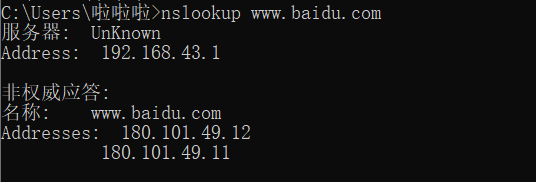
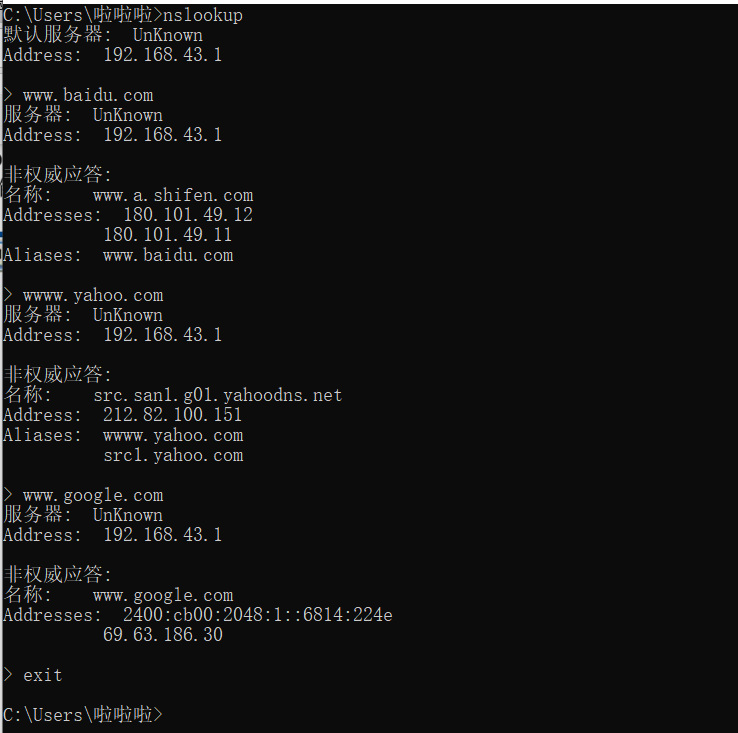
步骤一：lookup解析，wireshark捕获数据包进行分析

2.使用nslookup工具进行域名解析

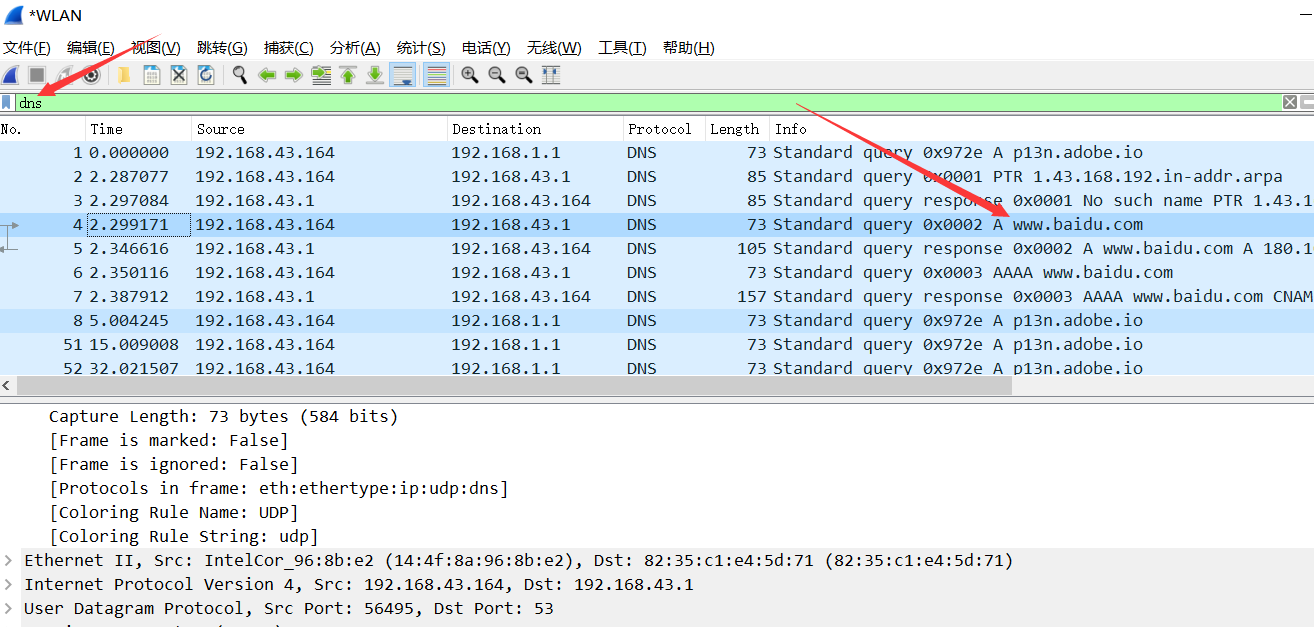


在“>”提示符后输入域名在进行解析，exit退出

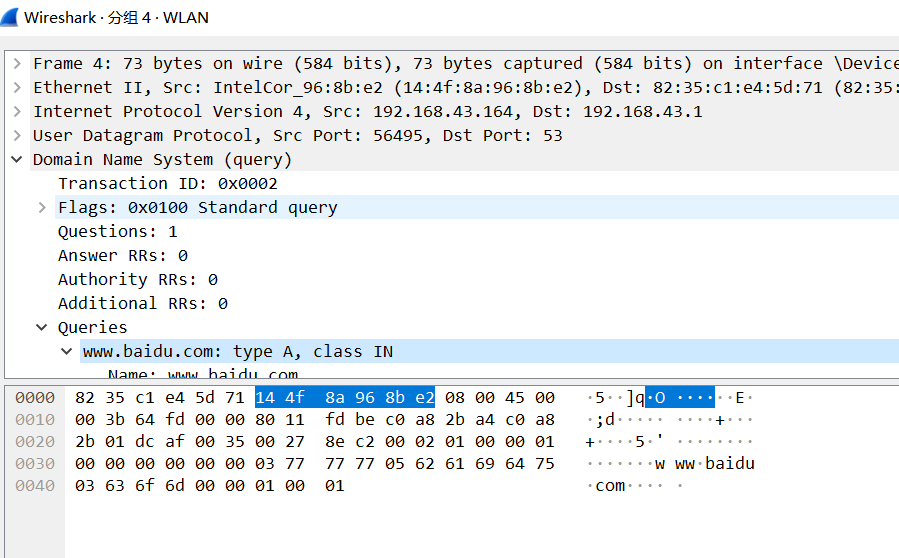


3.分析捕获到的数据报文

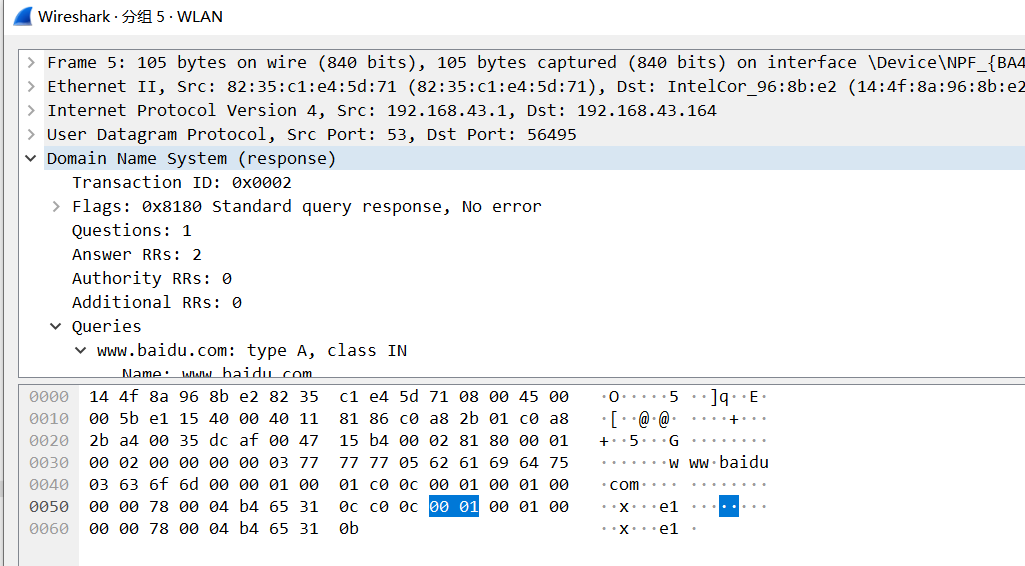
wireshark抓包，过滤出DNS数据包



查看DNS查询报文的详细信息，标识为0x0002, 问题数是1，答案数、权威答案数、附加答案数都是0，如下图



DNS响应报文，报文的标识为10，问题数是1，答案数为2，权威、附加答案数都是0

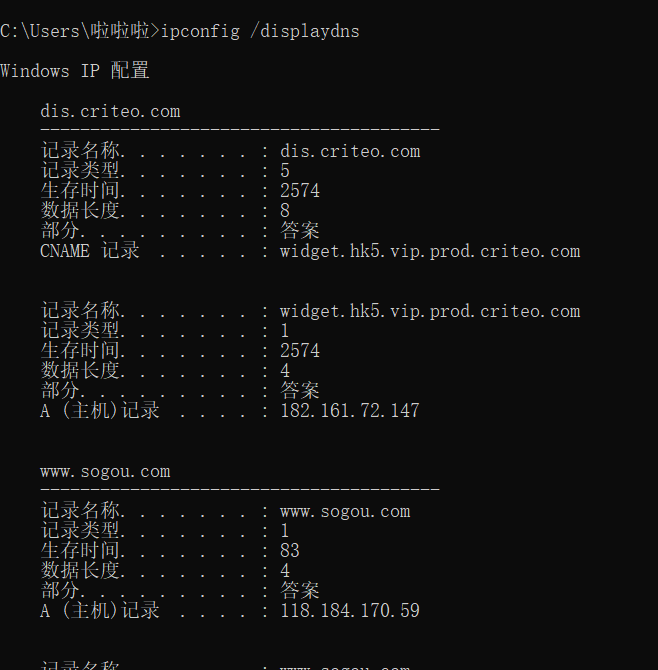


步骤二：使用ipconfig命令查看DNS缓存

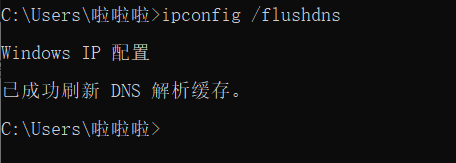
1.本机有了缓存后是不会再次发送DNS请求的

2.是。因为本机没有[www.sohu.com的DNS](http://www.sohu.com的DNS)解析记录

3.本机DNS缓冲区内容



4.清除本机DNS缓存记录

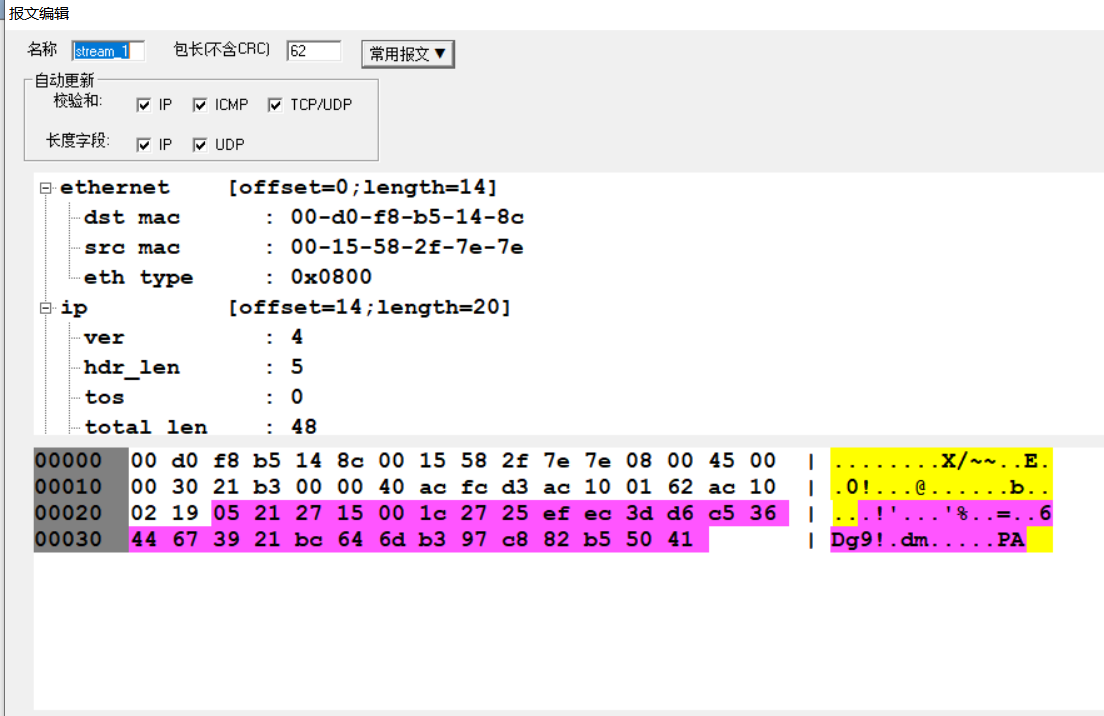


5.有DNS请求

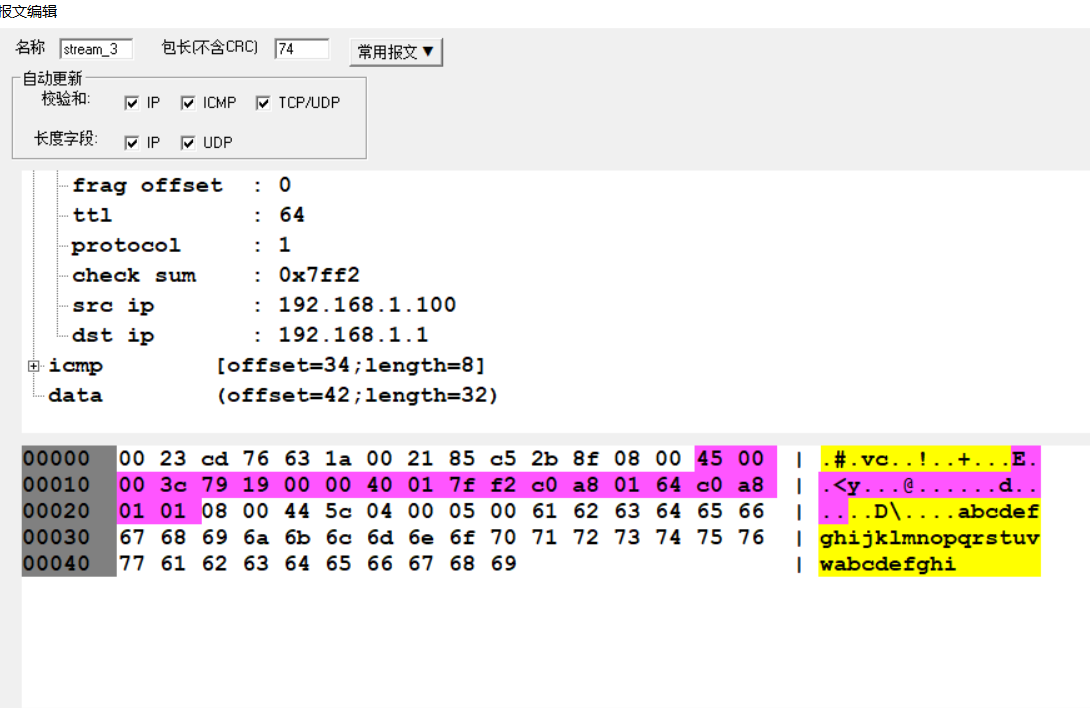
步骤三：编辑数据请求包

利用小兵以太网测试仪软件进行编辑

修改以太网首部信息



修改ip信息



抓包查看

