**1. 写出用ping指令向www.baidu.com 发送8个大小为80byte的ICMP包的指令。**



指令格式：ping –l 80 –n 8 www.baidu.com

-l 表示发送的包的大小（默认32KB）

-n 表示发送包的数量（默认4个）

TTL是往返所经过的路由节点的个数

**2、使用Wireshark软件抓取数据包分析网络封装，在过滤器中过滤源ip为192.168.1.10，目的ip为192.168.1.20的数据包。写出该过滤表达式。**

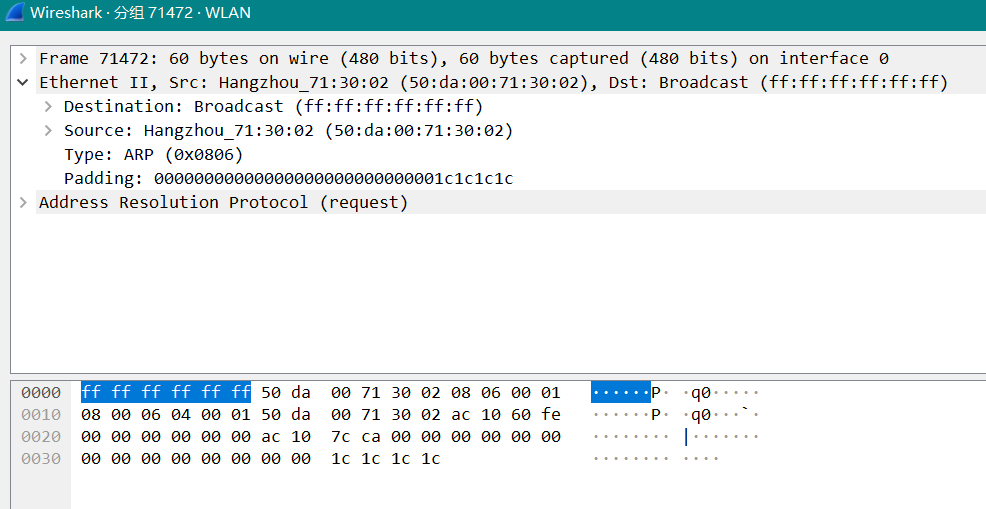
表达式：(ip.dst == 192.168.1.10 )&& (ip.src == 192.168.1.20)

dst是目的，src是源

ip.scr表示源ip地址

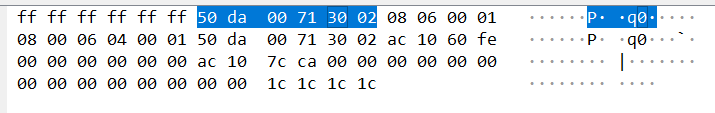
其他的括号和&& == 等符号和其他语言相同，过滤选择整个表达式值为true的所有内容。

3、使用Wireshark抓取一个ARP数据包，分析其各字段含义。

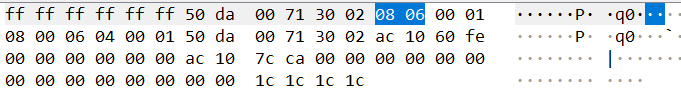


目的mac地址：ff ff ff ff ff ff（表示广播）

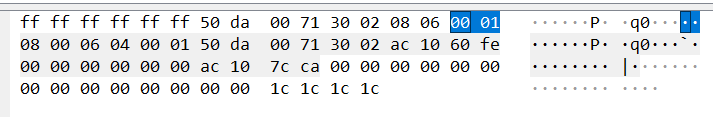
源mac地址：50 da 00 71 30 02



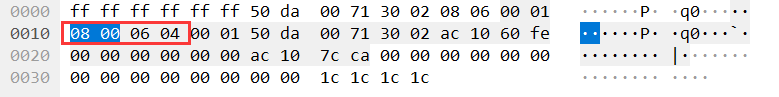
报文类型：(08 06 是ARP协议)



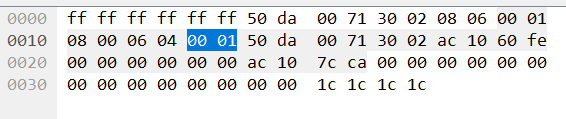
表示以太网1（ethernet1）



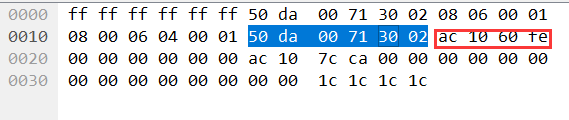
08 00表示IP协议中APR的协议号，06,04分别代表MAC、该协议的长度



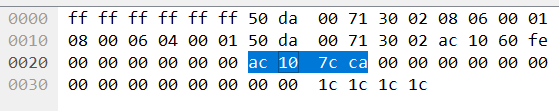
Opcode = 0001表示ARP请求报文（0002表示应答报文）



蓝色和红框分别代表源MAC和IP



由于是请求报文，该目的mac为空，只有目的IP = ac.10.7c.ca



ARP字节长度只有42字节，但是IP数据包最小长度为64字节，因此后续的0是填充部分，最后有四位没写出来是校验和。

