信息安全课程实验二--实验报告

1. **实验目的**

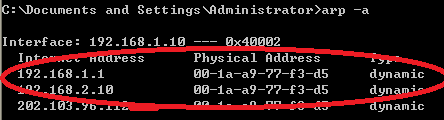
学习虚拟机安装，版本控制Git软件、收发包、抓包软件使用及初步具备协议分析能力；

1. **实验工具**

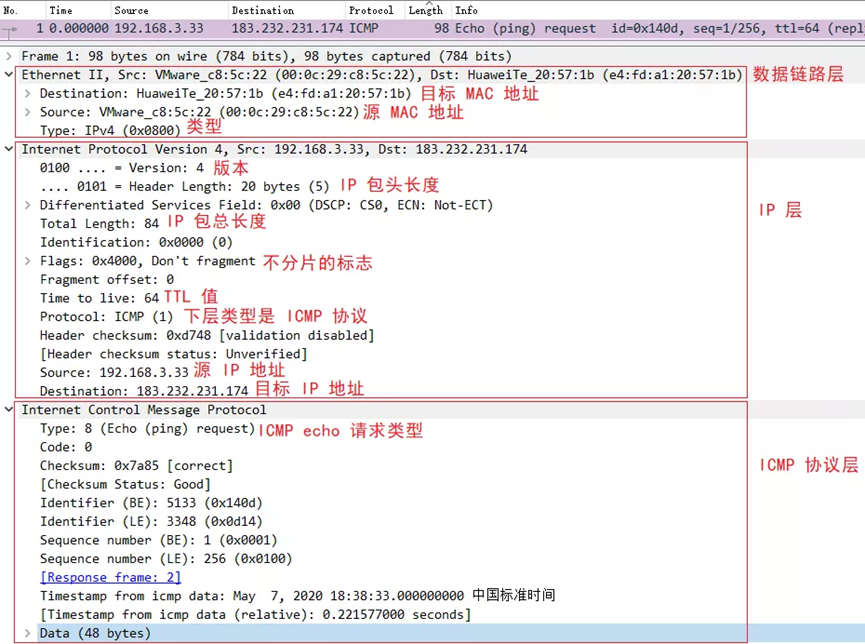
Centos6以上系统，GitHub，科来数据包生成器/科来数据包播放器软件（pktbuilder\_x64/pktplayer\_x64），Wireshark

1. **实验内容**
2. 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、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）



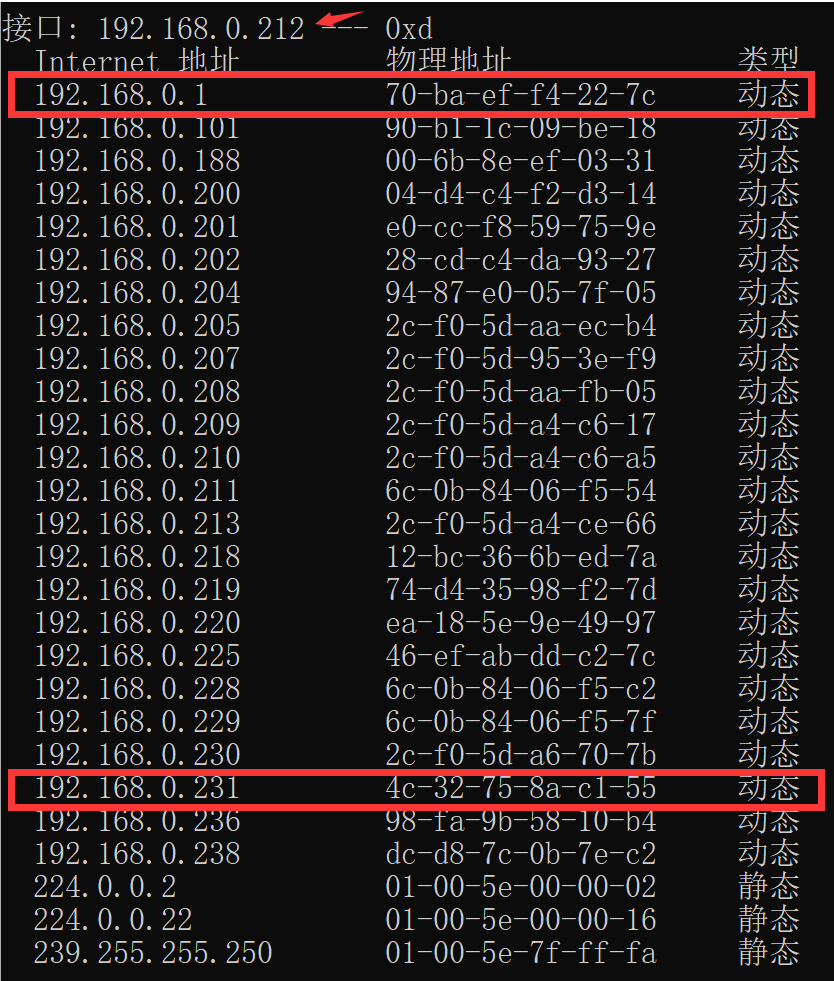
C、整个攻击过程采用Wireshark进行抓包并参考如下图对三种ARP协议进行协议分析和标注，同时对应攻击数据包导出以pcap包格式保存；



D、针对ARP攻击，如何进行防护，请提出自己的意见和建议。

1. **实验过程**

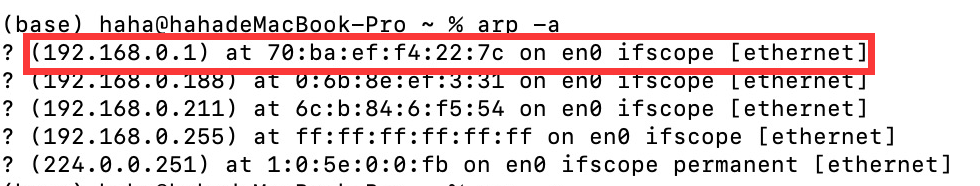
局域网内所有主机IP和mac地址信息如下：



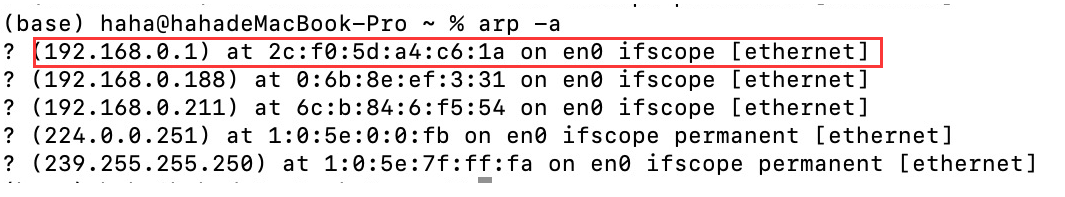
|  |  |  |
| --- | --- | --- |
| 主机 | IP地址 | MAC地址 |
| 网关 | 192.168.0.1 | 70:ba:ef:f4:22:7c |
| 本机(攻击者) | 192.168.0.212 | 2c:f0:5d:a4:c6:1a |
| Mac电脑(受害者) | 192.168.0.231 | 4c:32:75:8a:c1:55 |

1. **请求形式的ARP包**

1.用科来数据包播放器软件将伪造数据包向受害者主机发送，用arp命令查看攻击前后的目标机ARP缓存表截图如下：

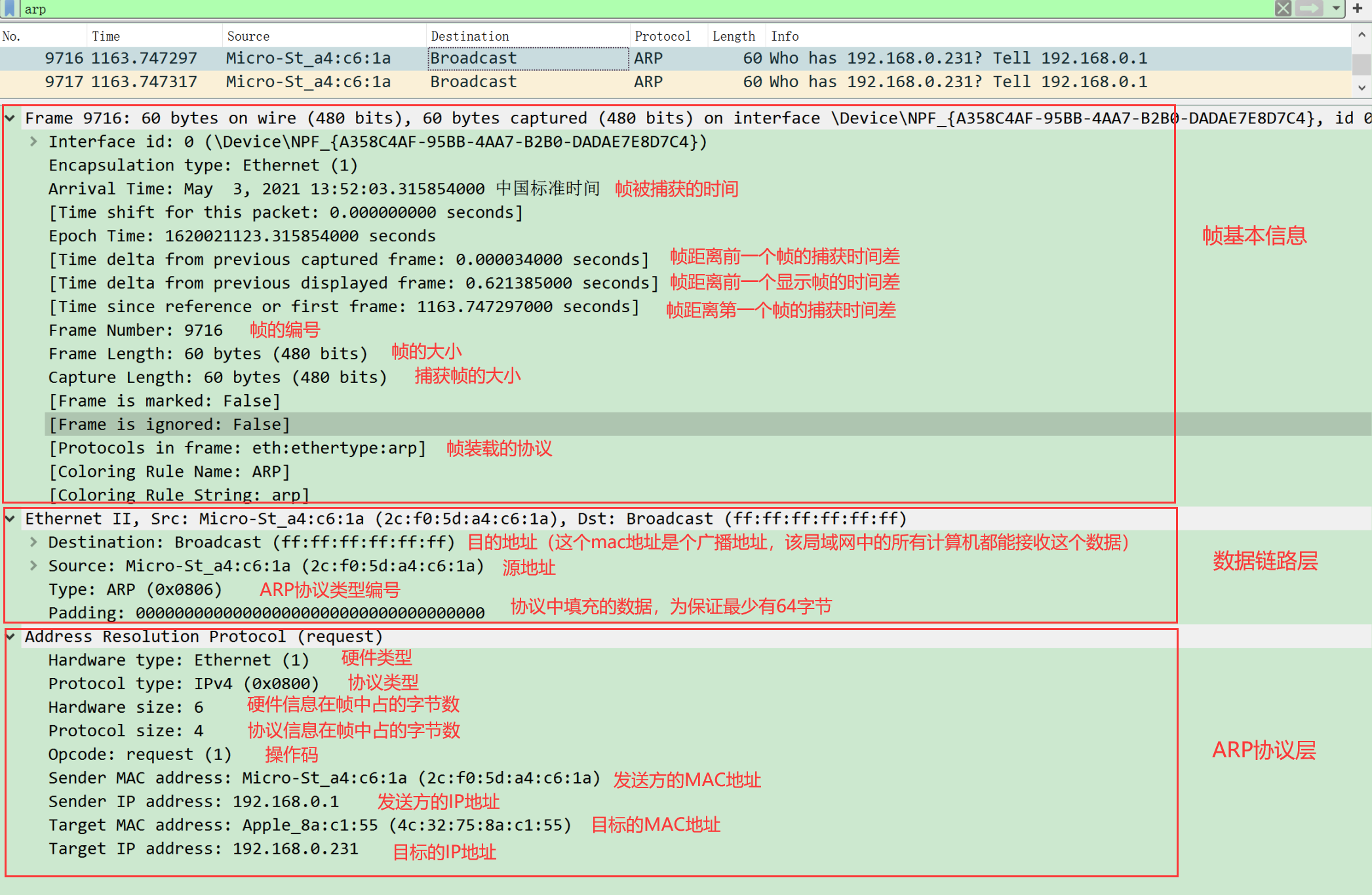


攻击前的ip地址与mac地址对应关系



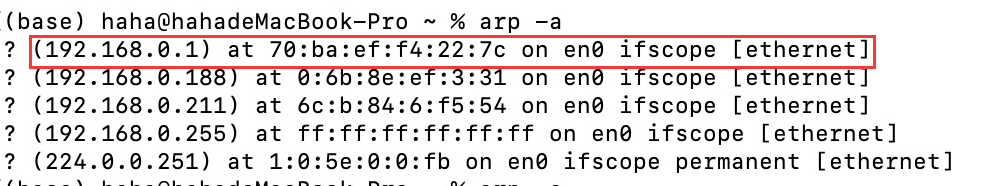
攻击后的ip地址与mac地址对应关系

1. 请求ARP协议分析和标注：

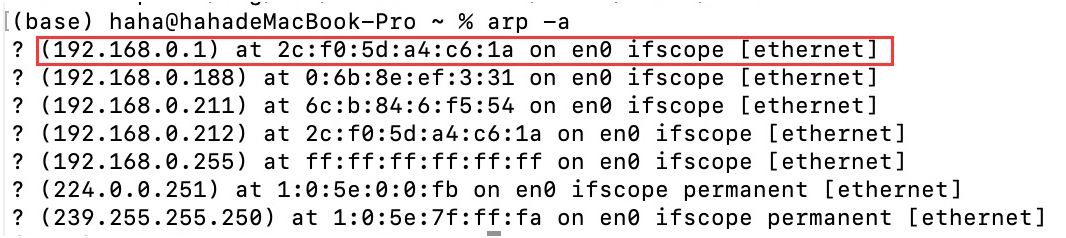


**B、应答形式的ARP包**

1.用科来数据包播放器软件将伪造数据包向受害者主机发送，用arp命令查看攻击前后的目标机ARP缓存表截图如下：

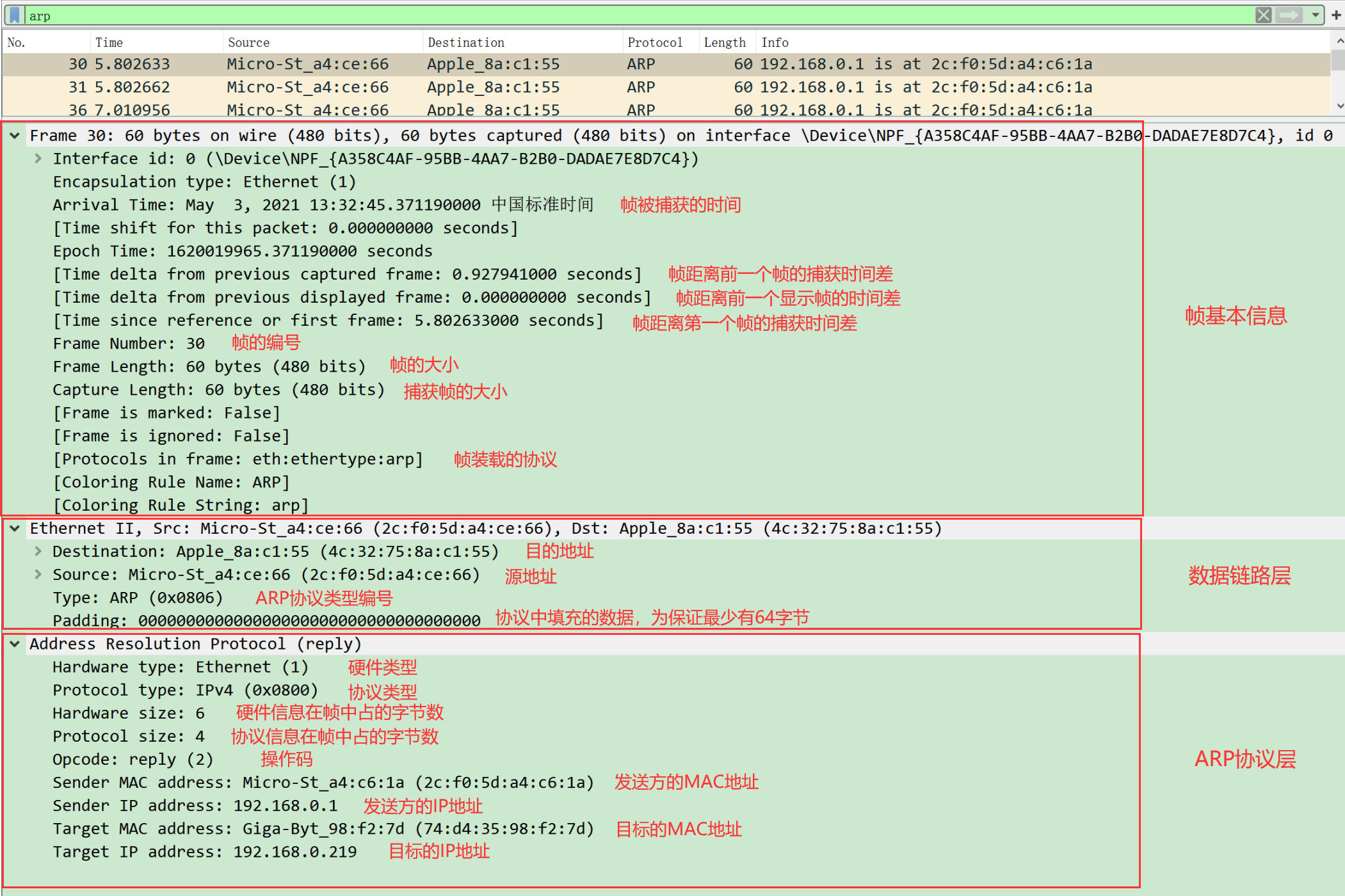


攻击前的ip地址与mac地址对应关系



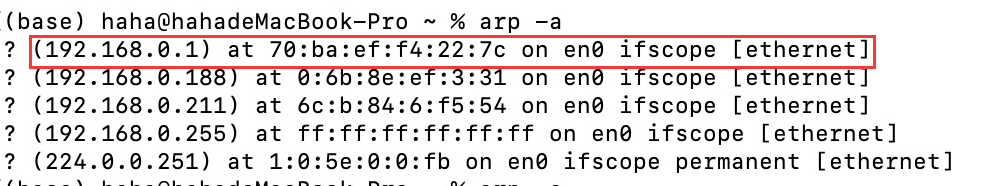
攻击后的ip地址与mac地址对应关系

2.应答ARP协议分析和标注：

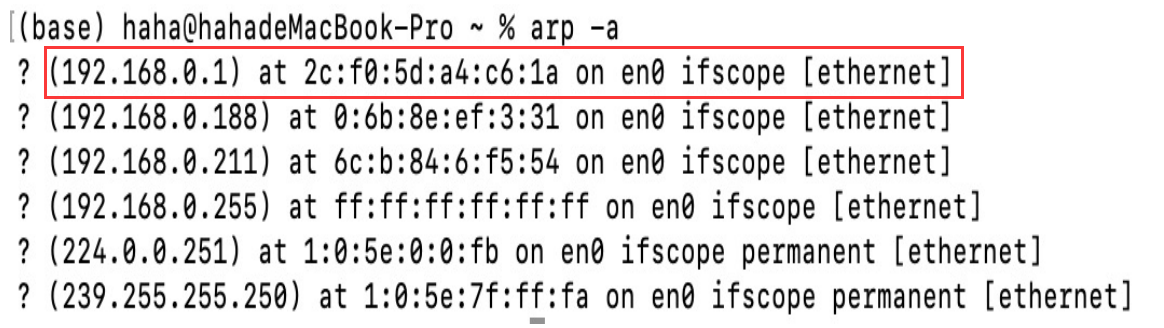


**C、Gratuitous形式的ARP包**

1.用科来数据包播放器软件将伪造数据包向受害者主机发送，用arp命令查看攻击前后的目标机ARP缓存表截图如下：

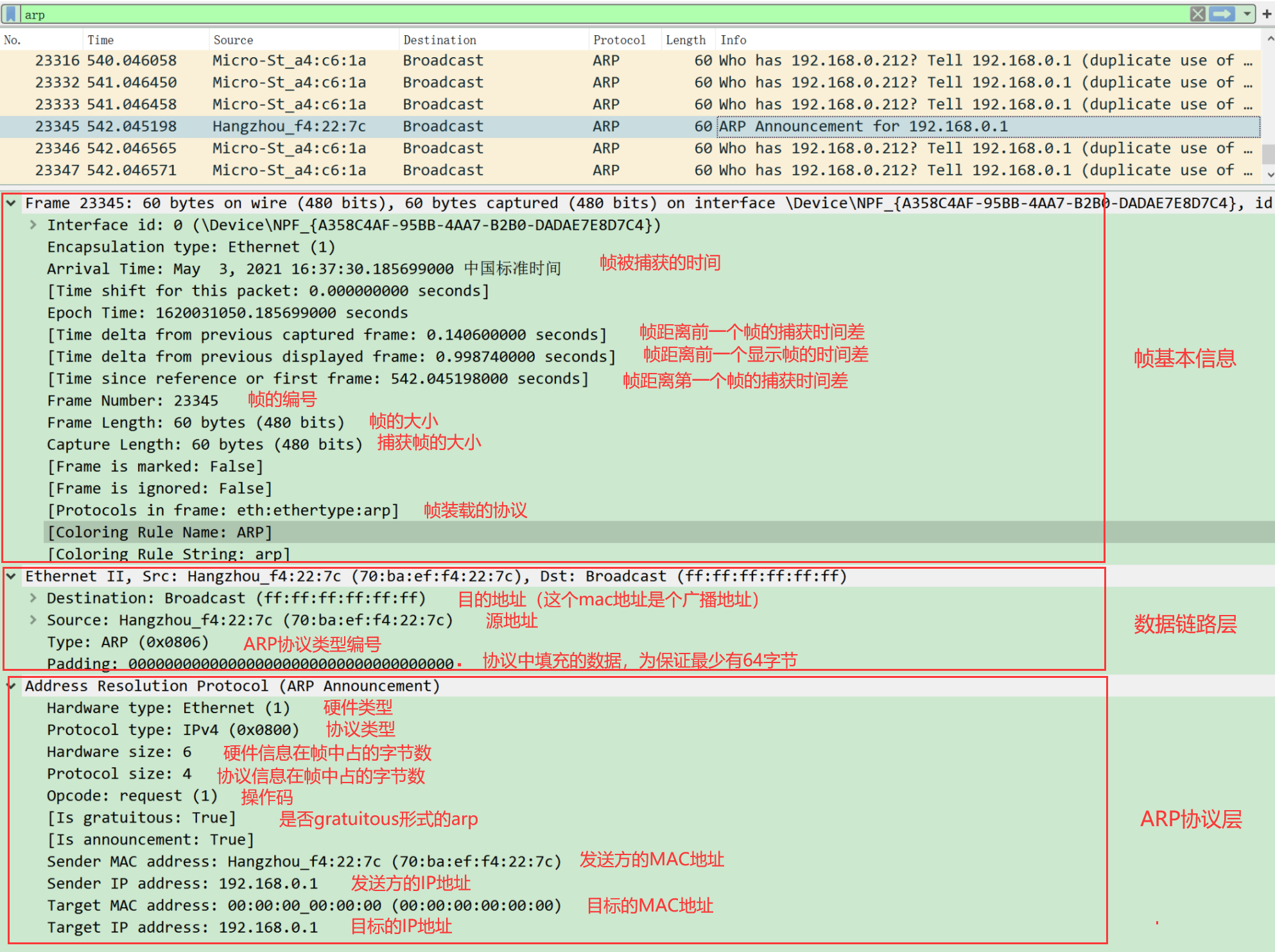


攻击前的ip地址与mac地址对应关系



攻击后的ip地址与mac地址对应关系

2.免费ARP协议分析和标注：



**5、建议**

**ARP欺骗方式分为二种:**  
第一种:广播错误的网关MAC,以使PC找到不真正的网关  
第二种:欺骗网关,告诉它错误的终端MAC,以使数据收不回来

在本实验中，使用的都是第一种欺骗方式，对受害者主机广播错误的网关，使其发给网关的数据全部发给攻击的主机，从而使被攻击的主机无法上网。

**防护arp攻击的建议：**

1、把网络安全信任关系建立在IP+MAC基础上。  
2、在接入层使用可管理交换机对每台机器的IP与MAC地址进行绑定。（如果网络规模小可以使用硬件防火墙或者宽带路由器进行IP、MAC绑定）  
2、设置静态的MAC-->IP对应表格，不要让主机刷新你设定好的转换表。

3、除非很有必要，否则停止使用ARP,将ARP作为永久条目保存在对应表中。

4、使用ARP服务器查找自己的ARP转换表来相应其他机器的广播。

5、定期用响应的IP包获得一个rarp请求，然后检查ARP响应的真实性。