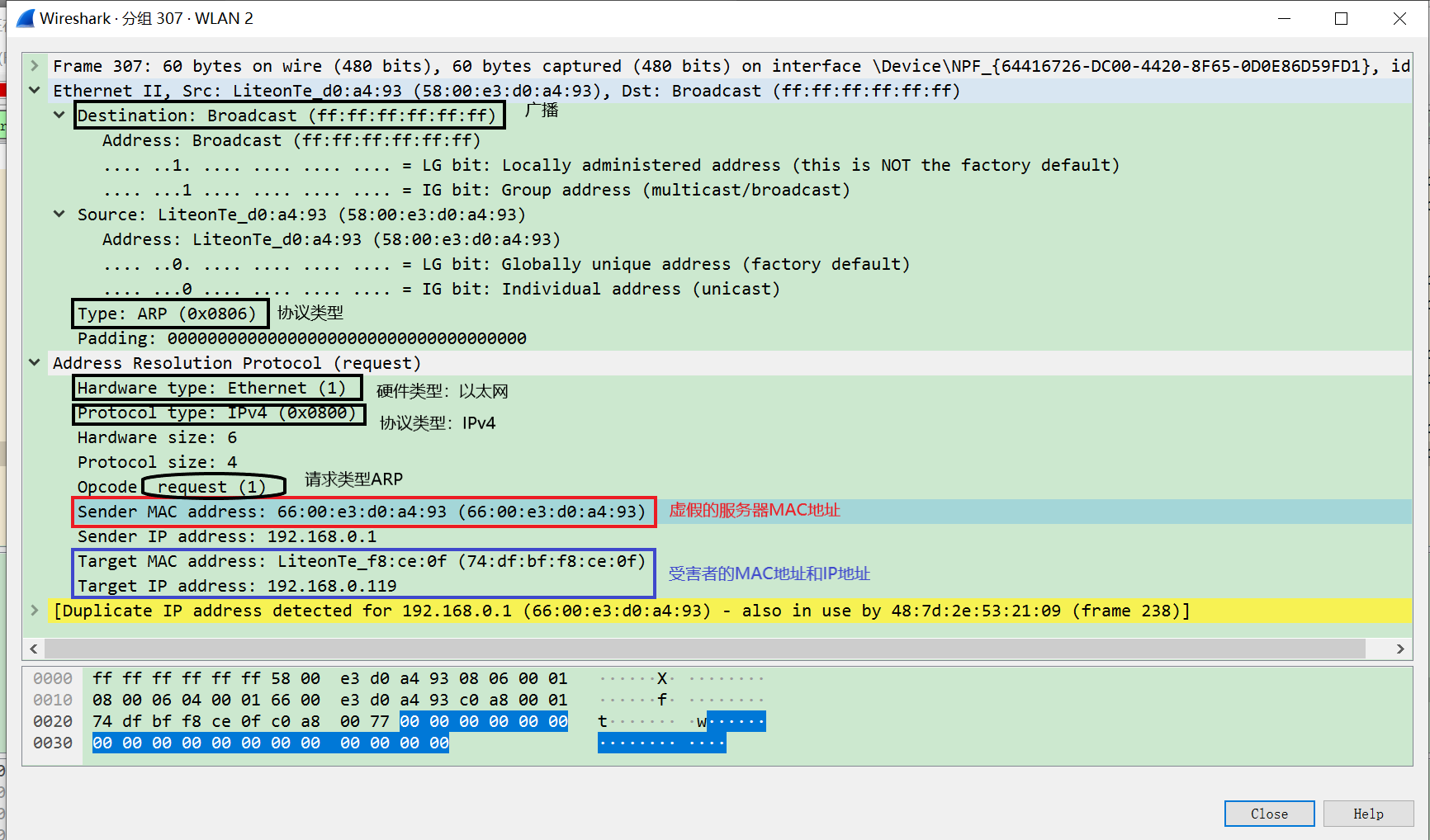


图3.4抓取arp请求包并分析

3.2. ARP应答包的生成及发送

如图3.5所示，发送ARP回复包的格式

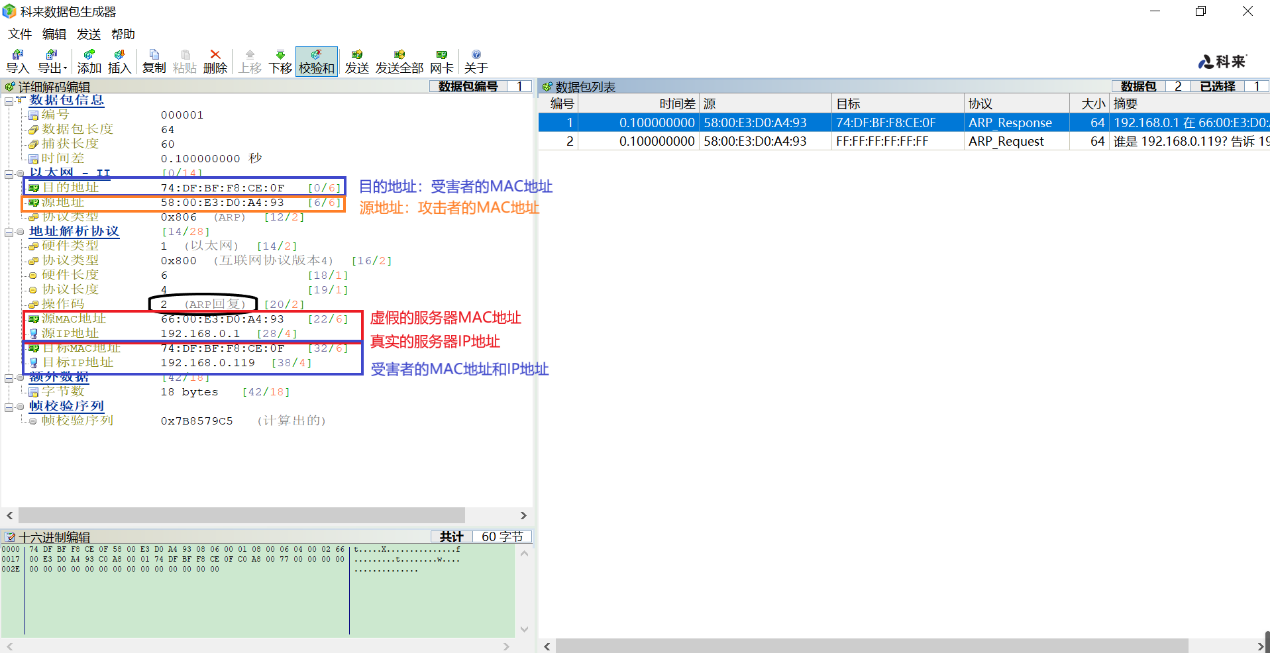


图3.5 ARP回复包的发送

发送数据前的arp缓存表

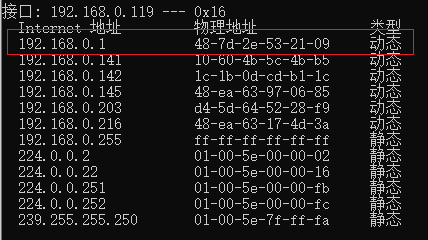


图3.6发送arp回复包前的缓存表

发送ARP回复包后的arp缓存表

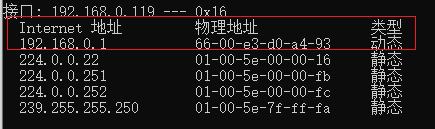


图3.7发送arp请求包后的缓存表

可以看到电脑显示已经断网；并对所发送的数据包进行抓取，可以得到以下数据

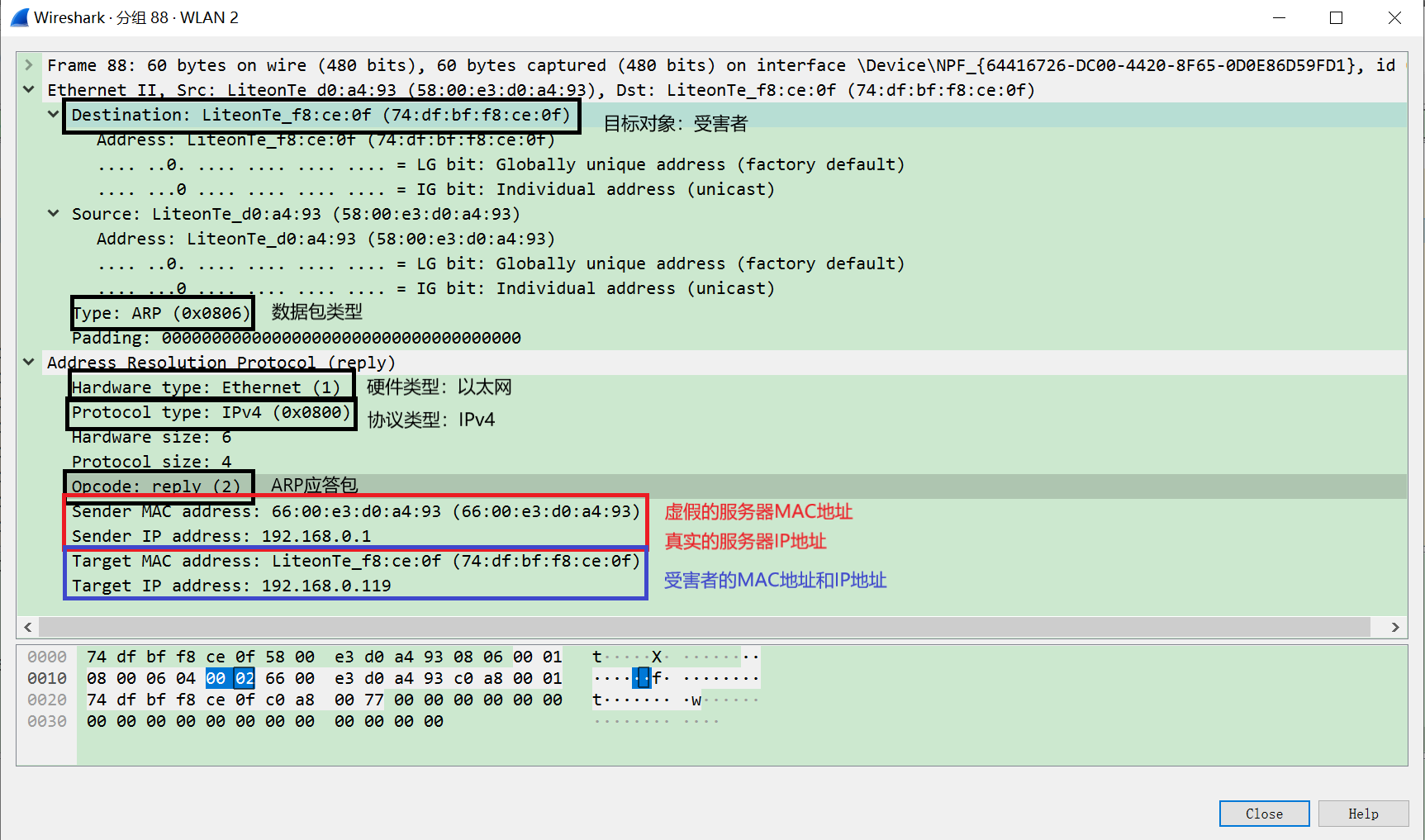


图3.8抓取arp回复包并分析

3.3. ARP免费包的生成及发送

如图3.9所示，发送ARP免费包的格式[1],[2]

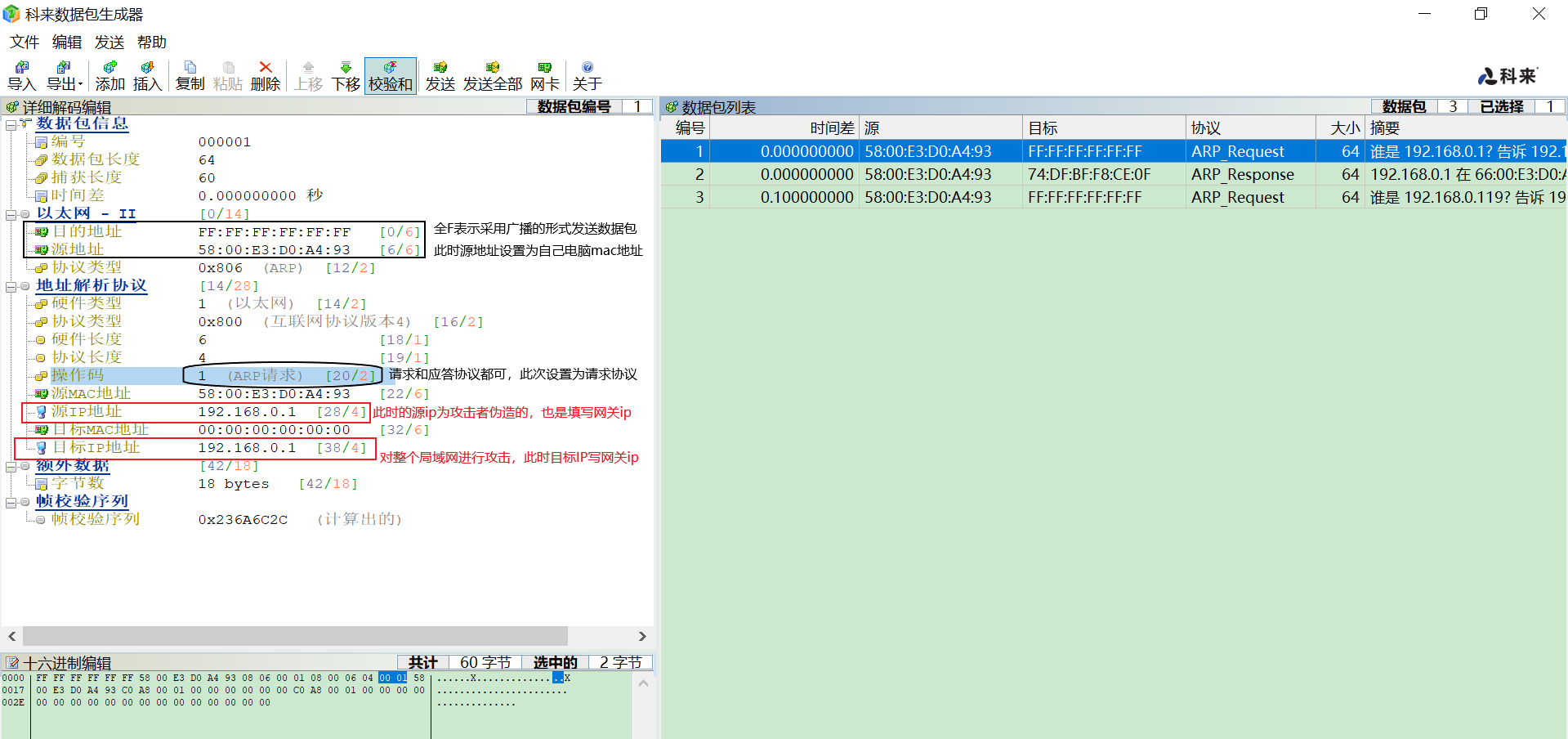


图3.9 ARP免费包的发送

其中58:00:E3:D0:A4:93是被请求的MAC地址，正常情况下，如果不是免费ARP，这里应该为全0，在响应的时候，由目的主机来填写，但是在免费ARP的请求报文中，这里已经自动填写上自身的MAC地址。

对arp免费包进行数据抓取，得到以下数据分析

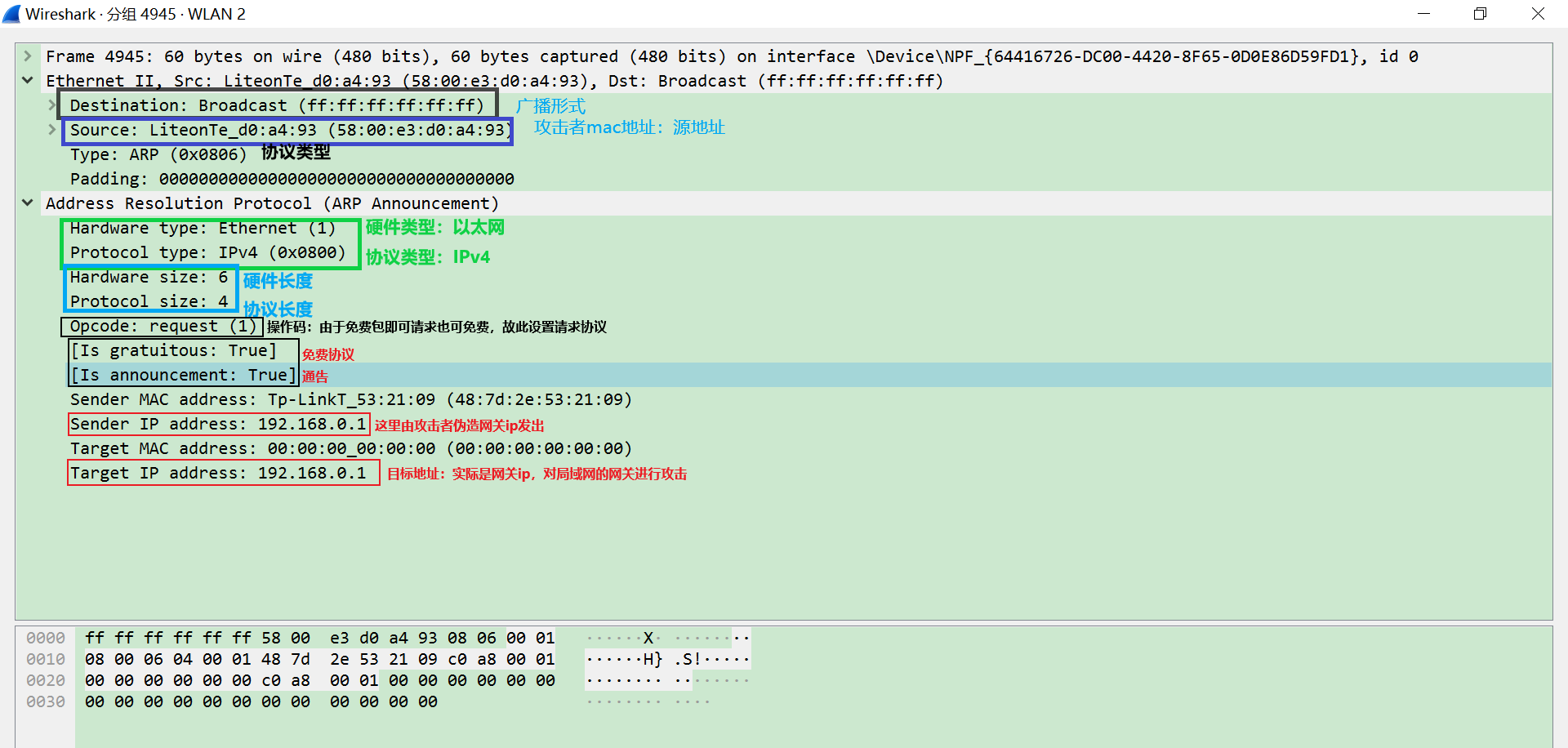


图3.10 arp免费包数据分析

## 4、实验总结

1.连接网络时，最好不要连校园网；

2.对于攻击者和受害者的ip和mac地址要要弄清楚，对于攻击者要做什么事，要知道些什么内容要理解，对于各协议要知道做了什么；

3.对于网络协议的分析要理解。

# 参考文献

[1]<https://www.zhihu.com/question/64514922/answer/221264172>

[2]https://blog.csdn.net/ethan0ly/article/details/53793078