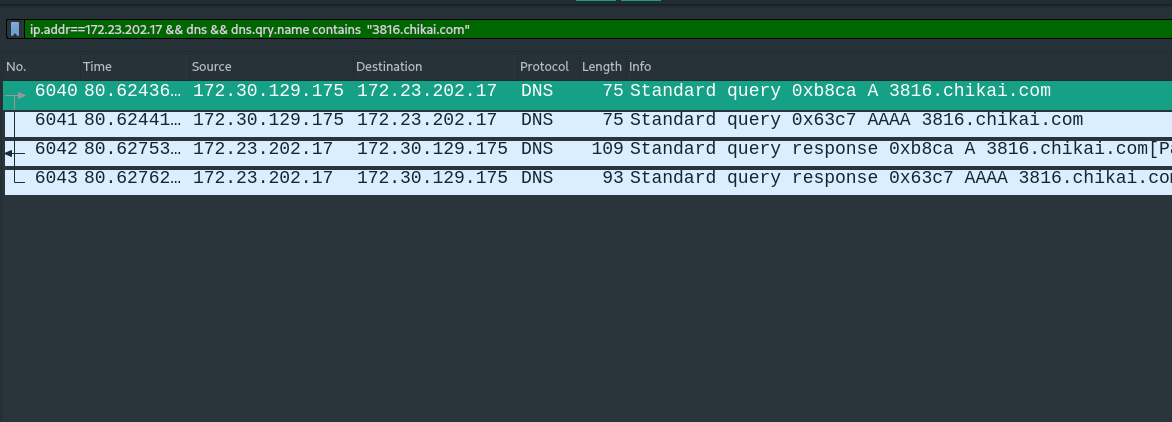


当客户机通过ping命令 请求 3816.chikai.com 时，在缓存中没有相应的记录

通过 设置的DNS 服务器 172.23.202.17 获取 对应的 IP

此时可以抓到相应的数据：



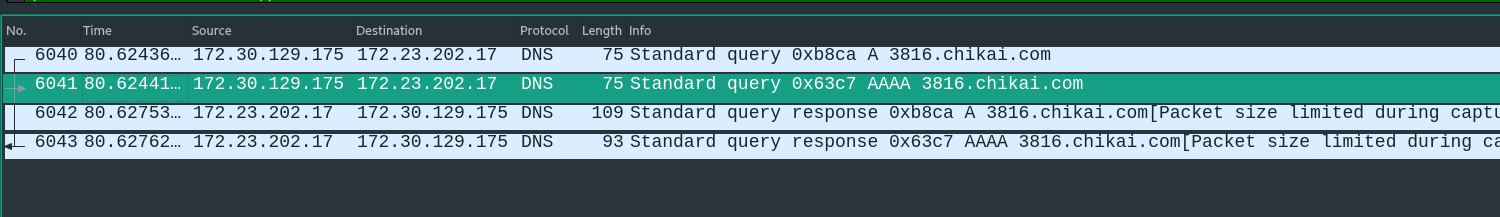
过滤条件为 ip.addr == 172.23.202.17 && dnd && dns.qry.name contains “3816.chikai.com ”

通过 服务器地址过滤 和 dns 协议过滤 加上 域名过滤 得到

ping 3816.chikai.com 的 报文

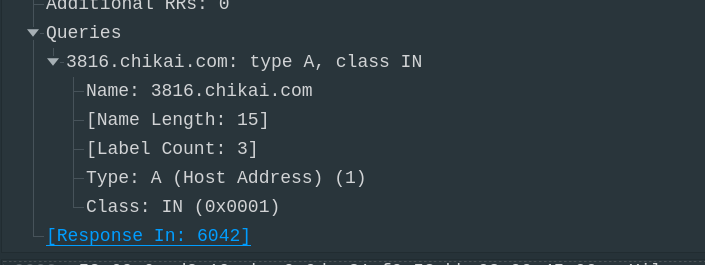
如图 从 6040 到 6043

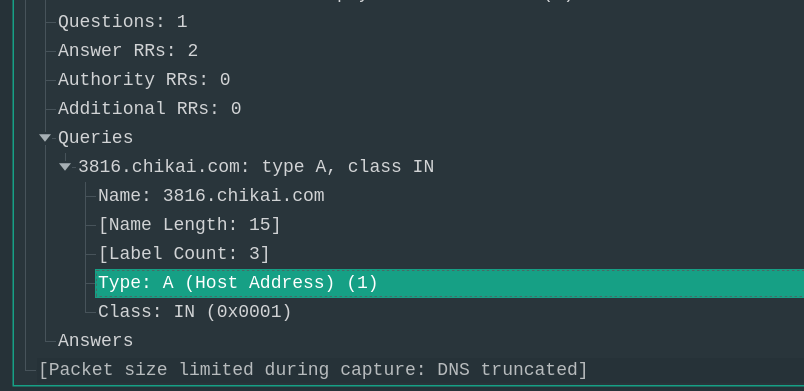
报文是两两相对应的



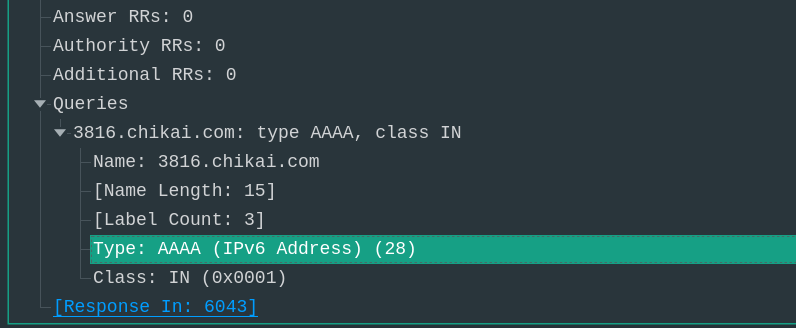
6040 与 6042 对应 ，6041 与 6043 对应

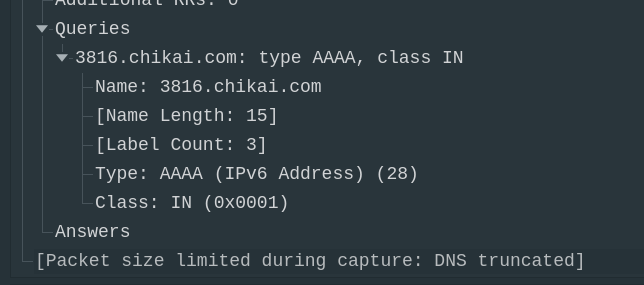
其中 6040 与 6042 查询 3816.chikai.com 的 IPV4 地址 如图：



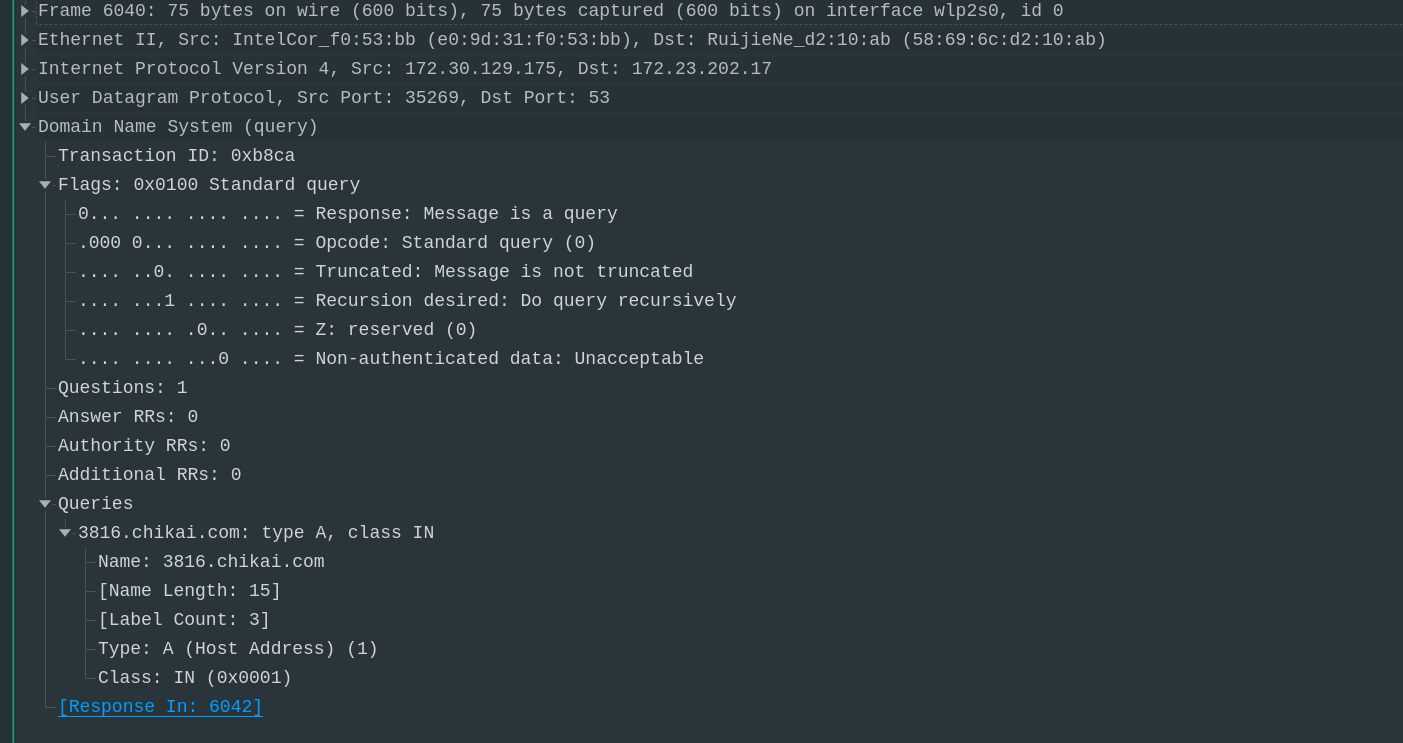


6041 与 6043 查询 IPV6 地址：





对 6040 分析：



可以看出 ， 传输层 使用 UDP 协议，端口为 53

DNS 协议部分：

事务 ID 与 相应的回答报文一致 为 0xb8ca

Question 表示问题数目为 1

问题部分：

type A 表明 查询 IPV4 ， AAAA 表明查询 IPV6

name 为相应的域名 3816.chikai.com

class 地址类型 互联网地址 为 1

回答报文 6042：

