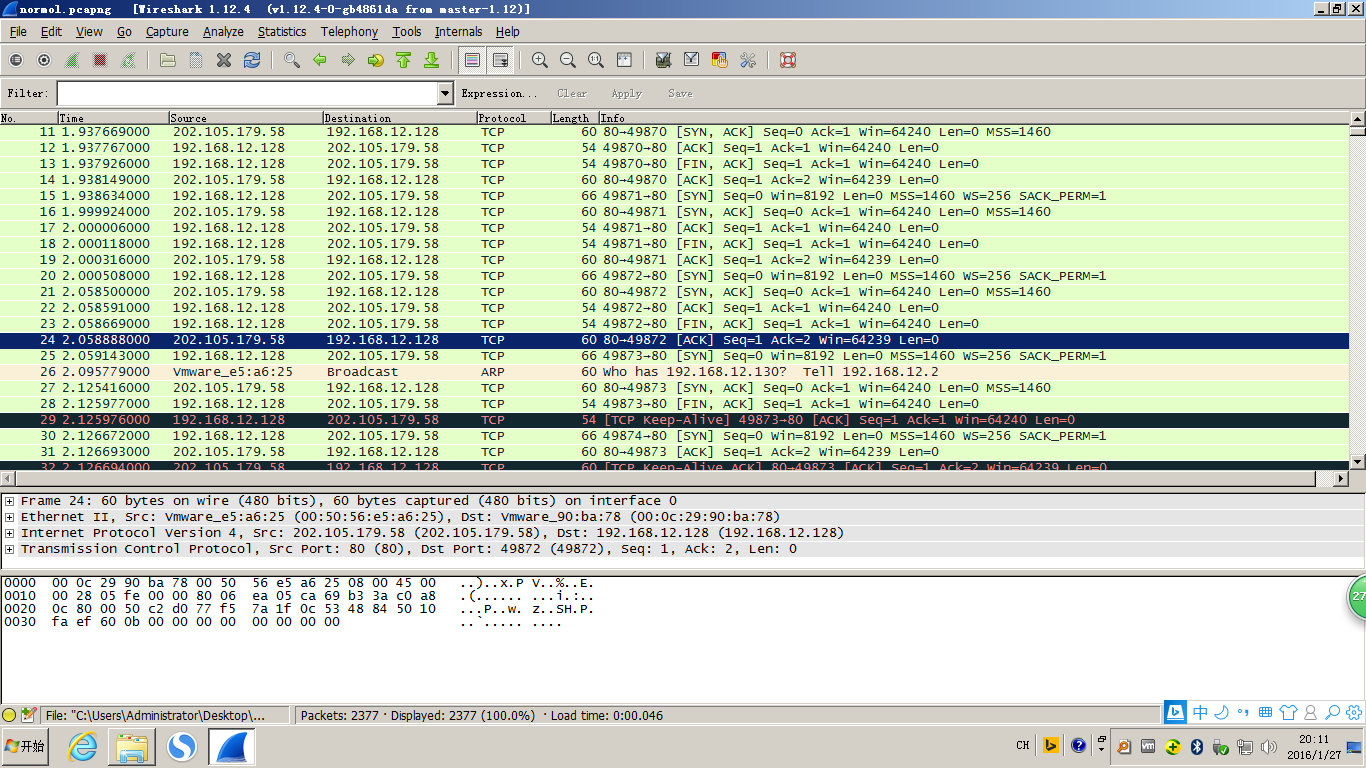
# Xoic

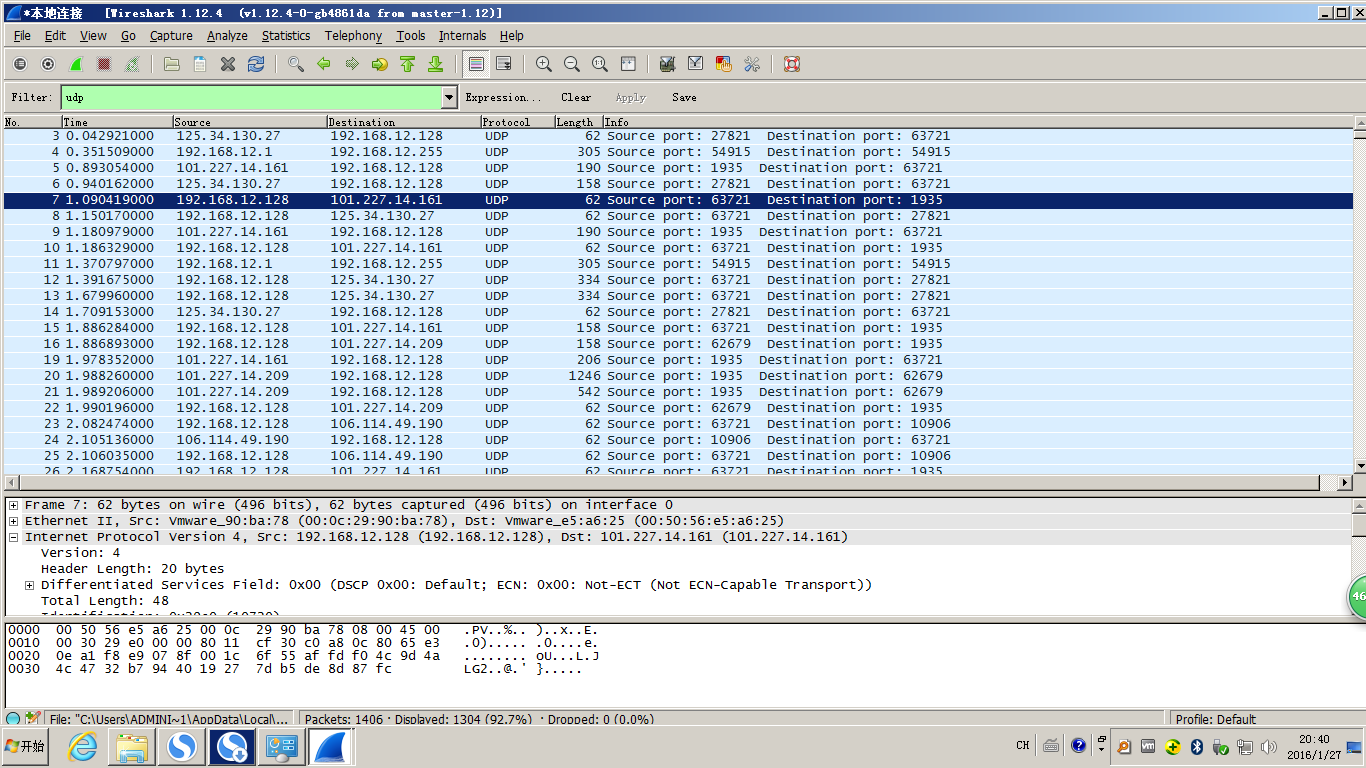
Xoic有4种攻击方式，分别是 normal，tcp，udp，icmp

Normal这种攻击方式是不停地用依次递增的端口去对服务器进行正常的tcp三次握手连接。连接完毕后发送结束连接，然后用下一个端口重复之前的操作。如图

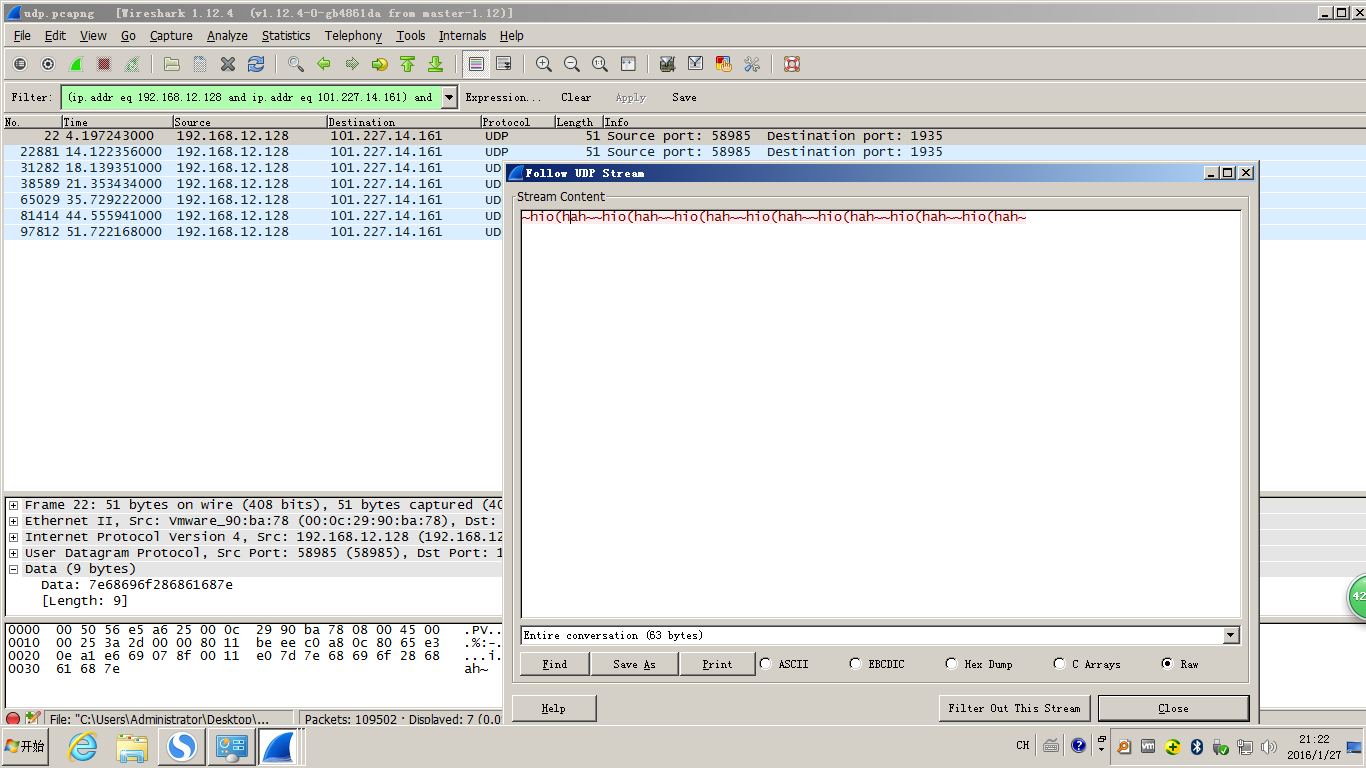
（图1）

Tcp 和 normal一样。

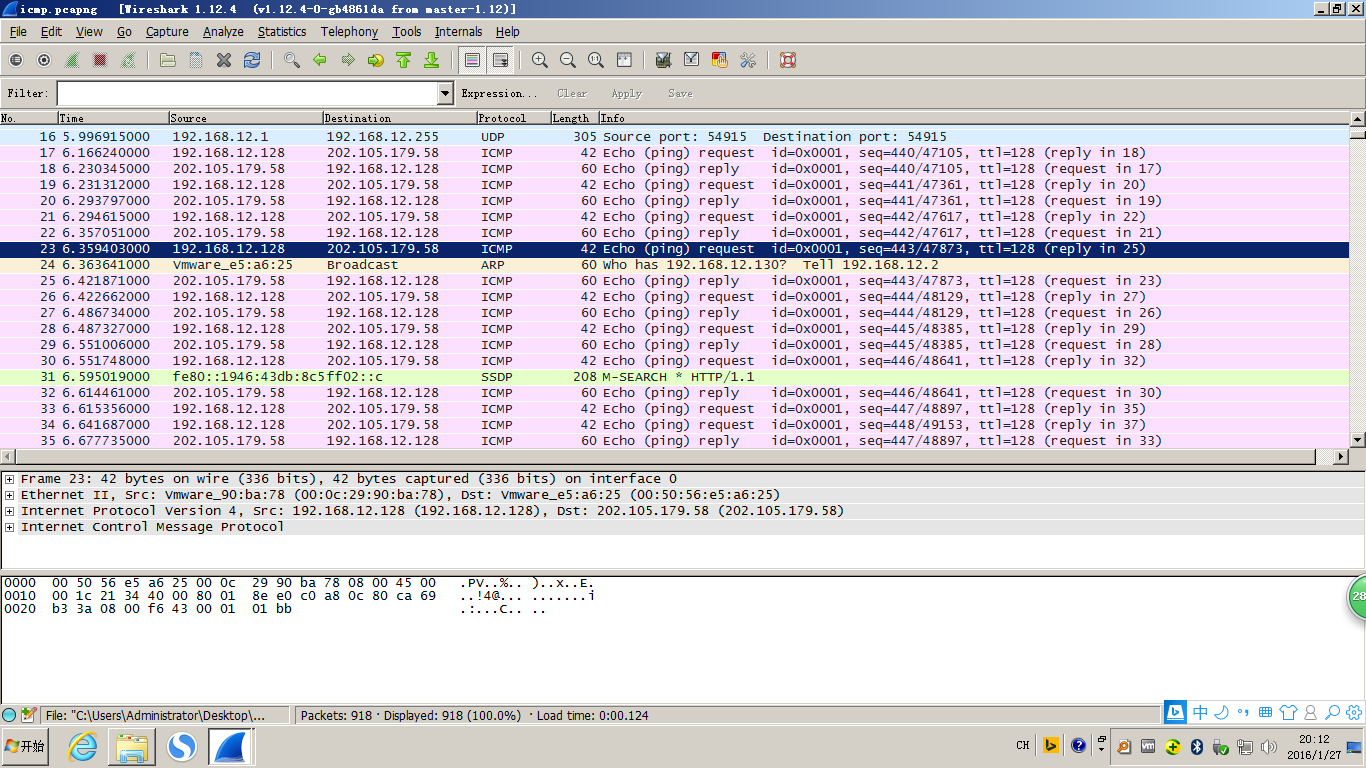
Udp 是一个无连接协议，传输数据之前源端和终端不建立连接，当它想传送时就简单地去抓取来自应用程序的数据，并尽可能快地把它扔到网络上。也就是说，没有发送方和接收方之间连接建立过程，直接发。对比TCP，是不可靠的，本身并不去检查传递过程中数据报的丢失情况。如下图（图二）数据包7和9就是UDP连接的过程。用XOIC进行UDP攻击的时候，软件进行的就是不断换端口给服务器发信息。



在抓包中发现，软件攻击特征。发送的数据都是~hio(hah~~hio(hah~~hio(hah~~hio(hah~~hio(hah~~hio(hah~~hio(hah~

如下图：

Icmp 这种攻击方式是不停地用依次递增的端口去对服务器进行ping连接。如图



（图3）