信息安全课程实验二

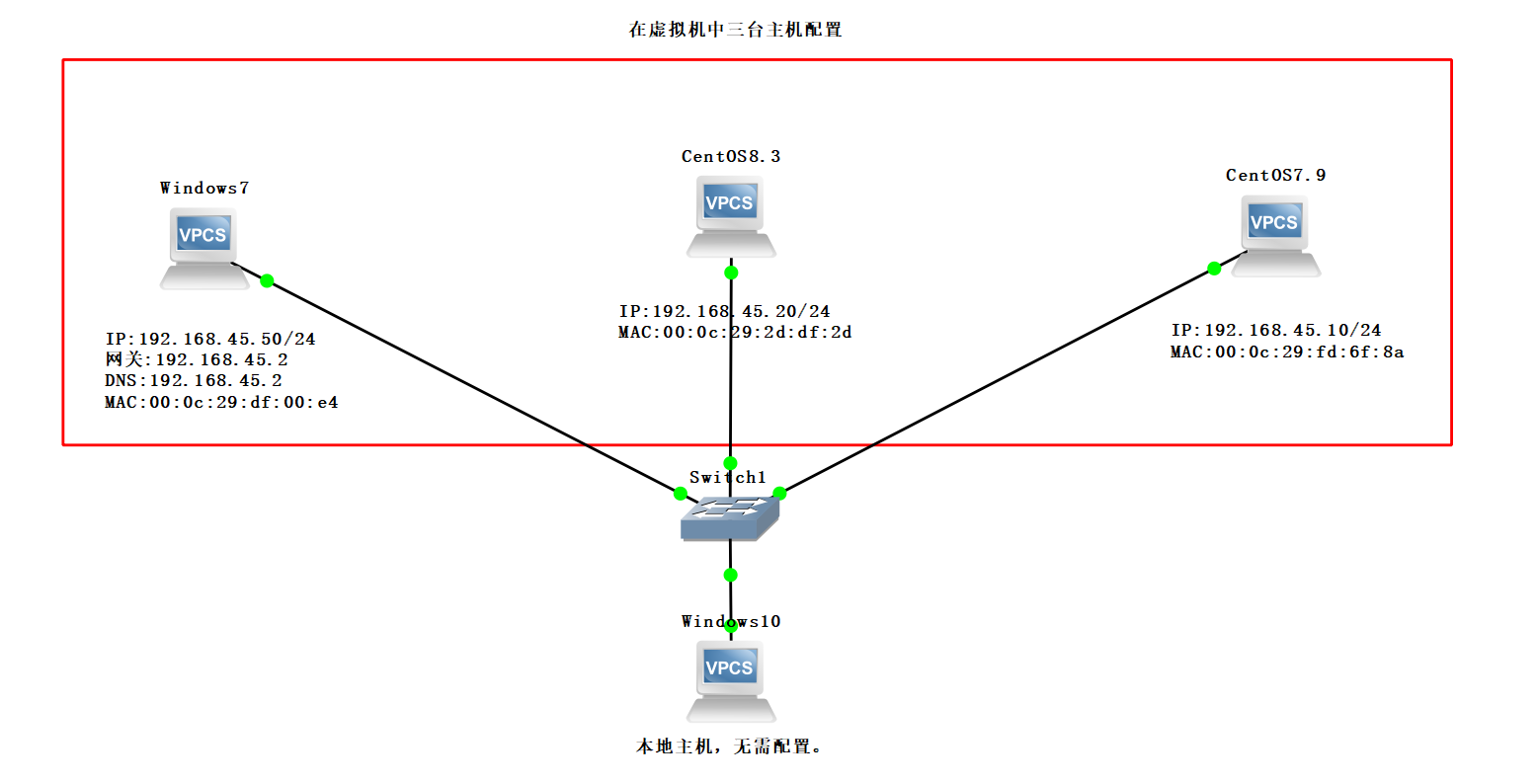
1. **实验目的**

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。

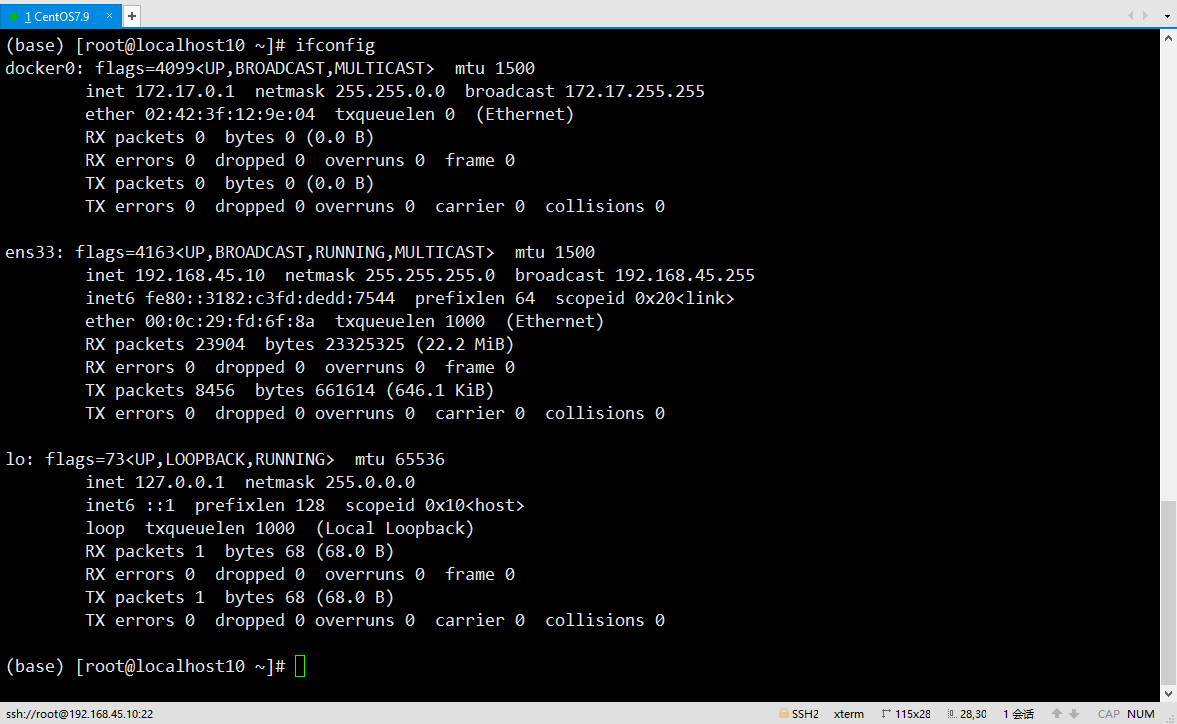
1. **实验工具**

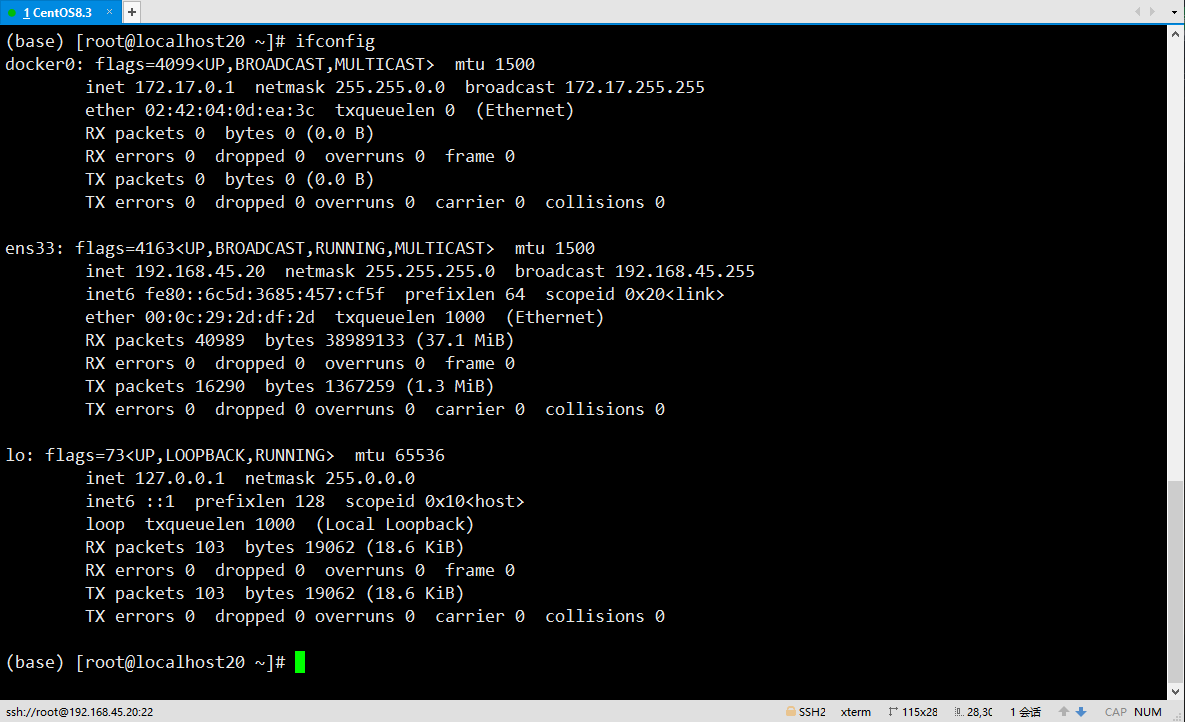
Centos6以上系统，GitHub，科来数据包生成器/科来数据包播放器软件（pktbuilder\_x64/pktplayer\_x64），Wireshark。

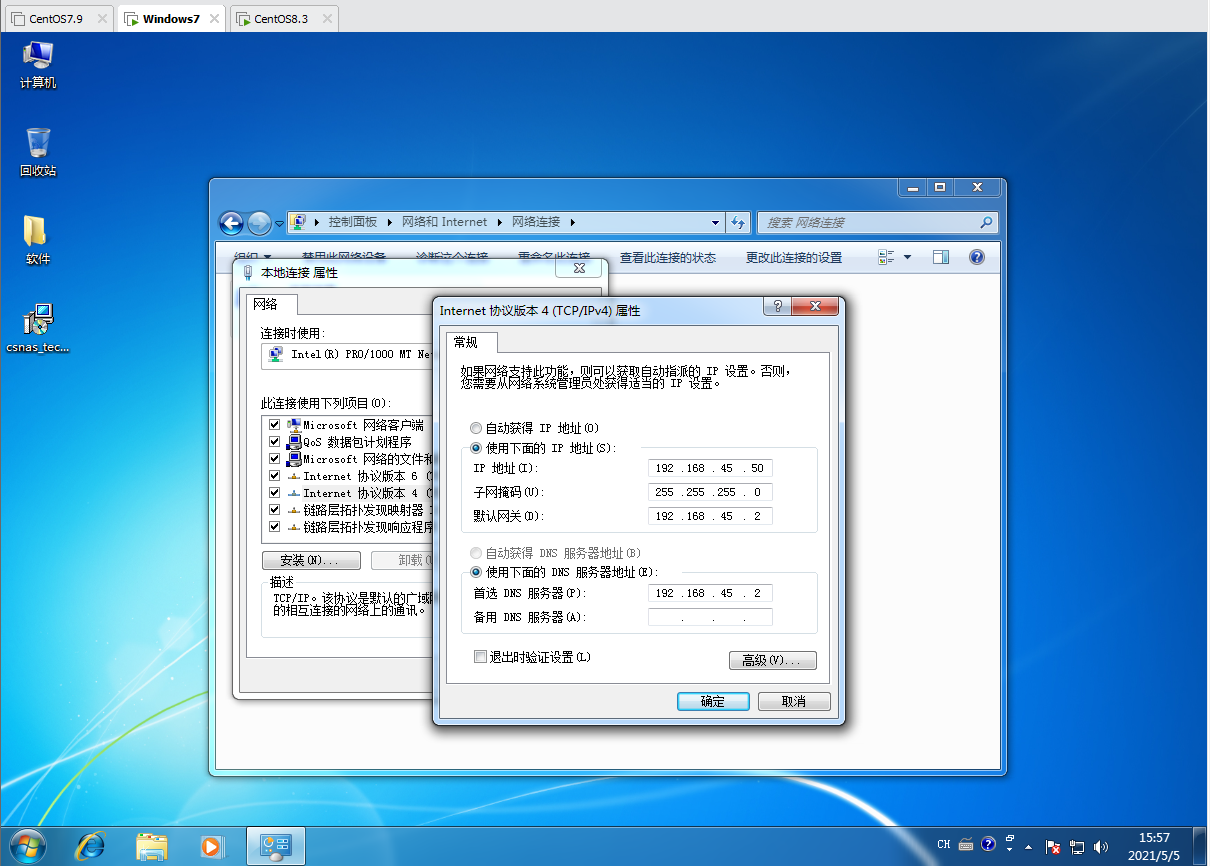
1. **实验内容**
2. ARP协议应答数据包攻击。
   1. 在虚拟机中创建3台虚拟主机，该局域网的网络结构如图所示。



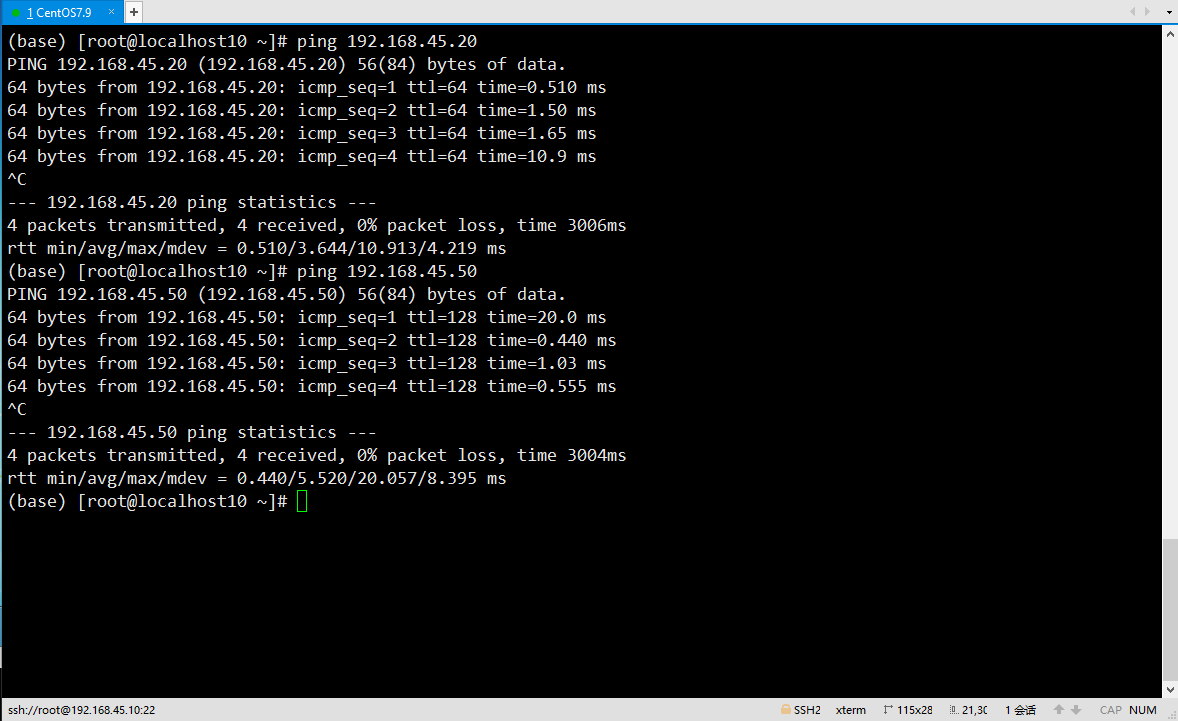
* 1. 配置并查看3台虚拟主机的ip地址。



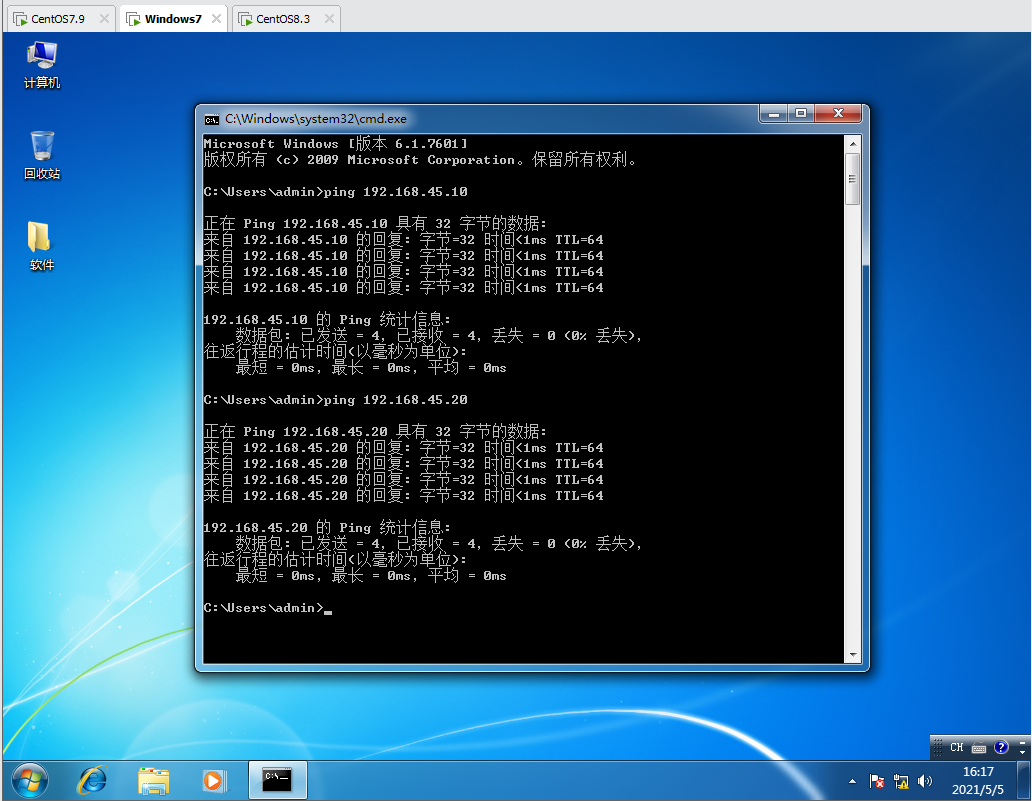




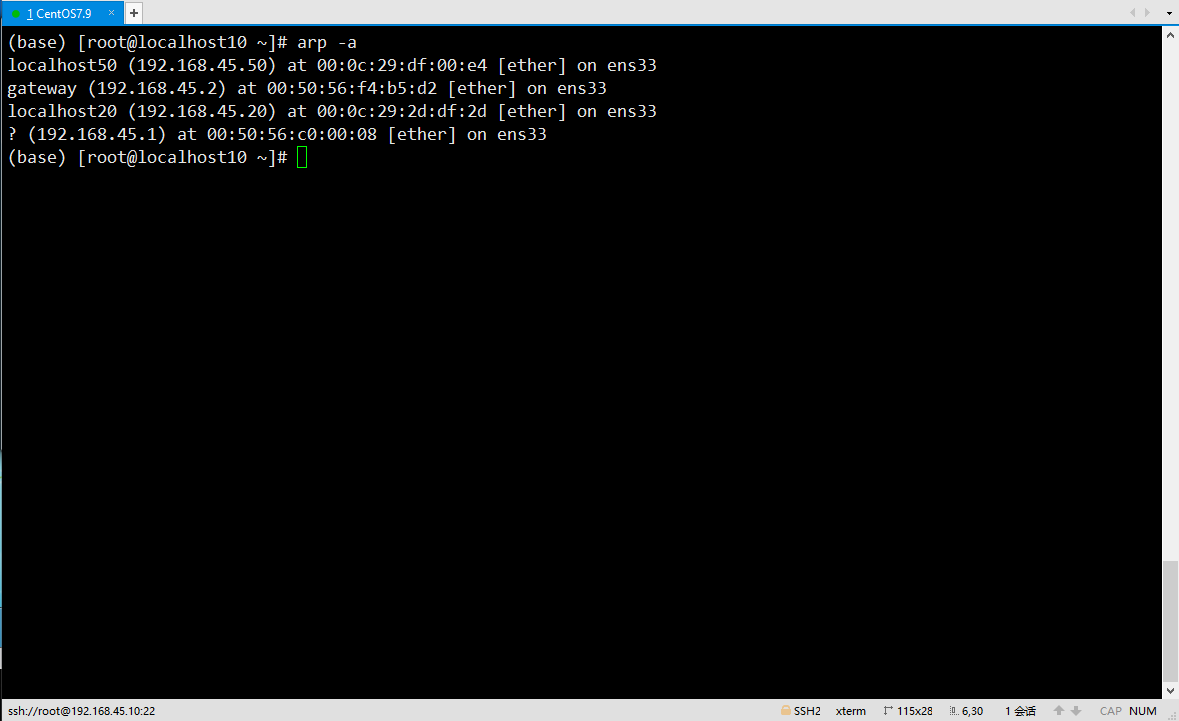
* 1. 使用ping命令在三台虚拟机上进行链接测试，确保它们相互之间能够正常通信。

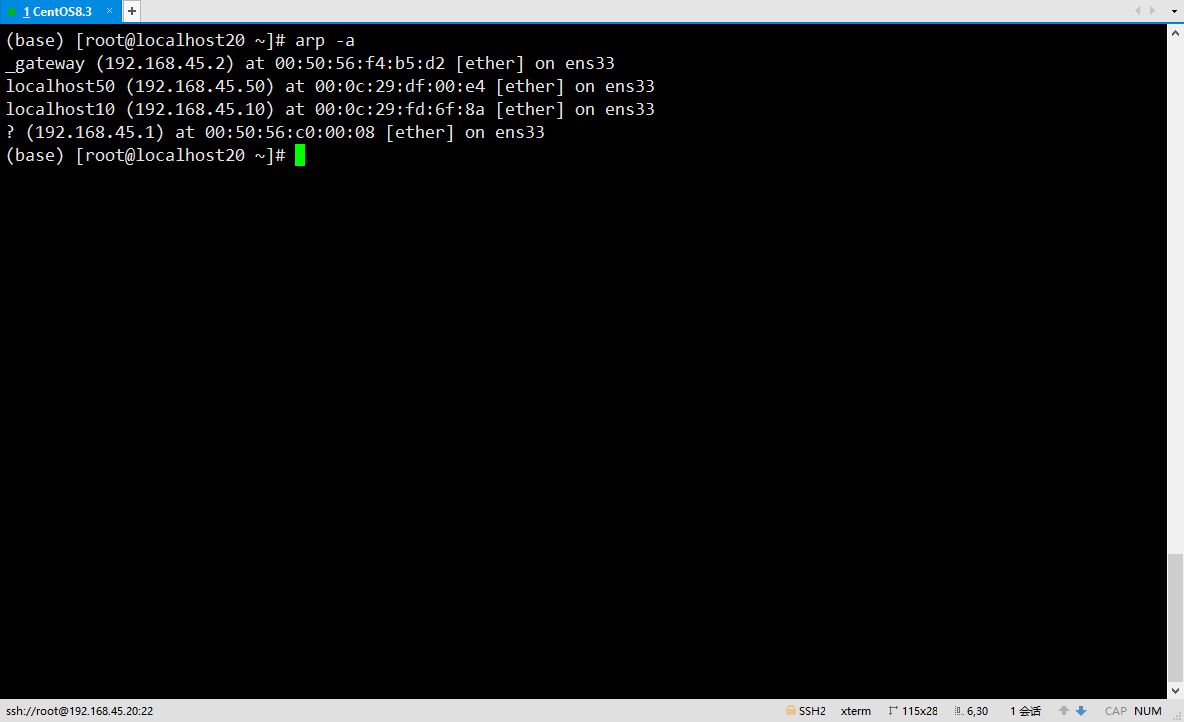


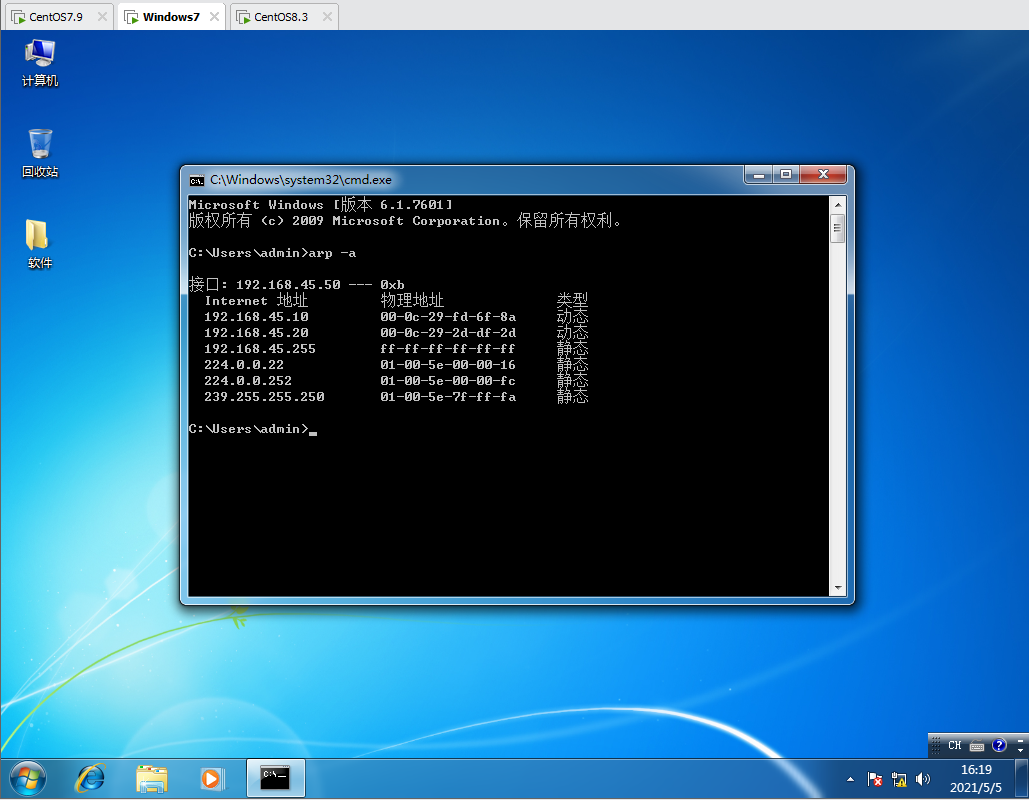




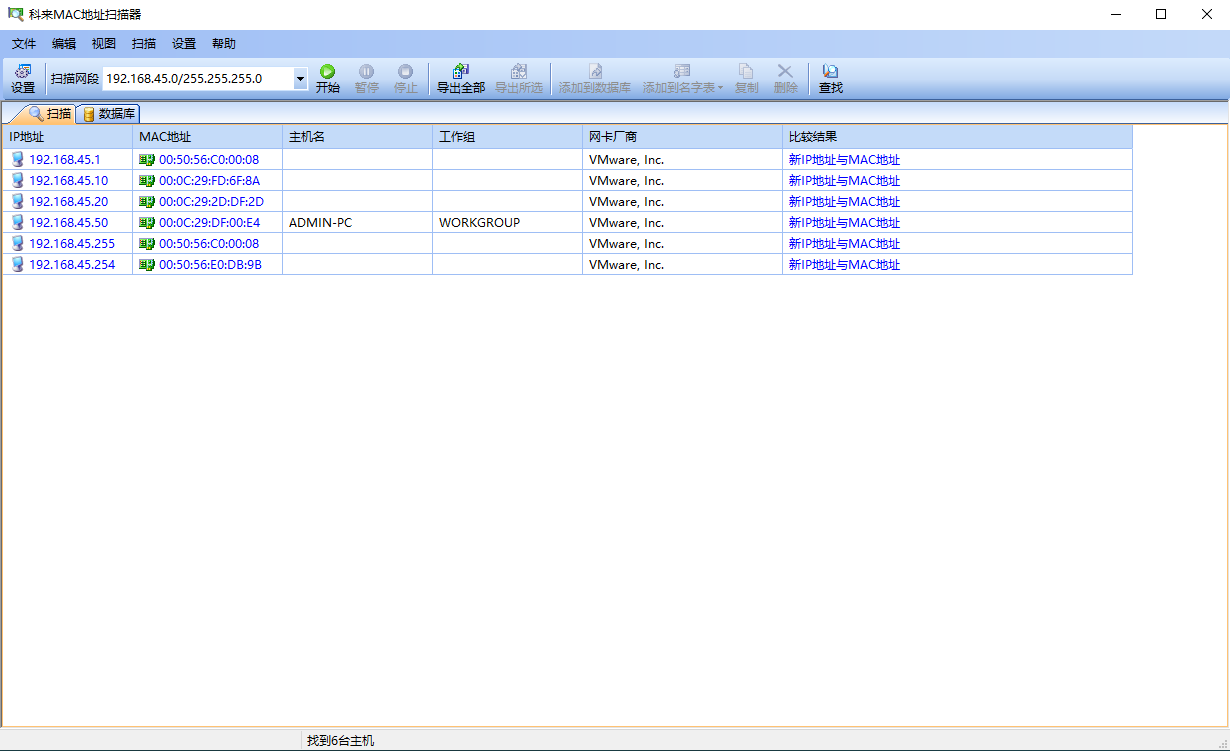
* 1. 查看三台虚拟机的arp缓存并记录。



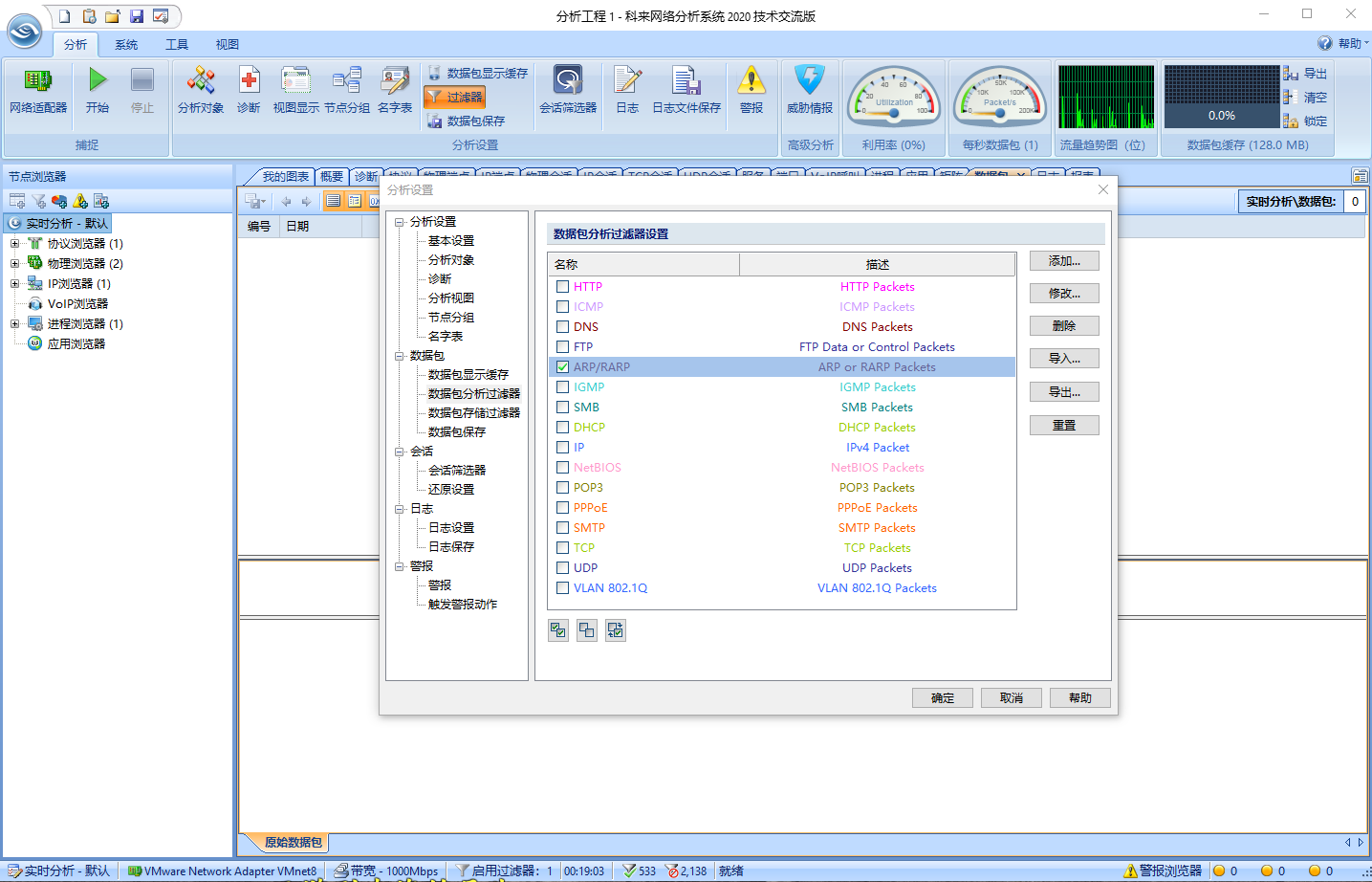




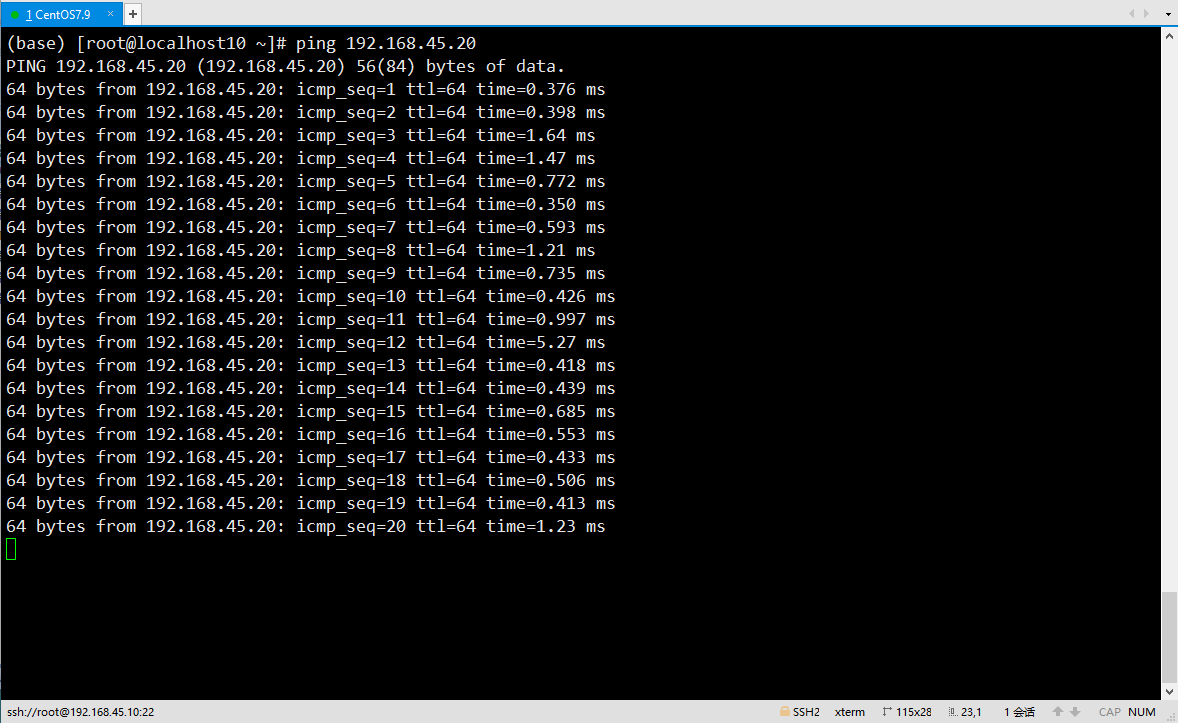
* 1. 使用科来MAC地址扫描器软件对192.168.45.0/24局域网进行扫描。



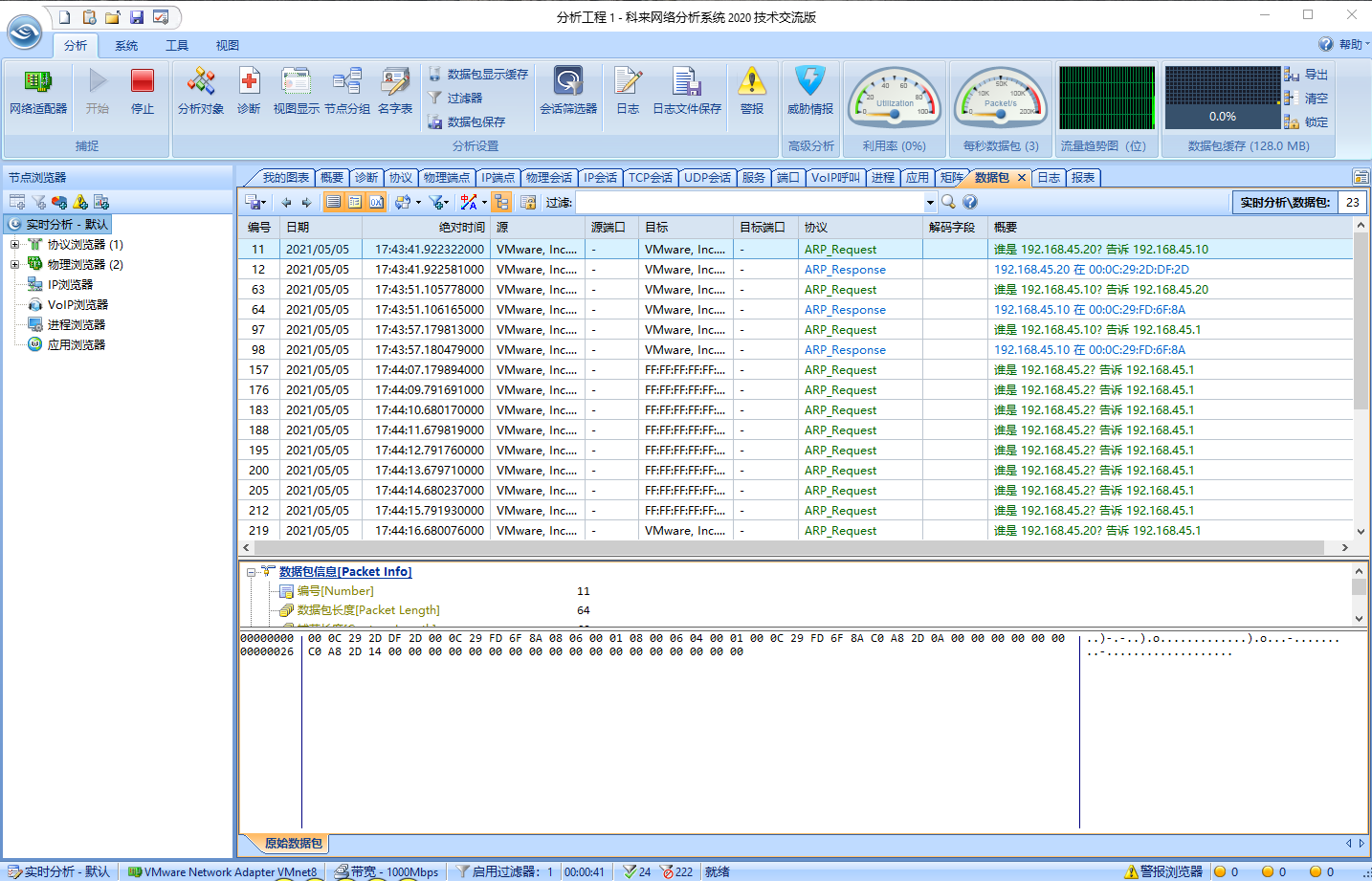
* 1. 打开科来网络分析系统软件，设置过滤器，只抓取ARP数据包。



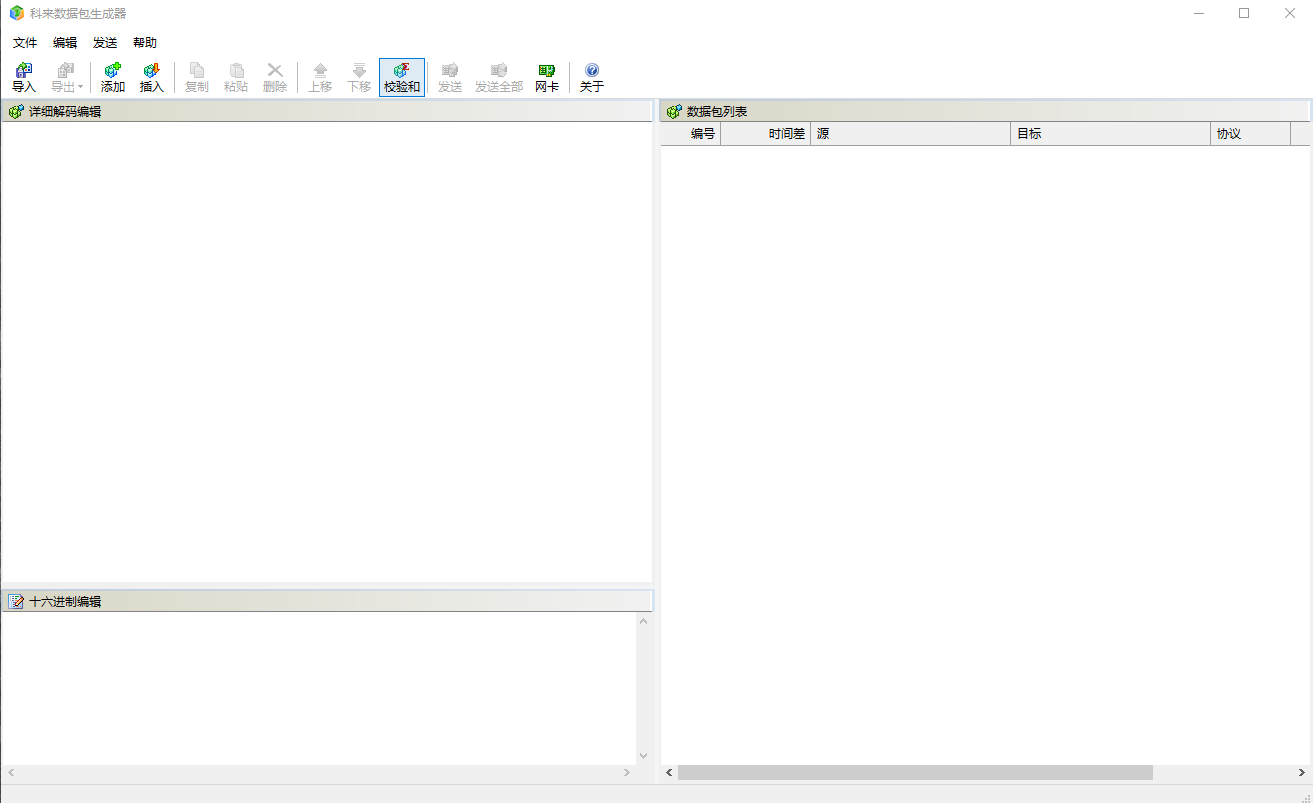
* 1. 在Centos7.9上使用ping命令去访问Centos8.3。



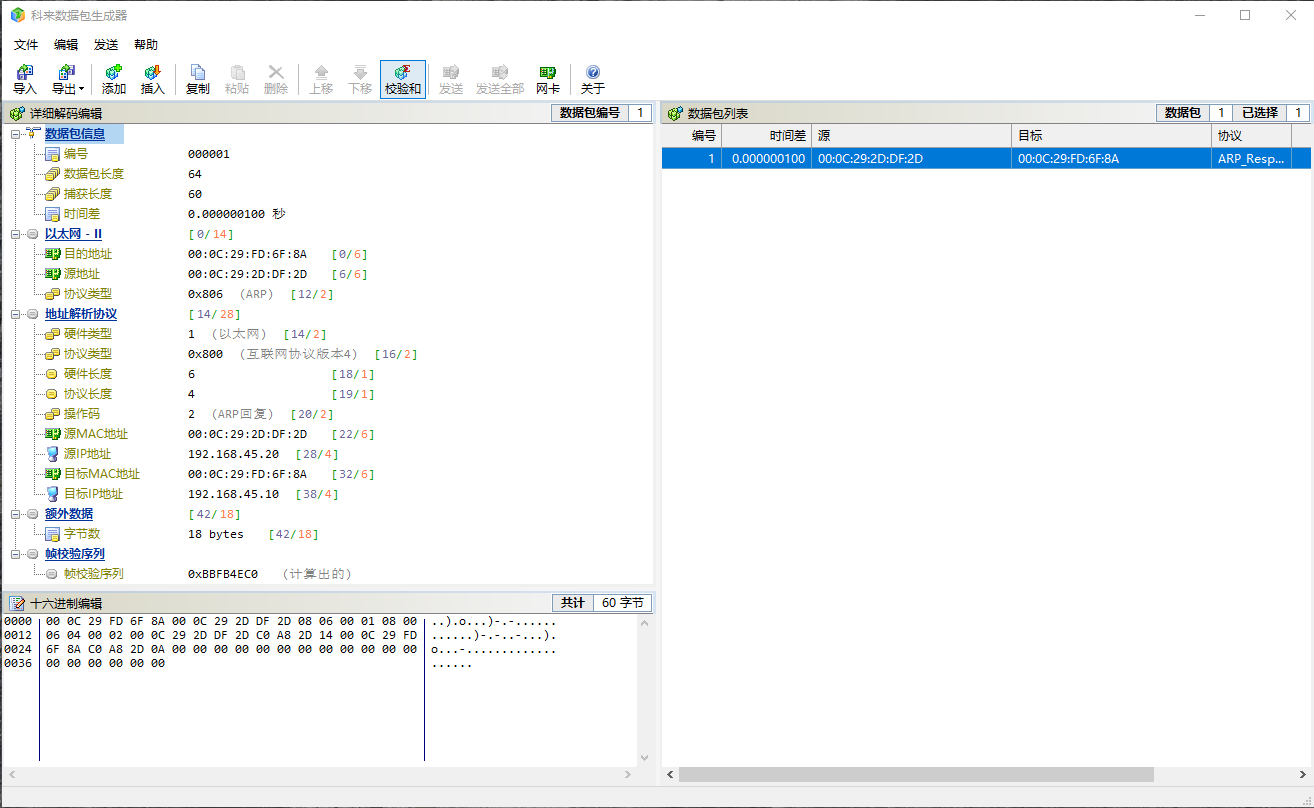
* 1. 查看抓取的数据包。



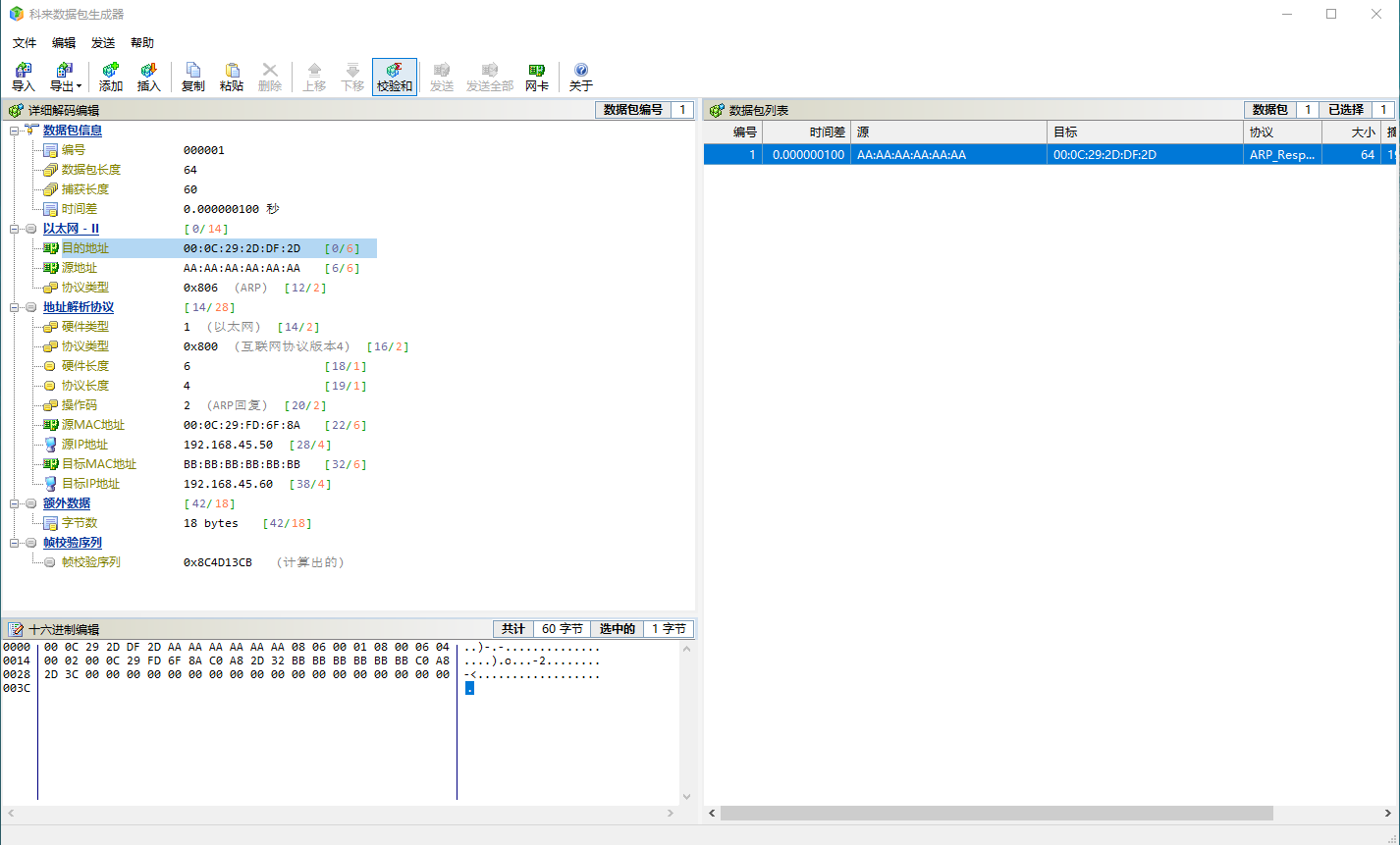
* 1. 打开科来数据包生成器软件。



* 1. 在抓取的数据包中选取一个应答数据包发送到科来数据包生成器软件。



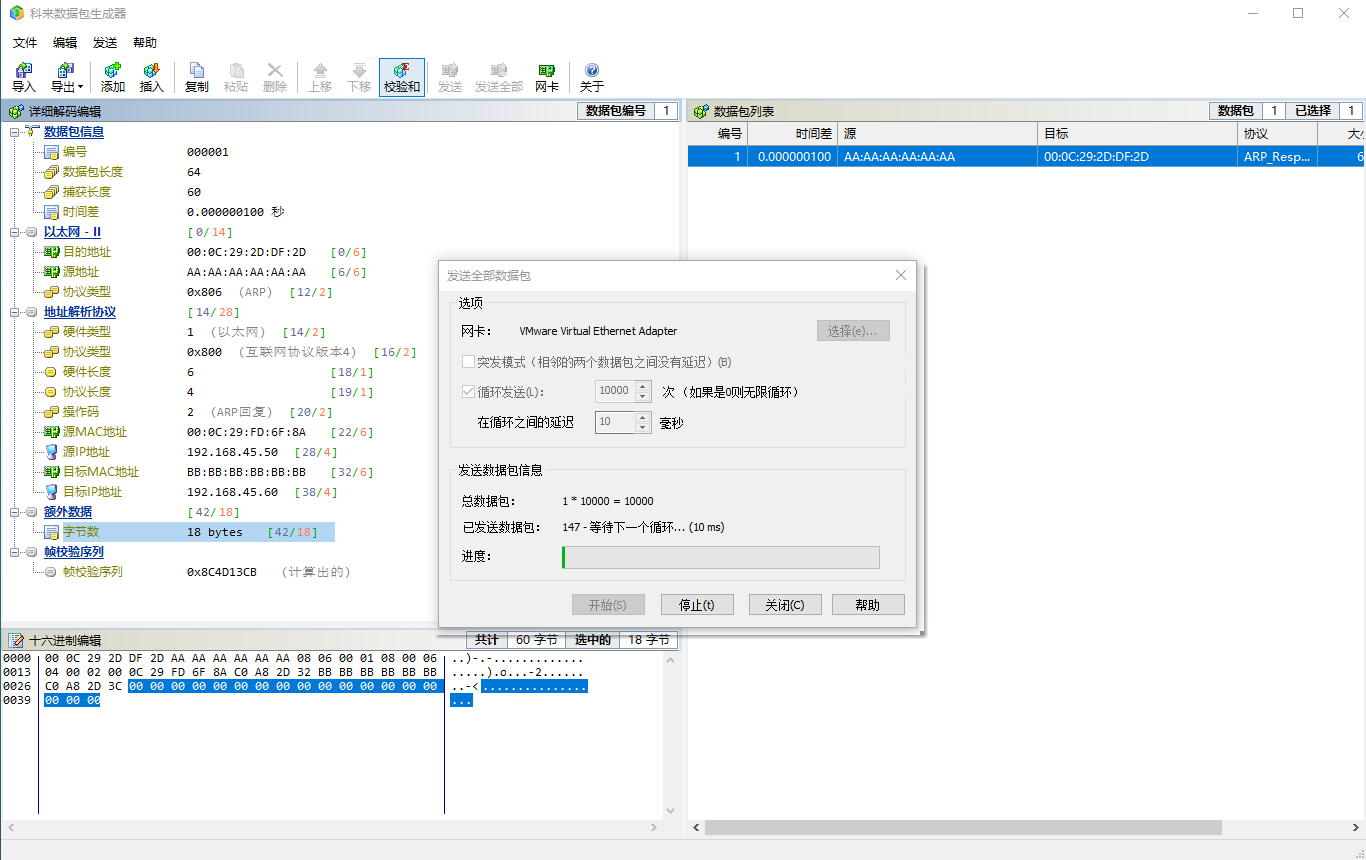
* 1. 对该应答数据进行修改，地址解析协议是CentOS7.9的MAC地址作为源MAC地址，Windows7的IP地址作为源IP地址。在CentOS8.3给Windows7发送请求包时，CentOS7.9冒充Windows7给CentOS8.3发送应答包，这样CentOS8.3就误认为IP为192.168.45.50的主机就是Windows7，实际上IP为192.168.45.50对应的主机是CentOS7.9，当CentOS8.3给Windows7发送数据时，实际上是发送给CentOS7.9。



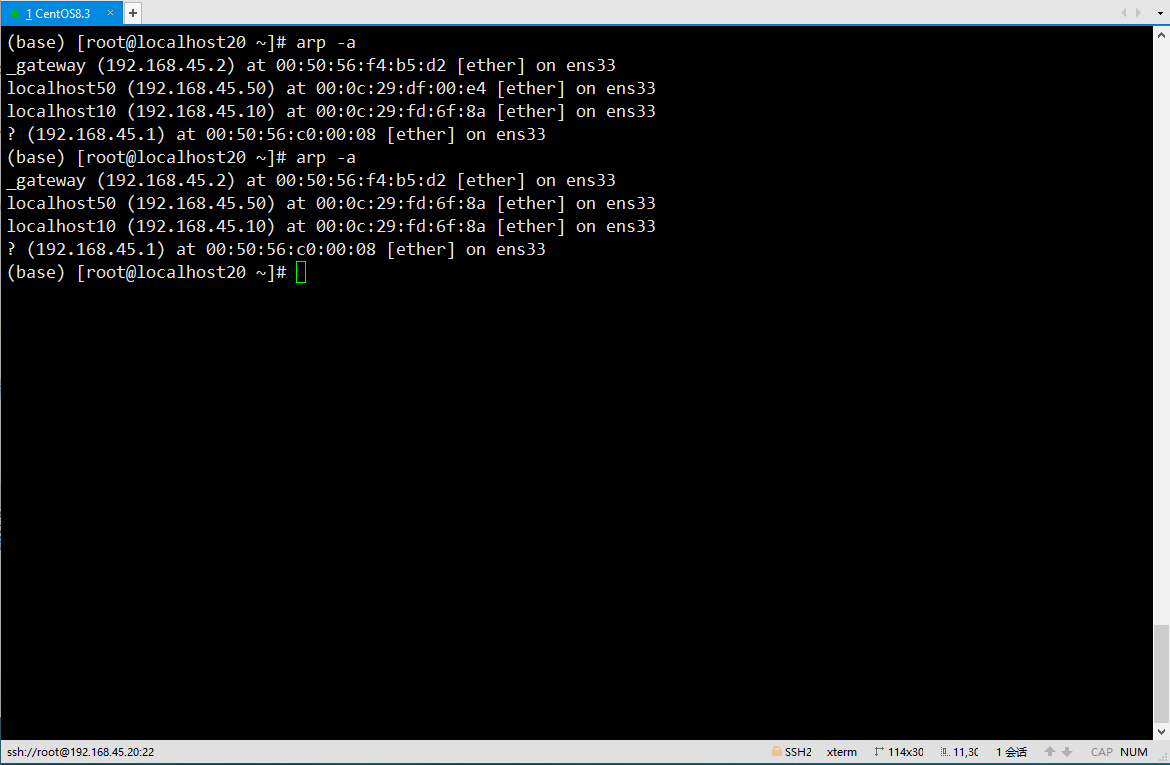
* 1. 查看CentOS8.3的ARP缓存。



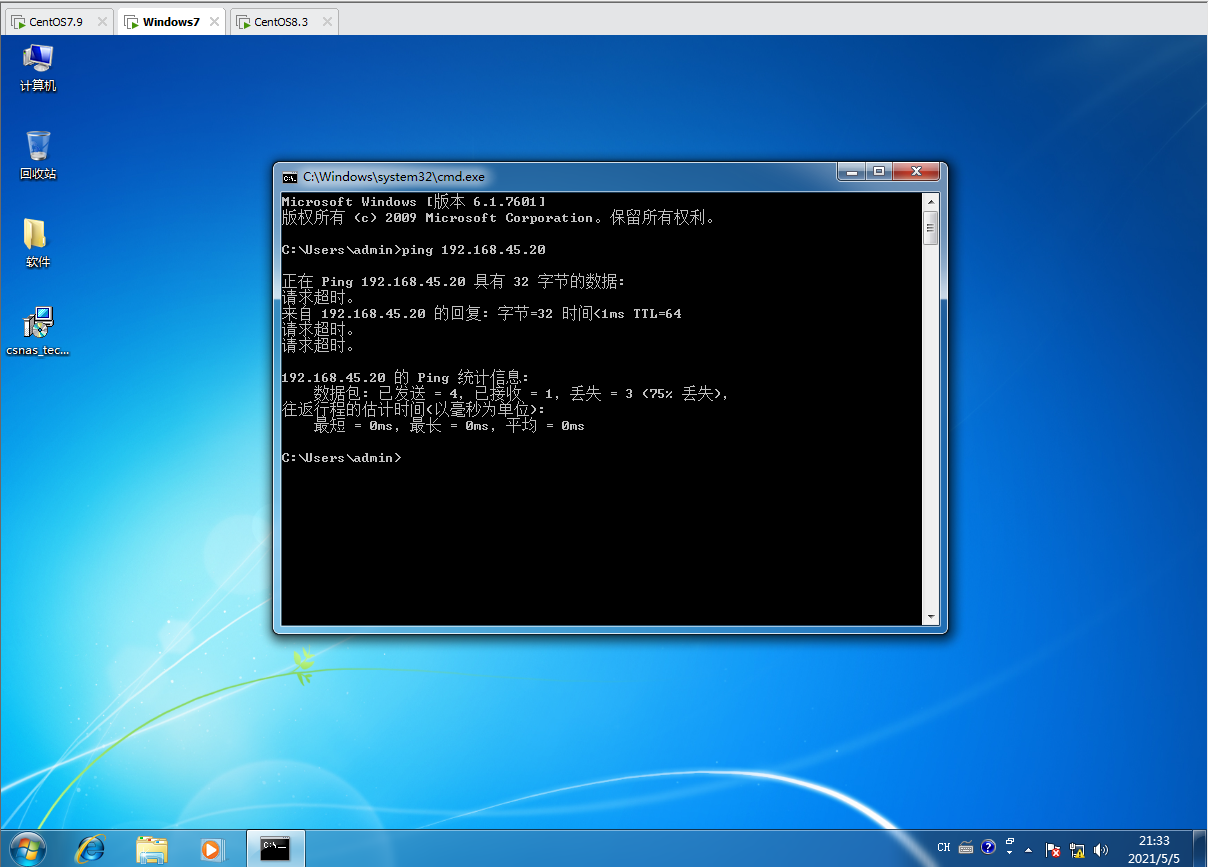
* 1. 把修改后的应答数据包发送到该局域网中。



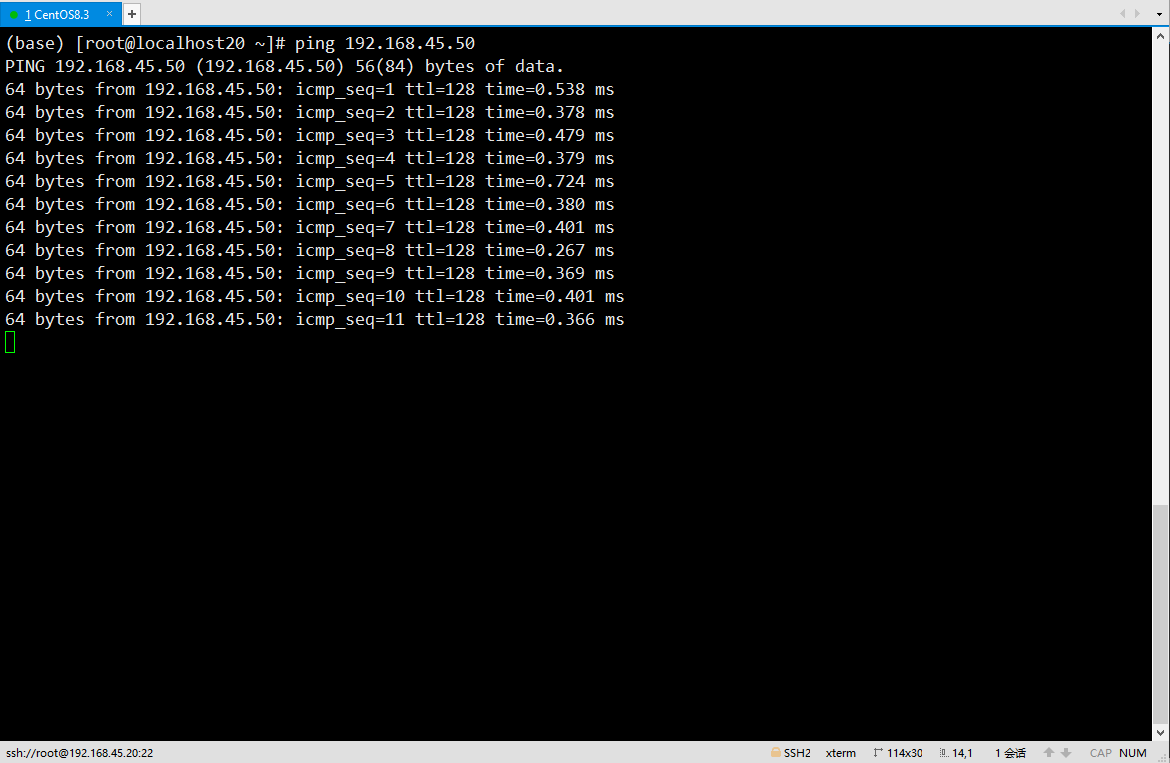
* 1. 再次查看CentOS8.3的ARP缓存，发现192.168.45.50对应的MAC地址发生了变化。



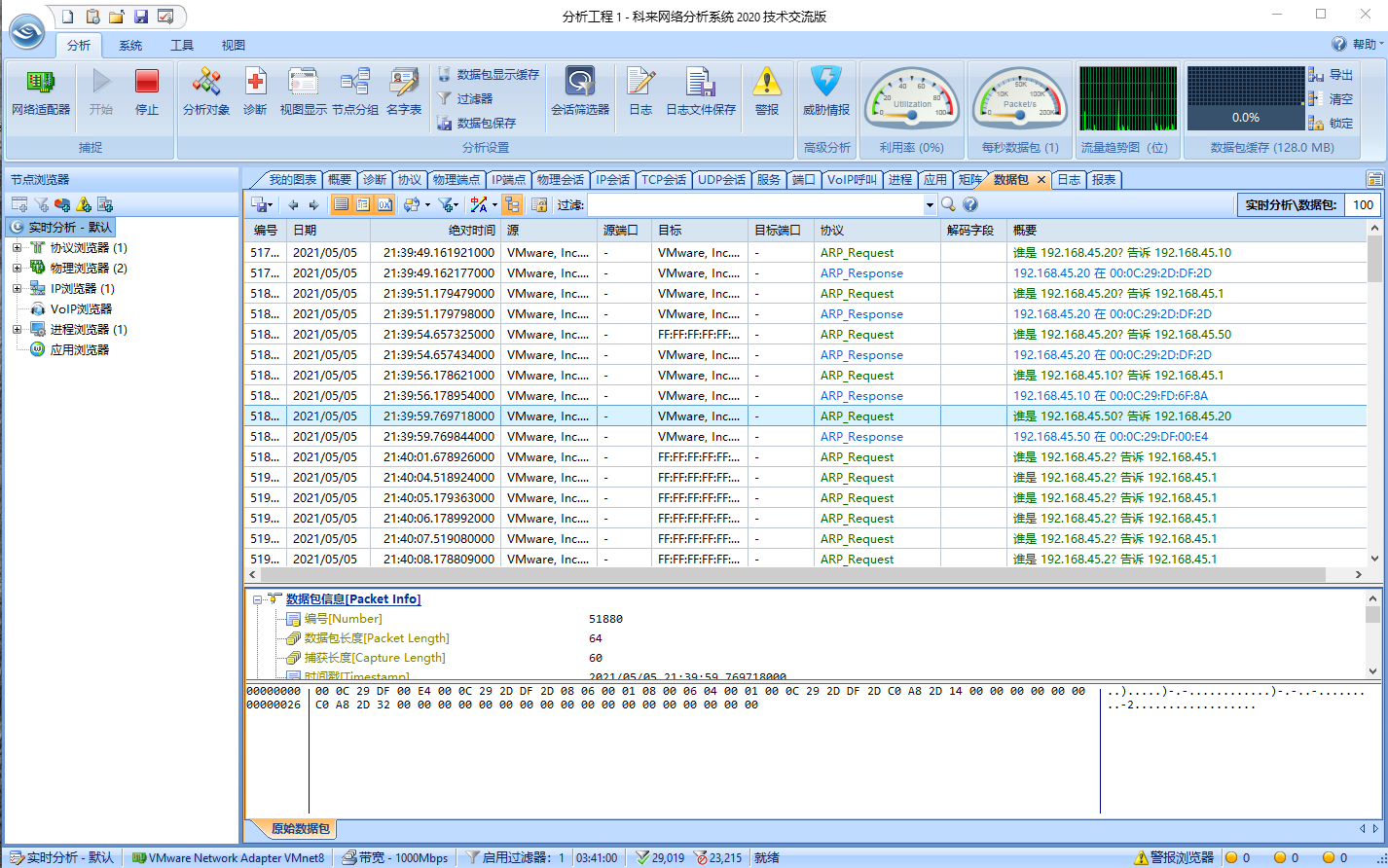
* 1. 在Windows7上访问CentOS8.3，发现出现超时现象，但很快又能正常访问，因为Windows7在访问CentOS8.3时，CentOS8.3更新了自己的ARP缓存。



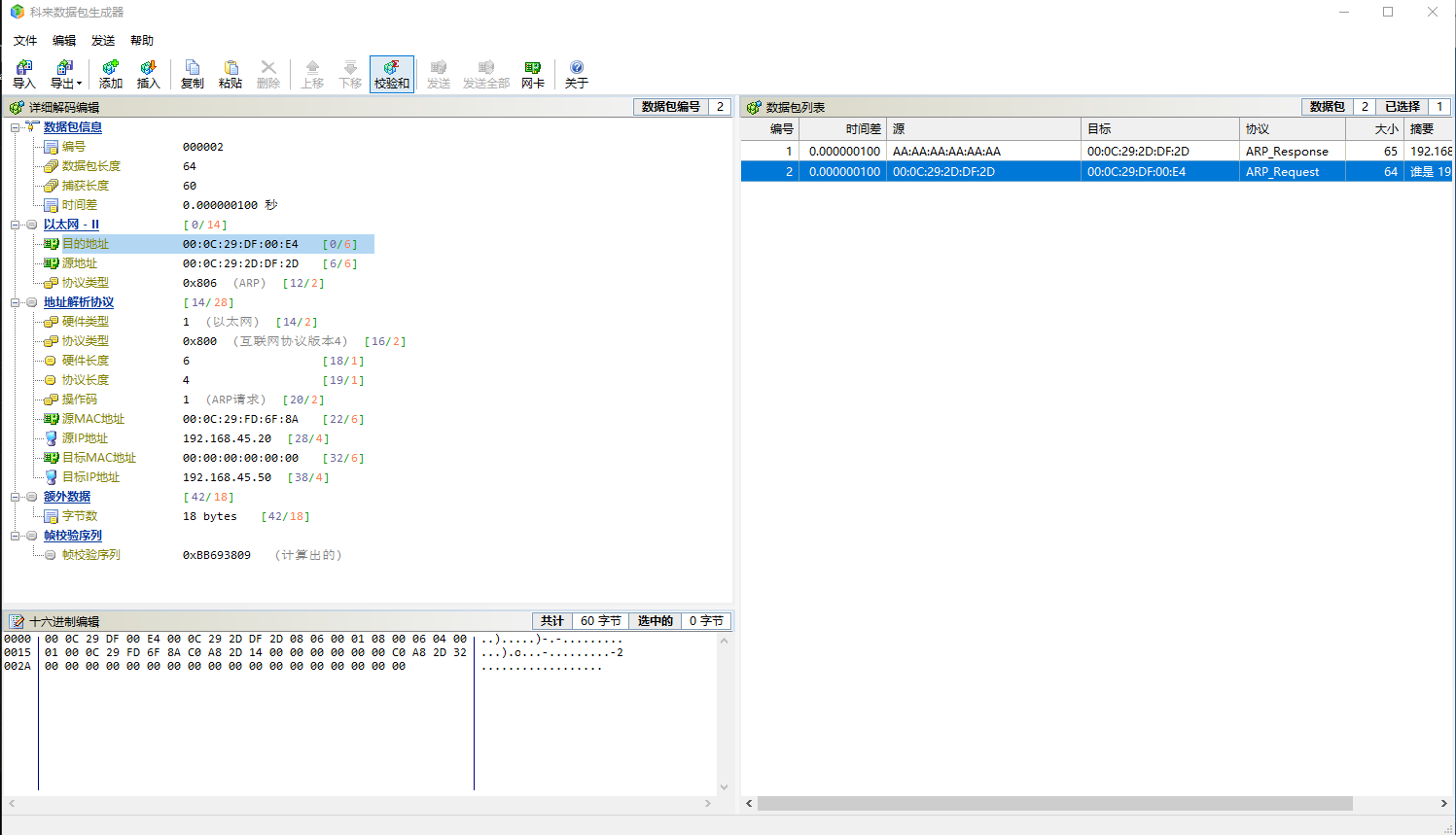
1. ARP协议请求数据包攻击
   1. 重复上述1.1-1.5步骤，即更新局域网中三台主机的ARP缓存，使得IP地址与MAC地址准确映射。
   2. 在Centos8.3上使用ping命令去访问Windows7。



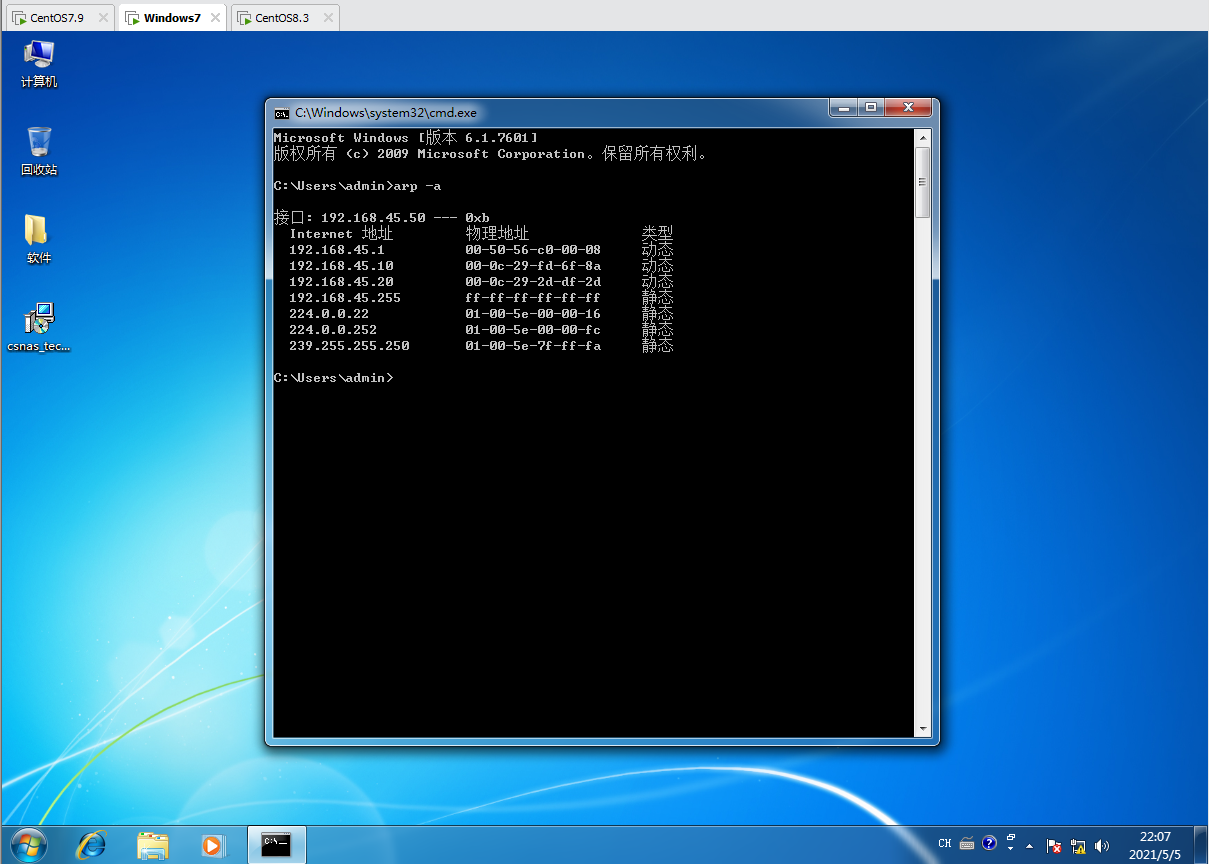
* 1. 查看抓取的数据包，在抓取的数据包中选取一个请求数据包发送到科来数据包生成器软件。



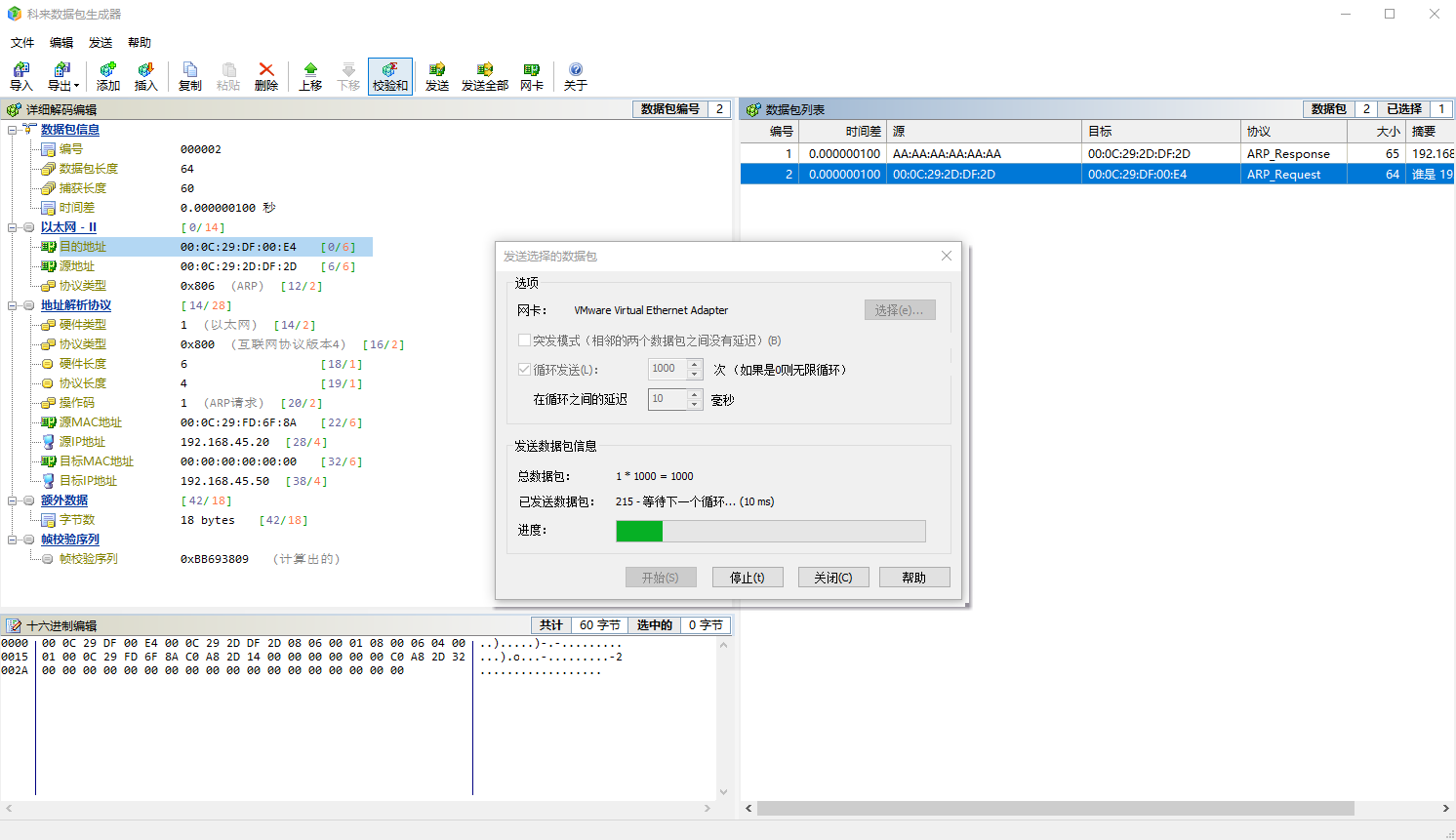
* 1. 对该请求数据进行修改，地址解析协议是CentOS7.9的MAC地址作为源MAC地址，CentOS8.3的IP地址作为源IP地址。这就相当于CentOS7.9冒充CentOS8.3的身份在局域网络中给Windows7发送请求数据包。



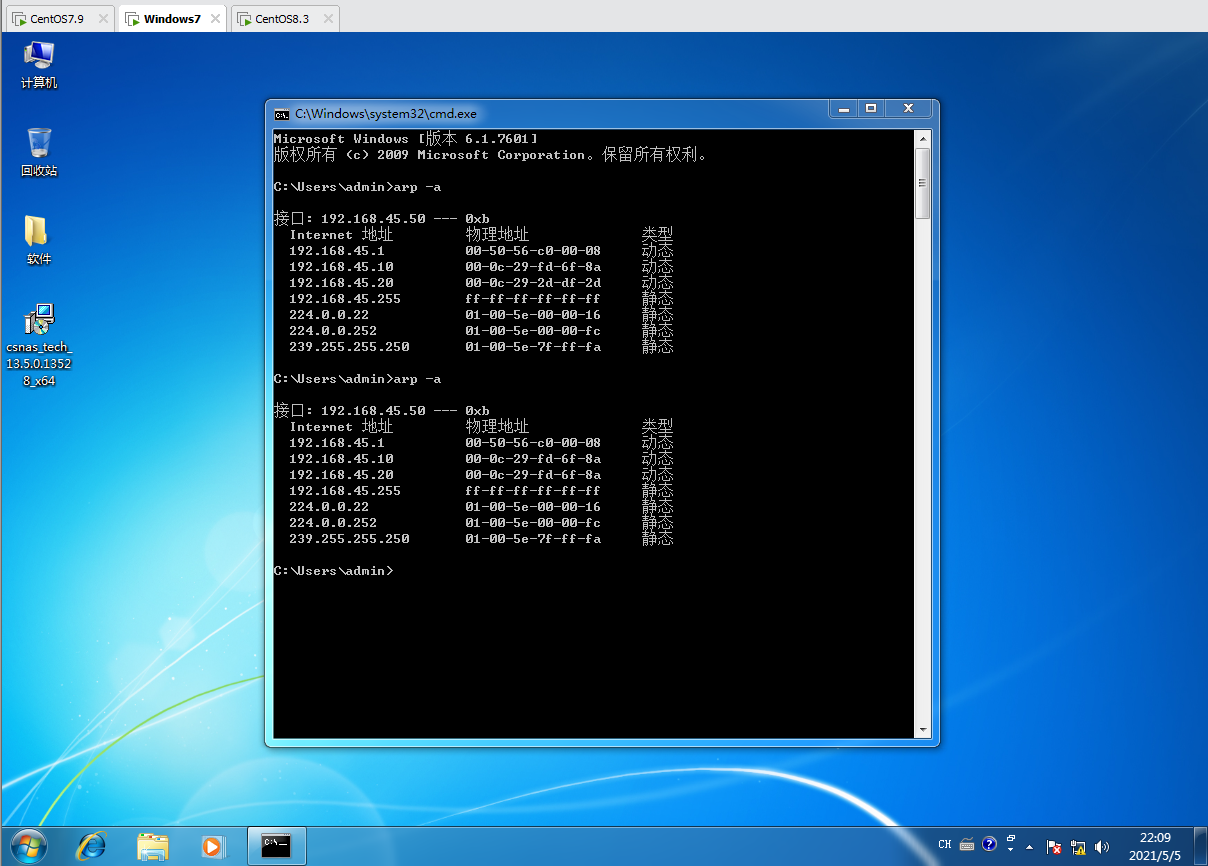
* 1. 查看Windows7的ARP缓存。



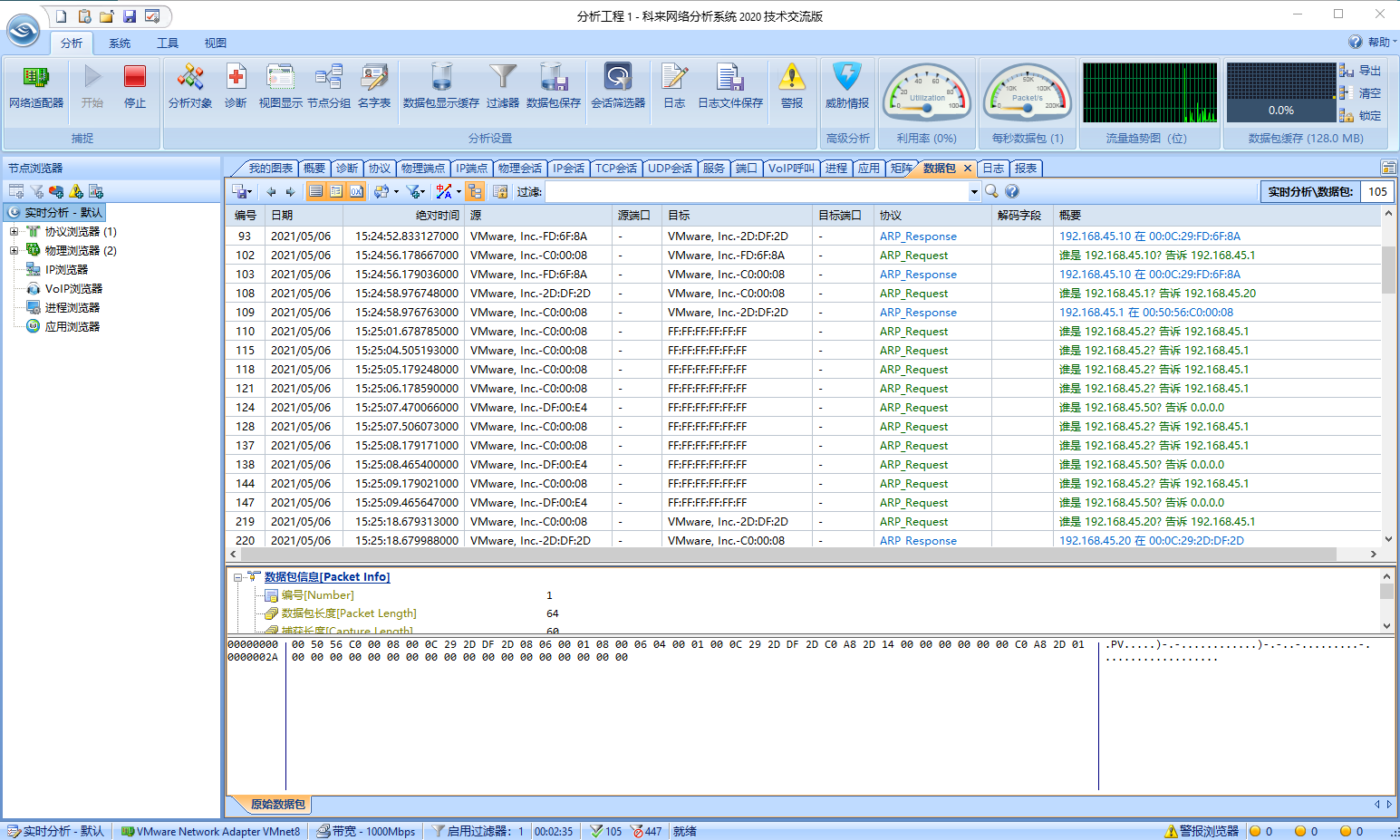
* 1. 把修改后的应答数据包发送到该局域网中。



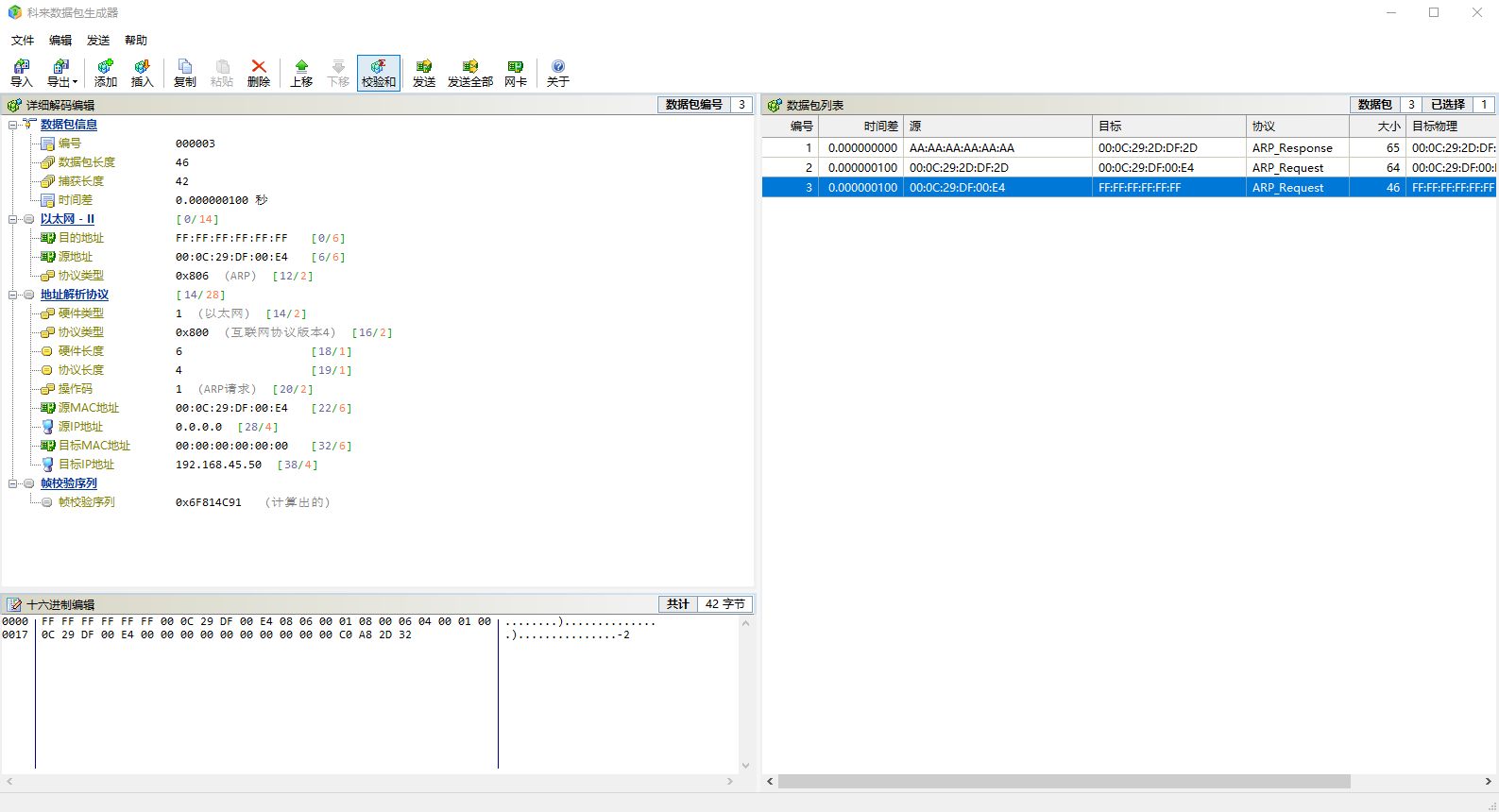
* 1. 再次查看Windows7的ARP缓存，发现192.168.45.20对应的MAC地址发生了变化。



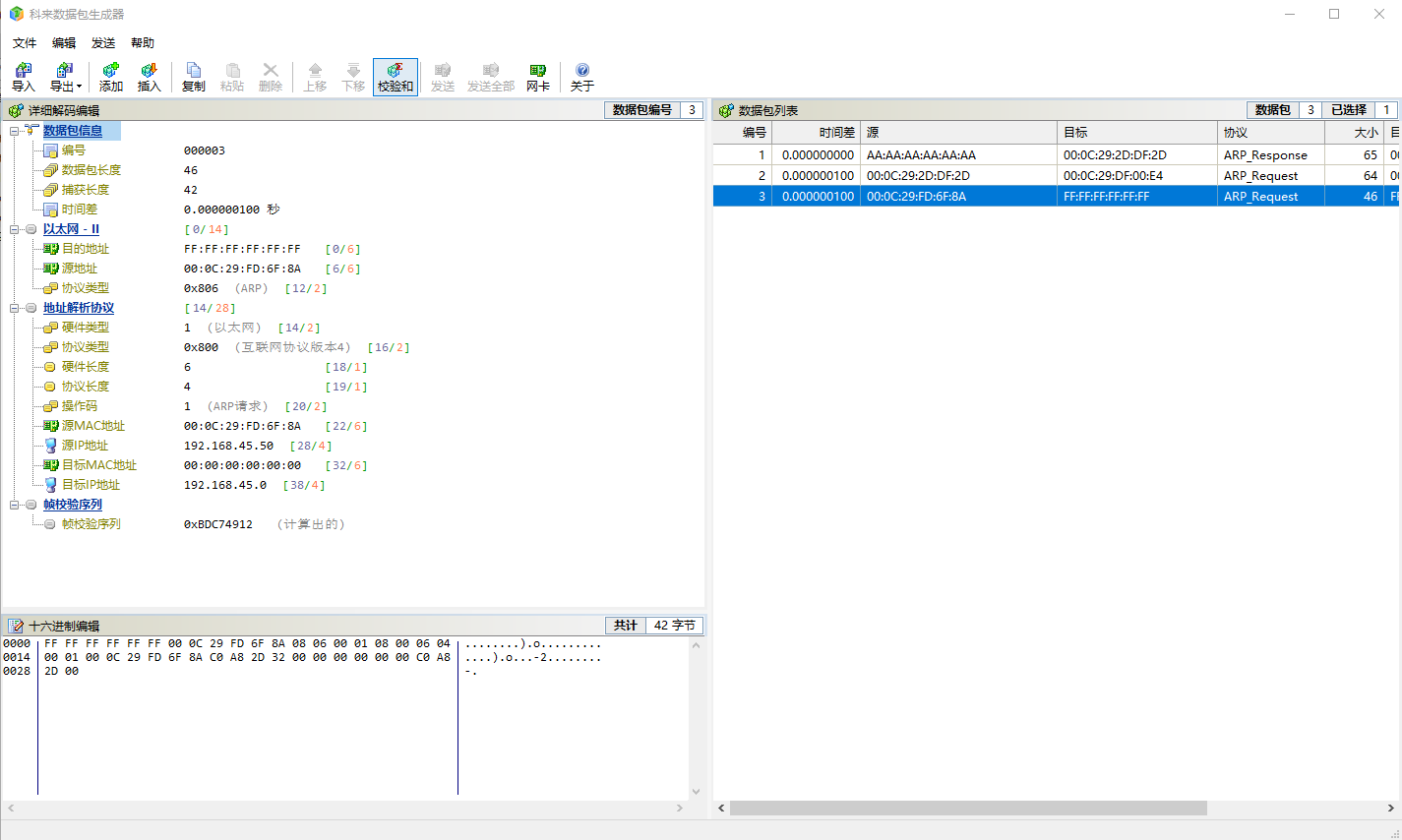
1. 免费ARP数据包攻击
   1. 重复上述1.1-1.5步骤，即更新局域网中三台主机的ARP缓存，使得IP地址与MAC地址准确映射。
   2. 修改Windows7的IP地址为192.168.45.20，重启Windows7前打开抓包软件并开始抓包。



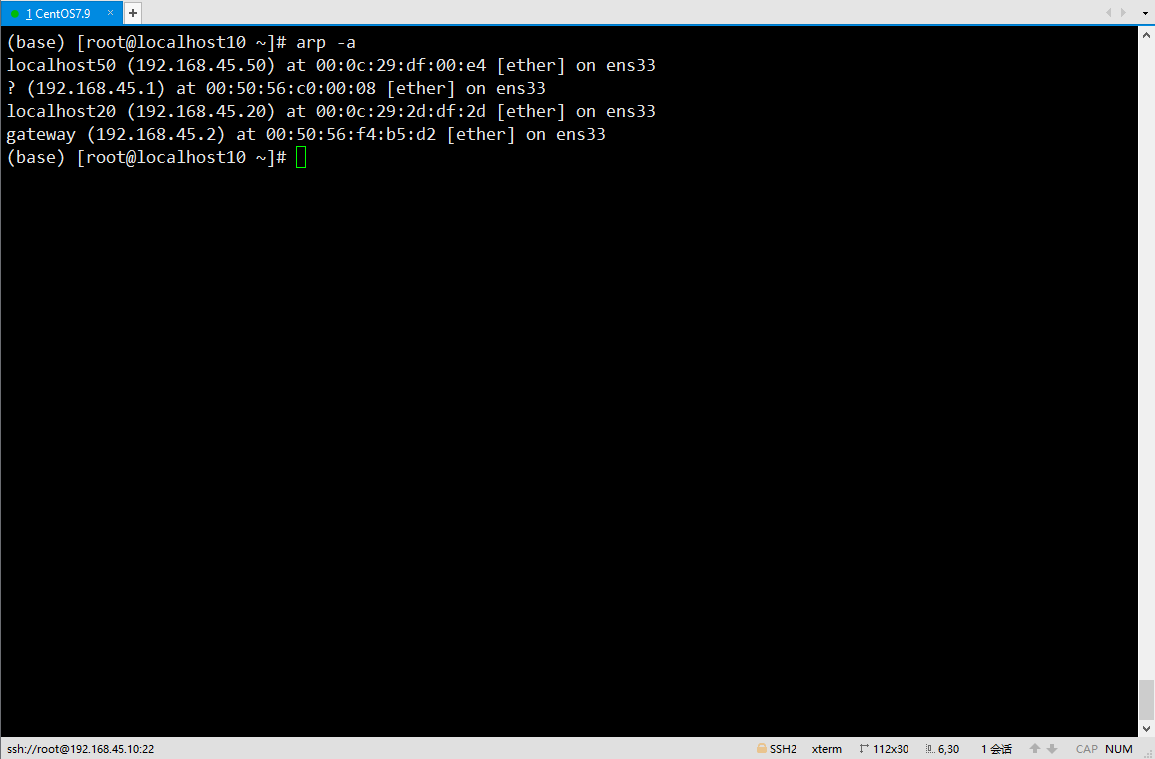
* 1. 在抓取的数据包中选取一个免费ARP数据包发送到科来数据包生成器软件。

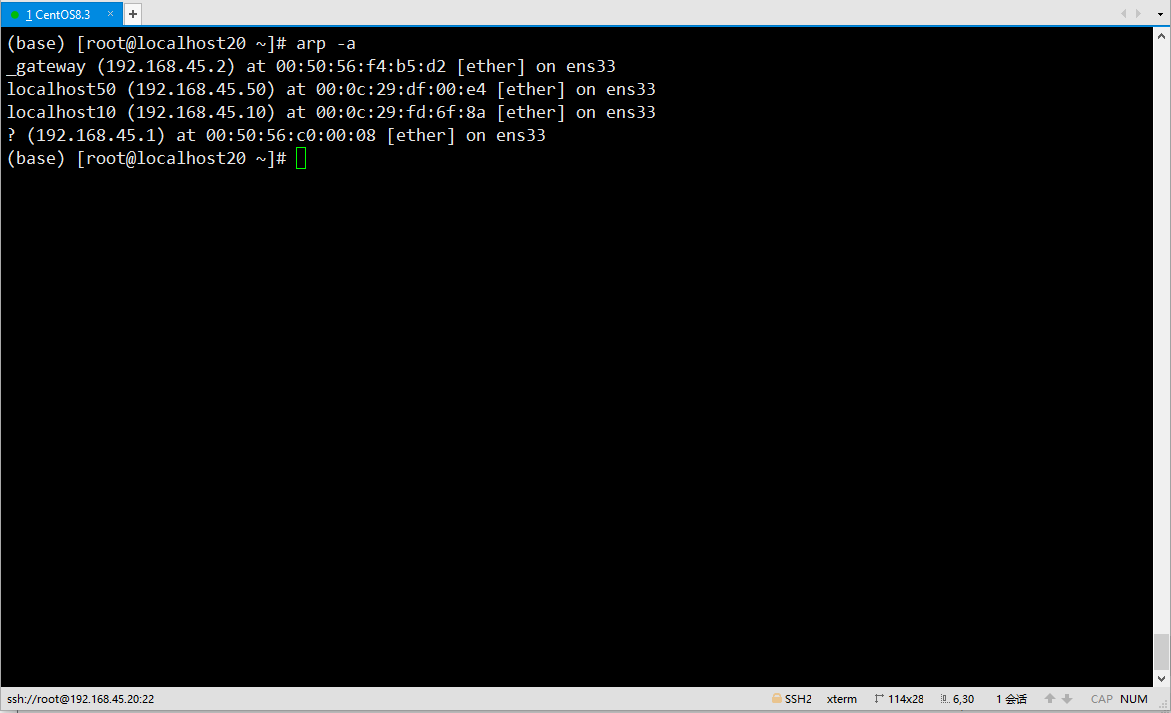


* 1. 对该应答数据进行修改，地址解析协议是CentOS7.9的MAC地址作为源MAC地址，Windows7的IP地址作为源IP地址。使用广播的方式告诉该局域网的所有主机，IP地址为192.168.45.50的主机的MAC地址是CentOS7.9的MAC地址，实际上192.168.45.50的主机是Windows7。

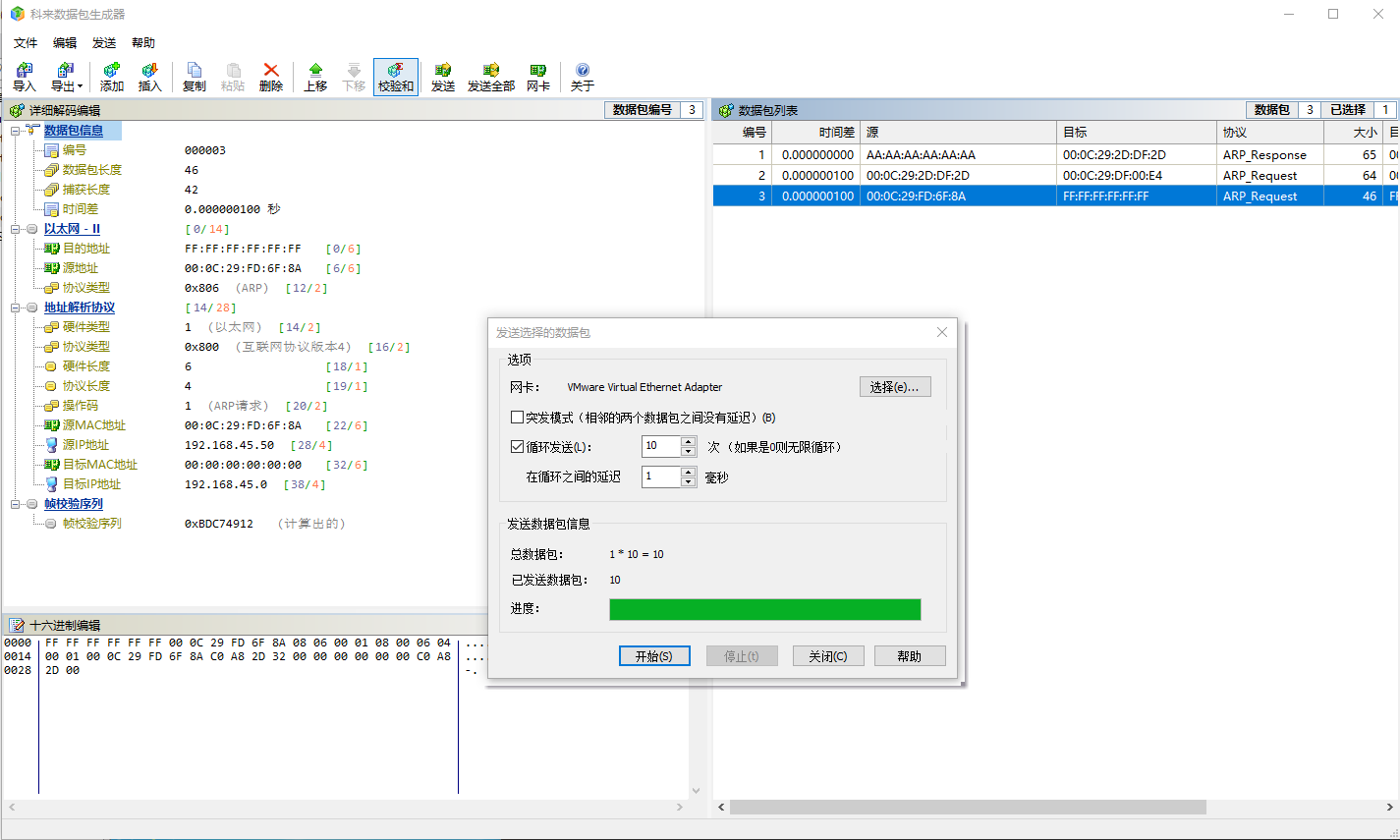


* 1. 在CentOS7.9和CentOS8.3主机的ARP缓存上查看IP为192.168.45.50对应的MAC地址。

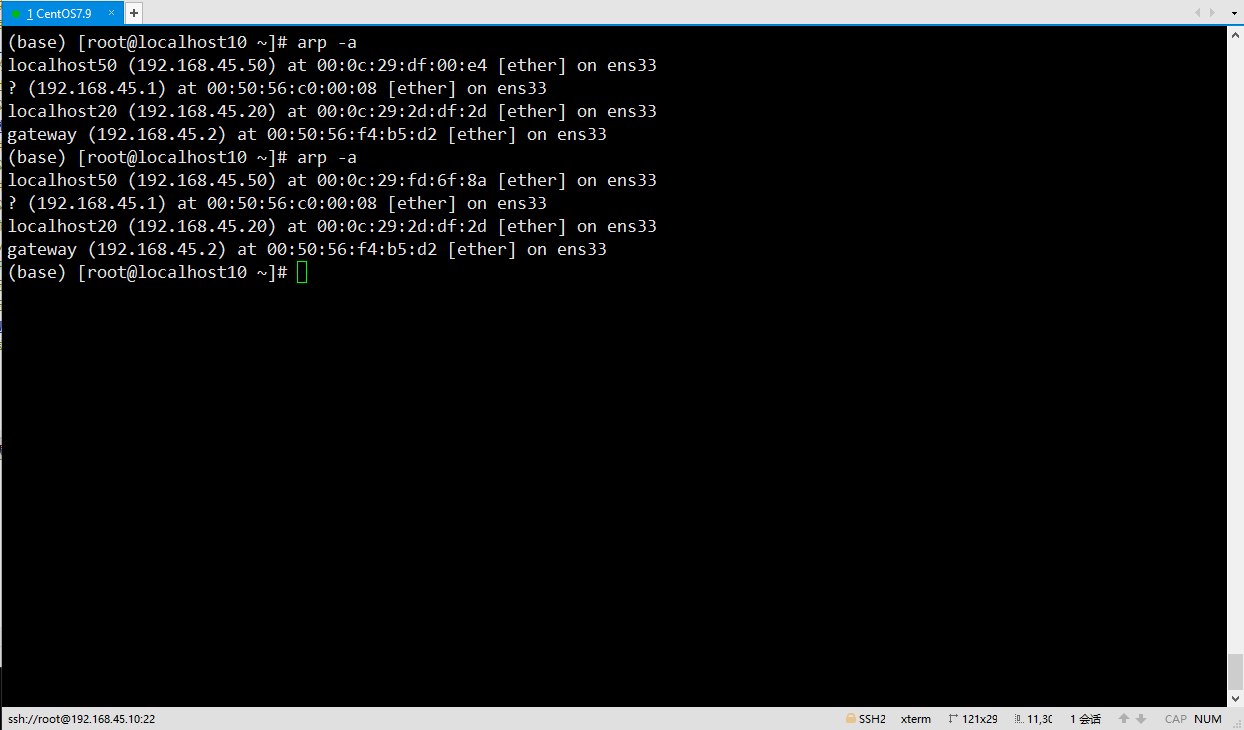


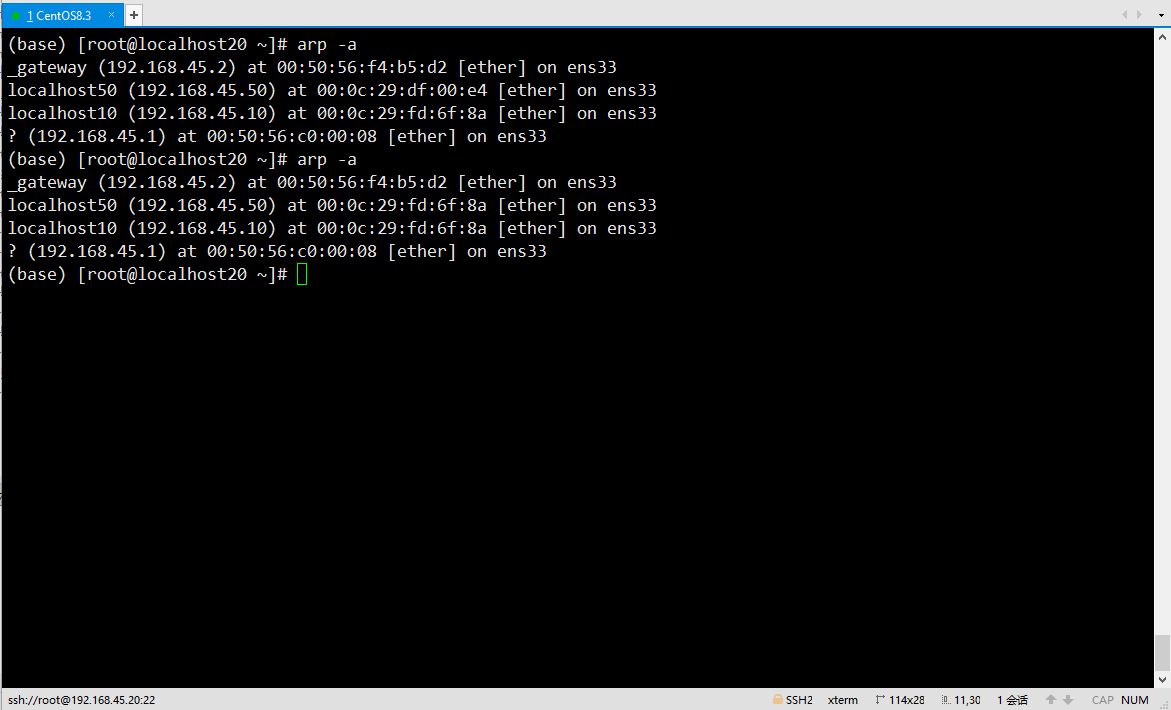


* 1. 把修改后的应答数据包发送到该局域网中。



* 1. 再次查看所有主机的ARP缓存，发现192.168.45.50对应的MAC地址发生了变化。





1. **实验总结**

通过本次实验，我深入的了解了ARP欺骗的原理，分别对三种形式的ARP协议数据包（请求、应答、免费)进行伪造并向攻击目标机发送，实验结果表明，三种形式的ARP包都具备一定的断网攻击能力，但不具有持久性，需要不断地发送伪造数据包才能达到持续攻击的目的。