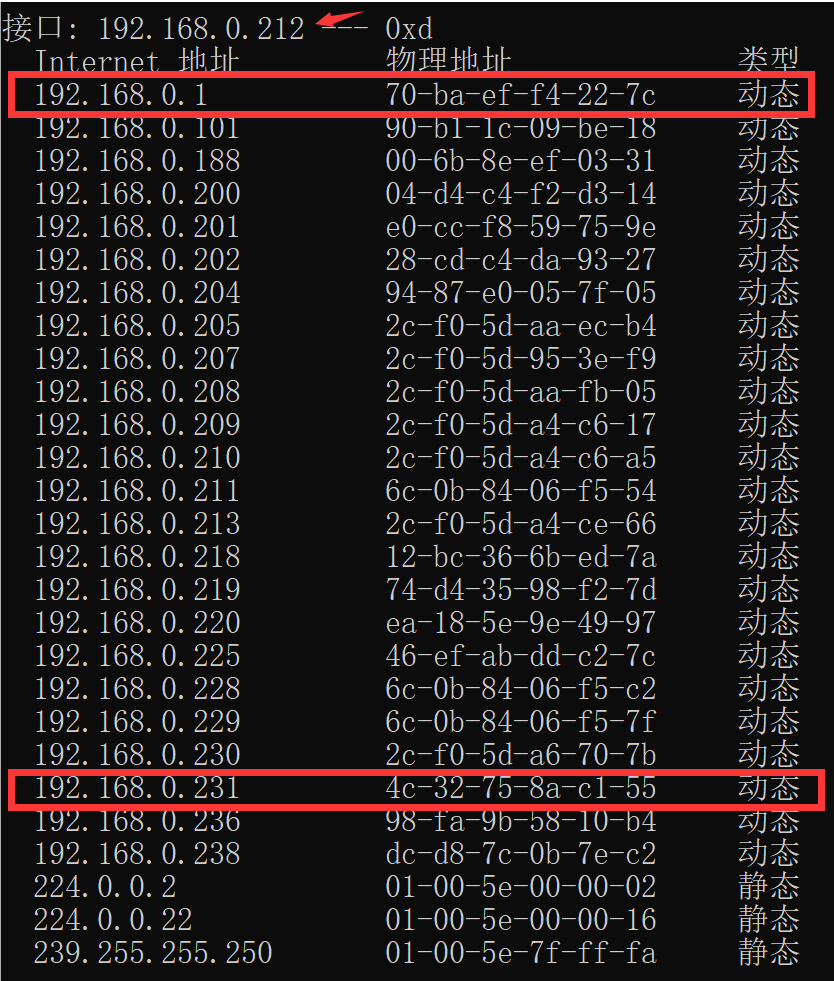
信息安全课程实验二--实验报告

1. **实验过程**

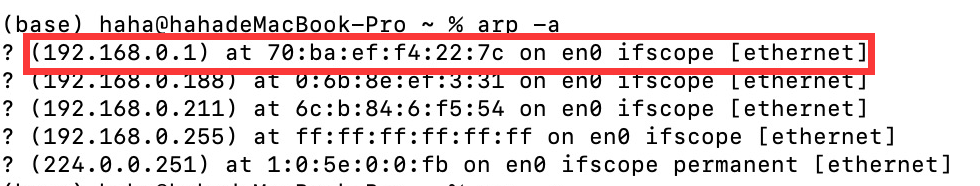
局域网内所有主机IP和mac地址信息如下：



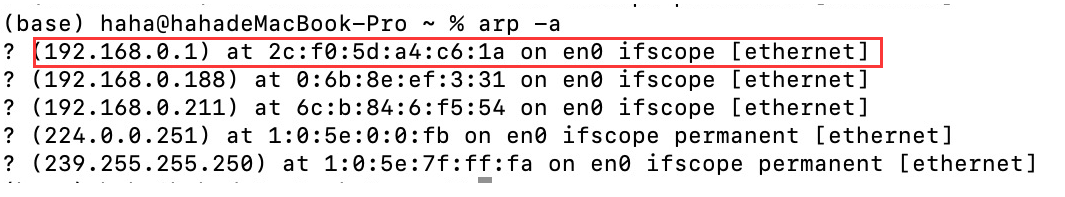
|  |  |  |
| --- | --- | --- |
| 主机 | IP地址 | MAC地址 |
| 网关 | 192.168.0.1 | 70:ba:ef:f4:22:7c |
| 本机(攻击者) | 192.168.0.212 | 2c:f0:5d:a4:c6:1a |
| Mac电脑(受害者) | 192.168.0.231 | 4c:32:75:8a:c1:55 |

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：

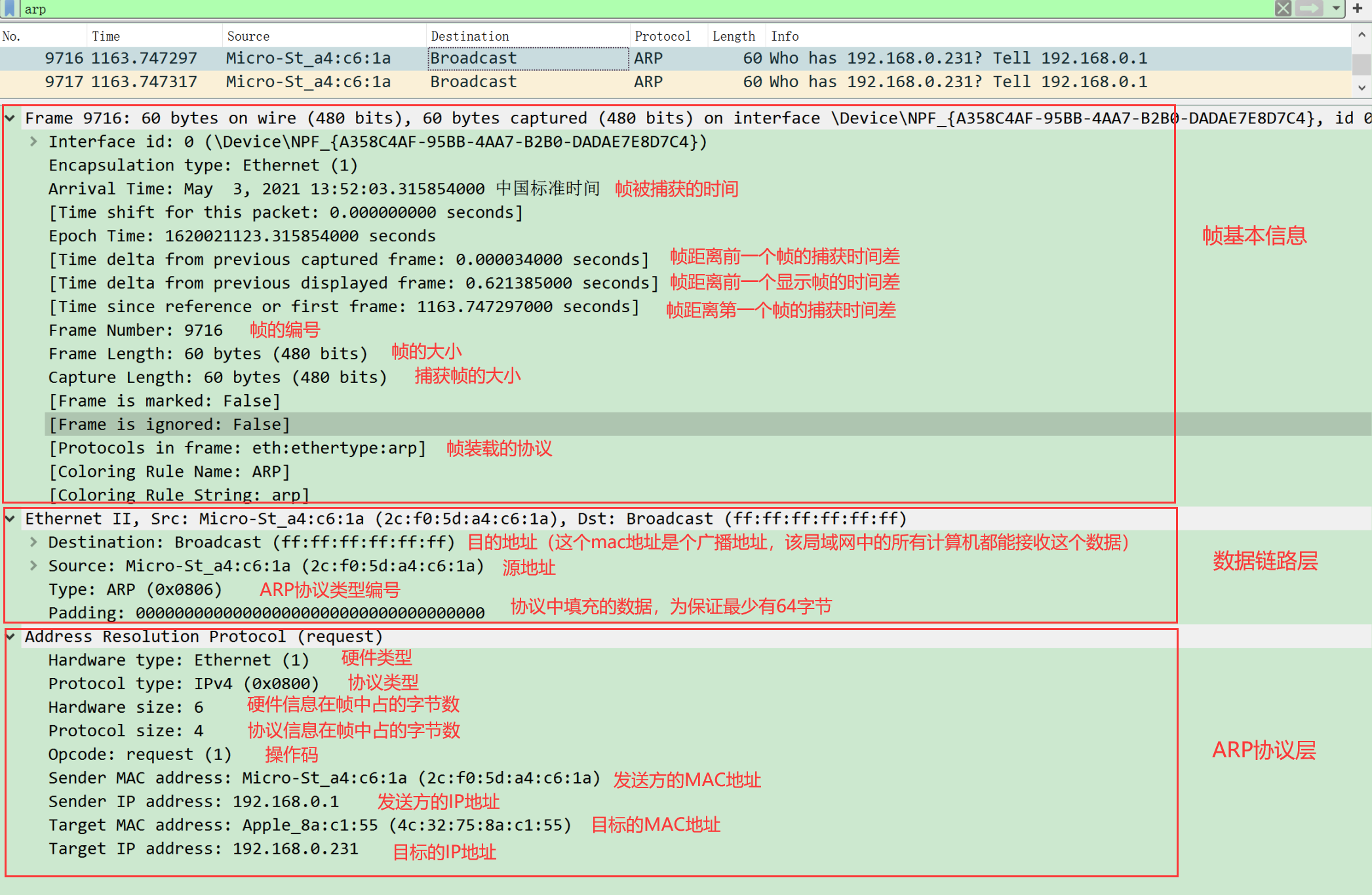


攻击前的ip地址与mac地址对应关系



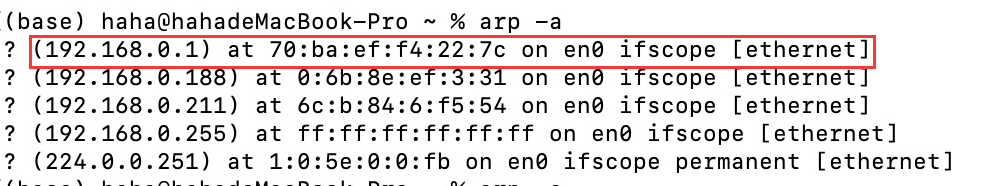
攻击后的ip地址与mac地址对应关系

1. 请求ARP协议分析和标注：

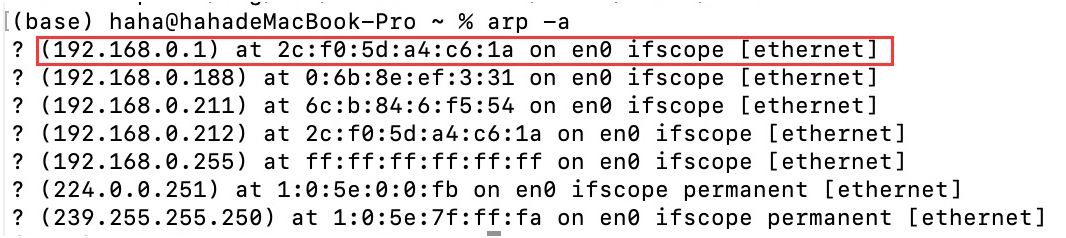


**B、响应形式的ARP包**

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：

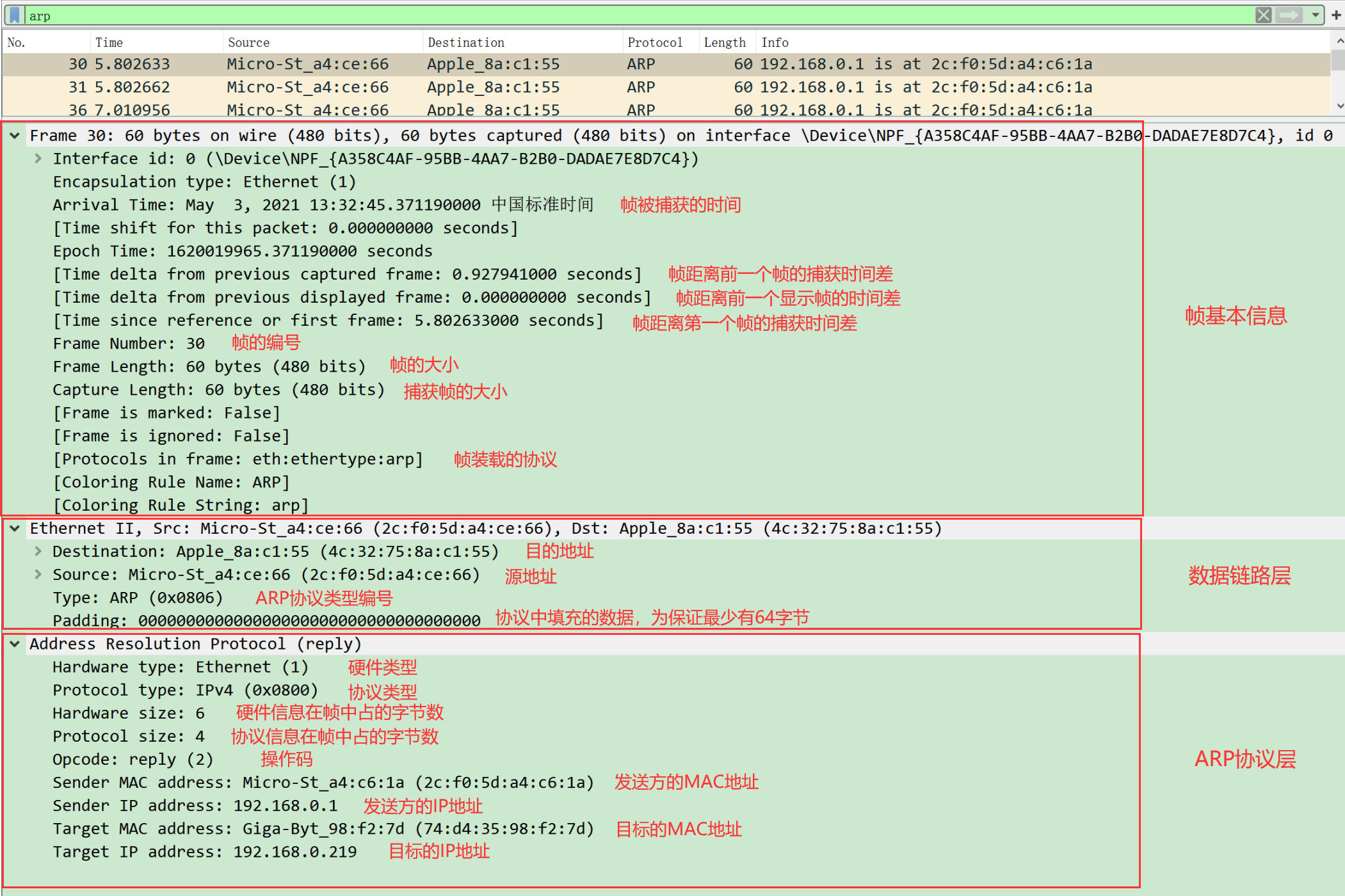


攻击前的ip地址与mac地址对应关系



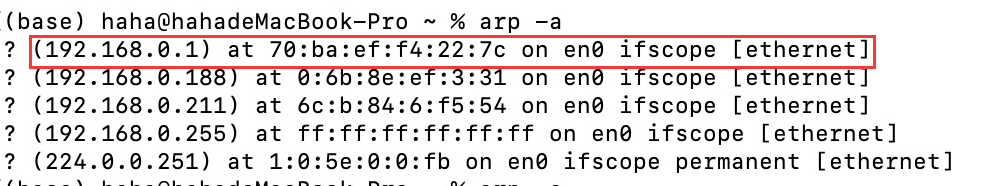
攻击后的ip地址与mac地址对应关系

2.响应ARP协议分析和标注：

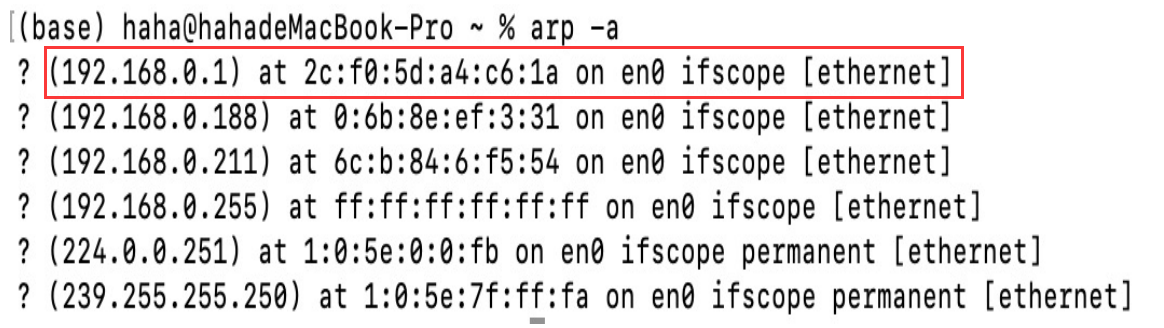


**C、Gratuitous形式的ARP包**

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：

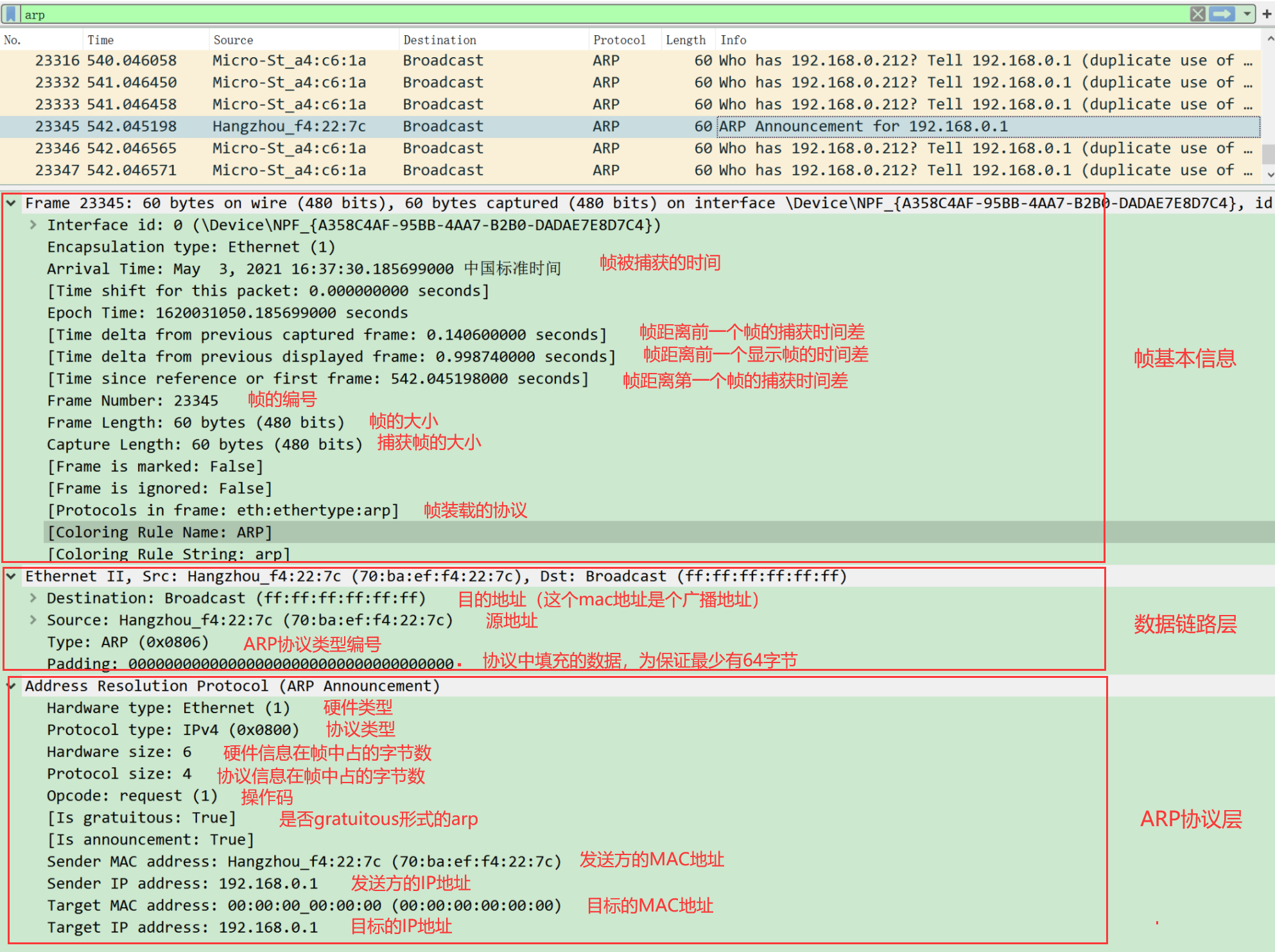


攻击前的ip地址与mac地址对应关系



攻击后的ip地址与mac地址对应关系

1.免费ARP协议分析和标注：



**总结：针对ARP攻击，如何进行防护，我的意见和建议如下：**

**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。

**解决arp攻击的方法：**  
1、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、客户端绑定网关MAC地址。编写一个自动批处理文件arp.bat,内容如下  
@echo off  
arp -d  
arp -s 192.168.0.1    70:ba:ef:f4:22:7c  
其中192.168.0.1为网关的IP地址，70:ba:ef:f4:22:7c为网关的MAC地址，  
最好将客户端设为开机自动运行该批处理文件。  
3、客户端安装杀毒软件，最好是正版可在线升级病毒库的。

4、客户端操作系统各种补丁一定要打全。