Wireshark常用过滤使用方法

过滤源ip、目的ip。

在wireshark的过滤规则框Filter中输入过滤条件。如查找目的地址为192.168.101.8的包，ip.dst==192.168.101.8；查找源地址为ip.src==1.1.1.1

端口过滤。

如过滤80端口，在Filter中输入，tcp.port==80，这条规则是把源端口和目的端口为80的都过滤出来。使用tcp.dstport==80只过滤目的端口为80的，tcp.srcport==80只过滤源端口为80的包

协议过滤

比较简单，直接在Filter框中直接输入协议名即可，如过滤HTTP的协议

http模式过滤。

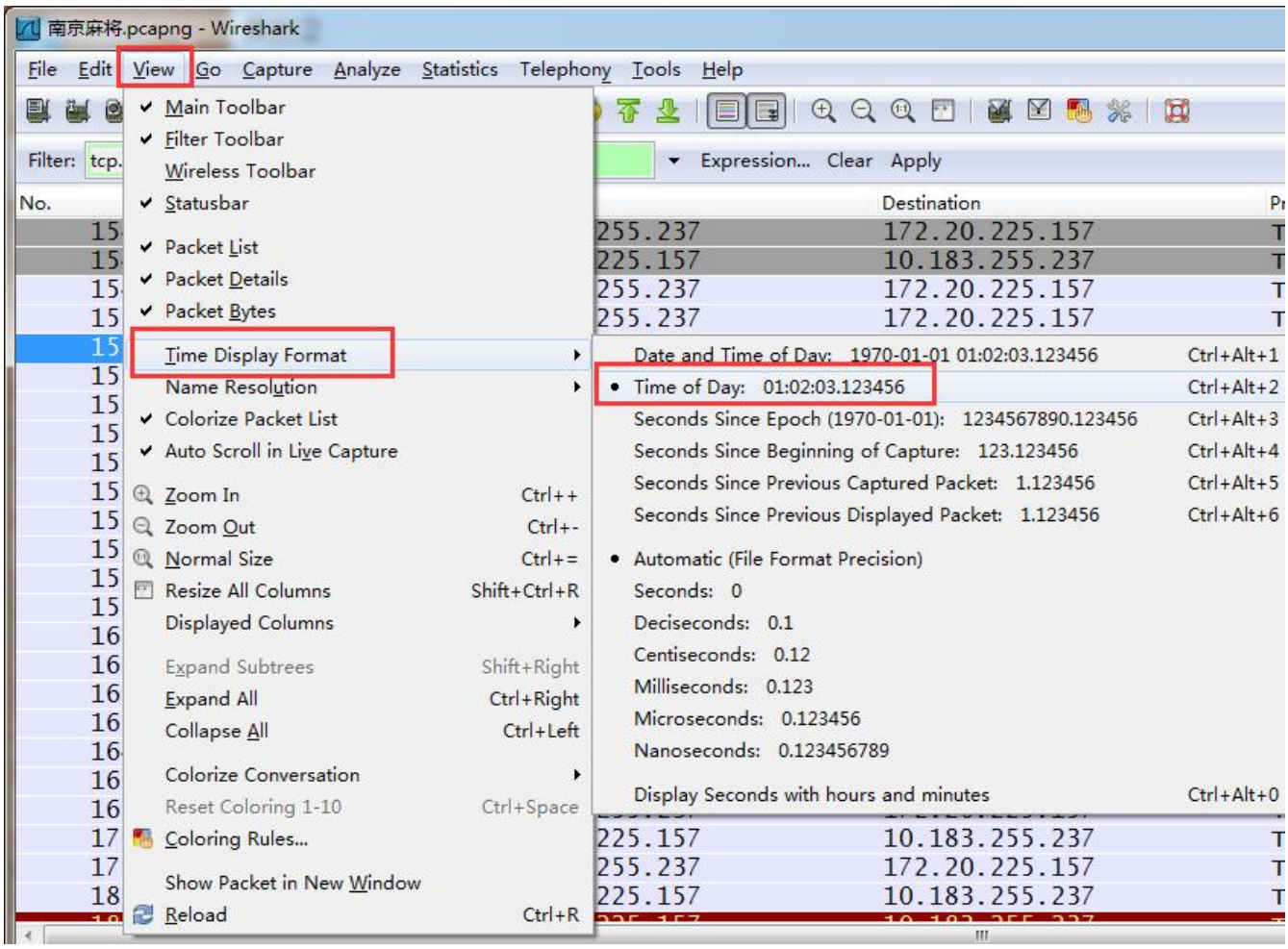
如过滤get包，http.request.method=="GET",过滤post包，http.request.method=="POST"

连接符and的使用。

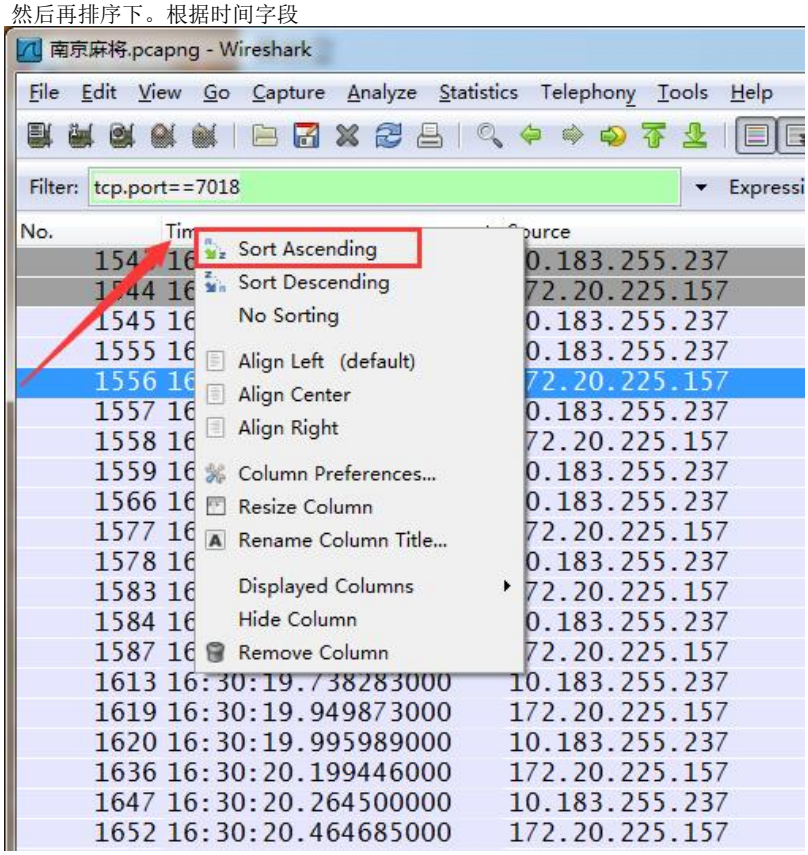
过滤两种条件时，使用and连接，如过滤ip为192.168.101.8并且为http协议的，ip.src==192.168.101.8 and http。

工作中，一些使用方式

调整时间格式



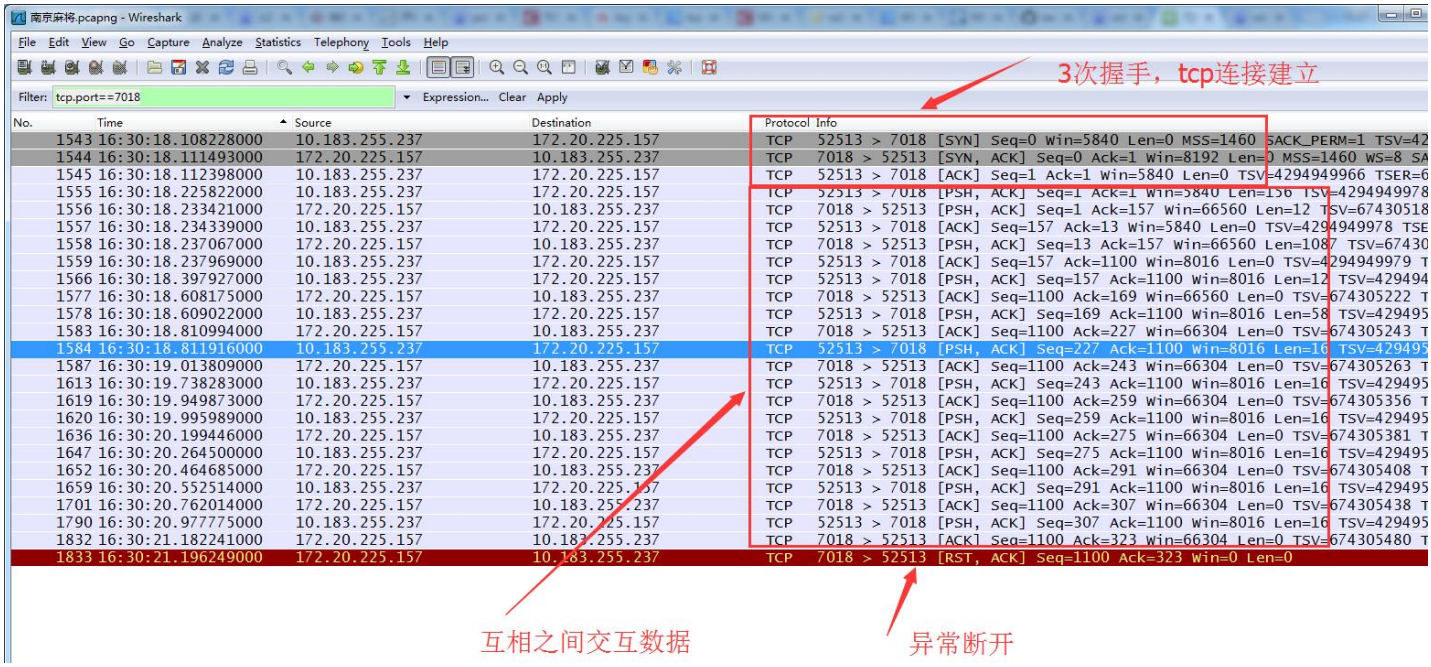
然后再排序下。根据时间字段



根据端口过滤

服务端端口是**7018**，和客户端建立**socket**连接，根据服务端的端口找到**2**者通信的所有**socket**数据（客户端进入房间后会异常断开，判断是客户端导致的还是服务端导致的）

tcp.port==7018，最后的**RST**报文是服务端发起的，说明是服务端主动断开的，缩小问题范围



仅从抓包信息看是服务器的一个流量控制机制启动了。服务器发回rst位，同时win置为0，是告诉客户端不要发包。按tcp流控机制来说，此时客户端应该停止发包，直至服务器发送信息告诉客户端可以继续发送。

TCP连接:SYN ACK RST UTG PSH FIN
三次握手：发送端发送一个SYN=1，ACK=0标志的数据包给接收端，请求进行连接，这是第一次握手；
接收端收到请求并且允许连接的话，就会发送一个SYN=1，ACK=1标志的数据包给发送端，告诉它，可以通讯了，并且让发送端发送一个确认数据包，这是第二次握手；
最后，发送端发送一个SYN=0，ACK=1的数据包给接收端，告诉它连接已被确认，这就是第三次握手。之后，一个TCP连接建立，开始通讯。

*SYN：同步标志
同步序列编号(Synchronize Sequence Numbers)栏有效。该标志仅在三次握手建立TCP连接时有效。它提示TCP连接的服务端检查序列编号，该序列编号为TCP连接初始端(一般是客户端)的初始序列编号。
在这里，可以把 TCP序列编号看作是一个范围从0到4，294，967，295的32位计数器。通过TCP连接交换的数据中每一个字节都经过序列编号。在TCP报头中的序列编号栏包括了TCP分段中第一个字节的序列编号。

*ACK：确认标志
确认编号(Acknowledgement Number)栏有效。大多数情况下该标志位是置位的。TCP报头内的确认编号栏内包含的确认编号(w+1，Figure-1)为下一个预期的序列编号，同时提示远端系统已经成功接收所有数据。

*RST：复位标志
复位标志有效。用于复位相应的TCP连接。

*URG：紧急标志
紧急(The urgent pointer) 标志有效。紧急标志置位，

*PSH：推标志
该标志置位时，接收端不将该数据进行队列处理，而是尽可能快将数据转由应用处理。在处理 telnet 或 rlogin 等交互模式的连接时，该标志总是置位的。

*FIN：结束标志
带有该标志置位的数据包用来结束一个TCP回话，但对应端口仍处于开放状态，准备接收后续数据。

TCP的几个状态对于我们分析所起的作用。在TCP层，有个FLAGS字段，这个字段有以下几个标识：SYN, FIN, ACK, PSH, RST, URG.其中，对于我们日常的分析有用的就是前面的五个字段。它们的含义是：SYN表示建立连接，FIN表示关闭连接，ACK表示响应，PSH表示有 DATA数据传输，RST表示连接重置。
其中，ACK是可能与SYN，FIN等同时使用的，比如SYN和ACK可能同时为1，它表示的就是建立连接之后的响应，如果只是单个的一个SYN，它表示的只是建立连接。
TCP的几次握手就是通过这样的ACK表现出来的。但SYN与FIN是不会同时为1的，因为前者表示的是建立连接，而后者表示的是断开连接。
RST一般是在FIN之后才会出现为1的情况，表示的是连接重置。一般地，当出现FIN包或RST包时，我们便认为客户端与服务器端断开了连接；而当出现SYN和SYN＋ACK包时，我们认为客户端与服务器建立了一个连接。
PSH为1的情况，一般只出现在DATA内容不为0的包中，也就是说PSH为1表示的是有真正的TCP数据包内容被传递。TCP的连接建立和连接关闭，都是通过请求－响应的模式完成的。