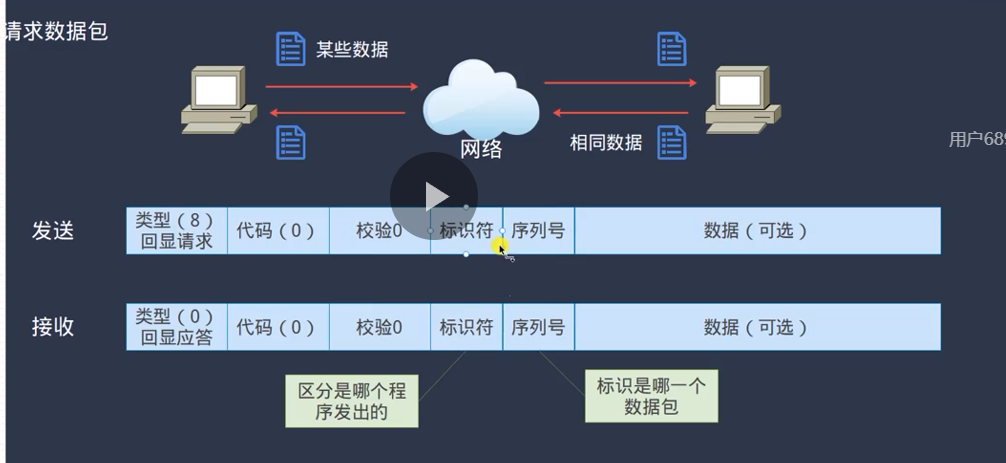
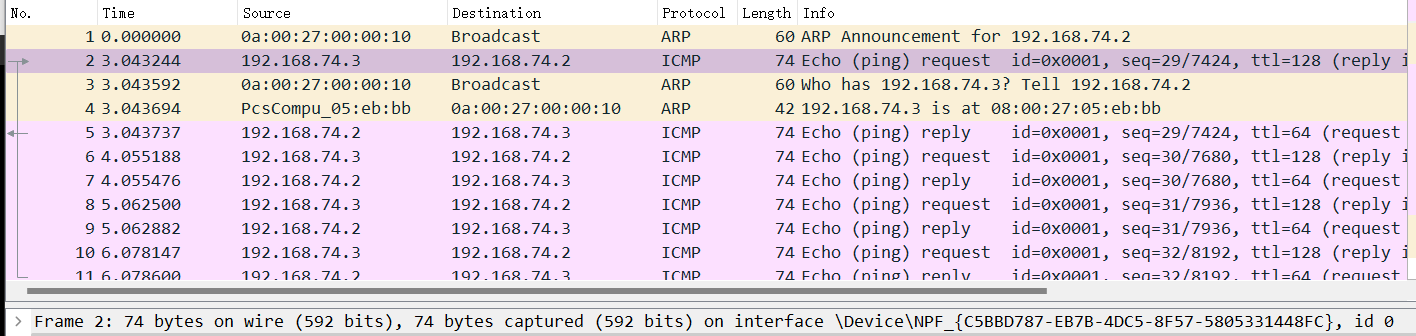


这里注意，ipv4的校验和只是覆盖了ipv4包头的本身,而icmp的校验和覆盖了整个icmp数据包



因为可能会有多个cmd发送ping命令，所以标识符是标识哪个cmd发出的，一般填入进程号，而ping命令，可能会连续好几个icmp包发出去，所以序列号标识回包对应着哪次发出去的包

报文分析(包在同目录下):

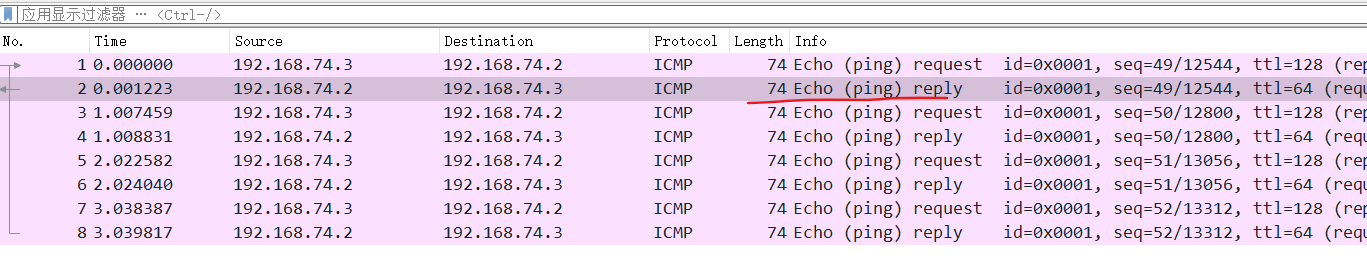


第一条报文,是我方协议栈启动的时候,自动发送的,告诉别的机器,这个ip我用了,如果你们不回复,那么这个ip我就可以用(也是由于这个arp,别的机器会缓存这个arp发送方的网卡ip和mac地址)。然后虚拟机发送ping命令,协议栈收到该报文后, 因为arp缓存中没有虚拟机的mac地址，所以就发了arp包出去，接着收到arp回包后，就回复ping包了

但是这样的逻辑其实是有点问题的

因为这个icmp包是包含发送方的ip和mac地址的，所以可以直接更新协议栈中的arp缓存，这样就协议栈就不用再发送arp去查询回包需要的对端mac地址了

重新修改逻辑后，里面回复icmp包了(报文见icmp\_ipdate.pcapng)



注意：协议栈启动的时候会发arp协议

如果没有对方mac地址，肯定会发arp去查询mac地址，就算ping命令也是，所以如果本地没有对方mac，而且对方挂了，那么arp发出去没响应(,由于没有mac，所以先arp，等收到mac再发ping)，如果本地有mac地址，但是对方挂了，ping发出去也没响应，而且可能还有arp的发送包