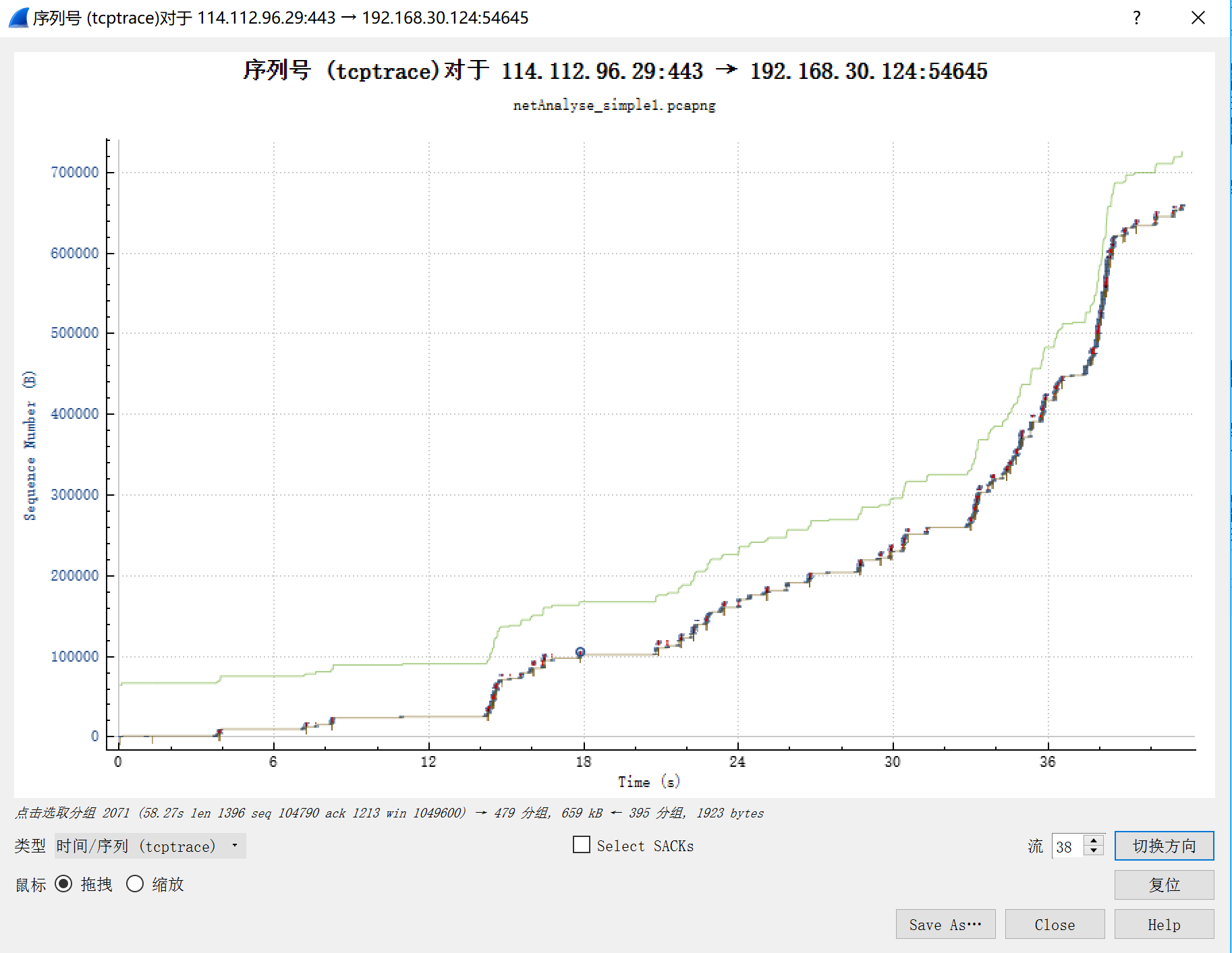
# 如何打开TCP数据流分析图形

和TCP数据流图形Stevens一样，TCP数据流图形tcptrace同样是对单个TCP会话分析。

打开抓包文件，点击任意一个要分析的TCP数据帧。选择菜单统计——TCP流图形——图形序列（tcptrace）。如下图。

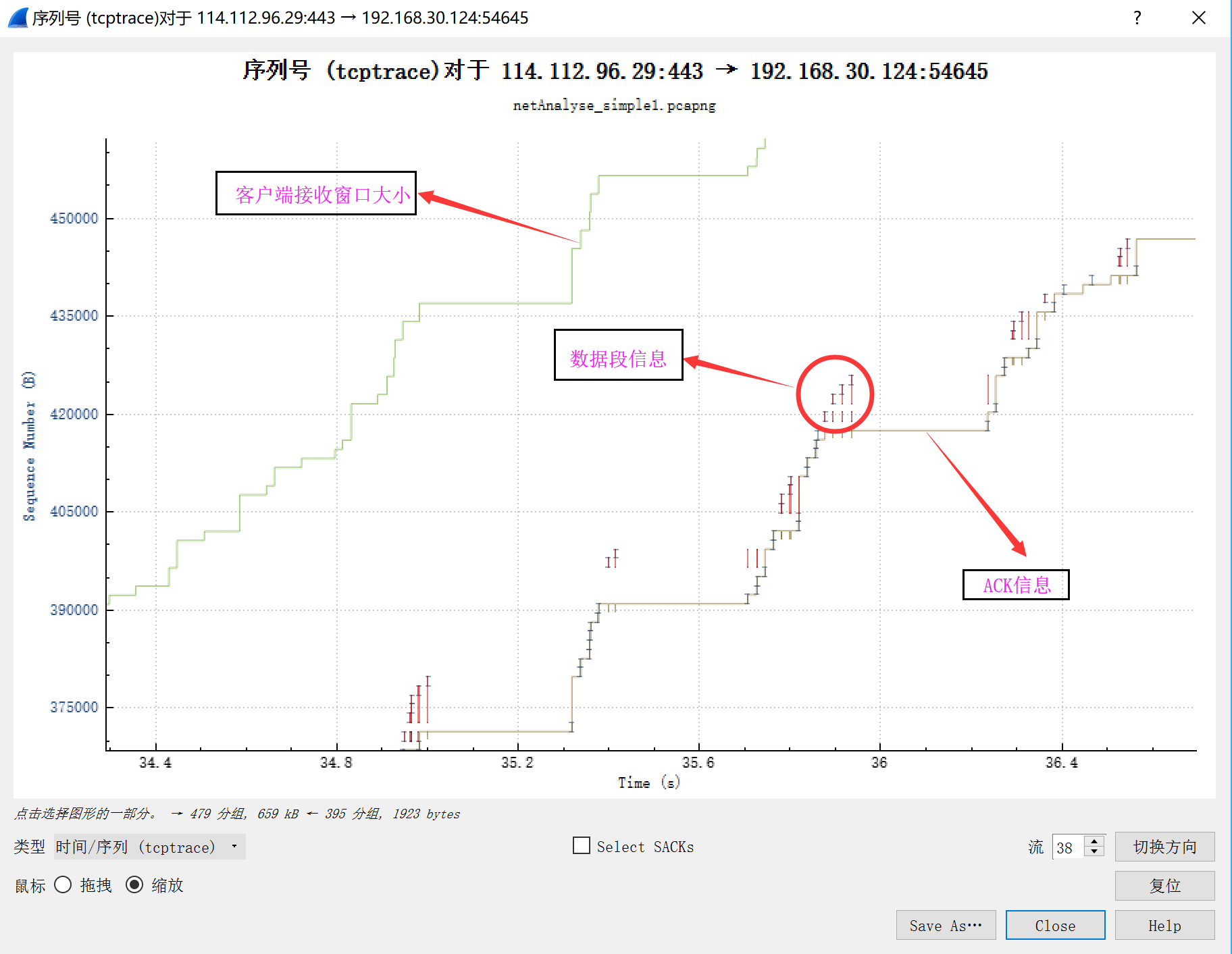


# 如何使用TCP数据流图形分析

和Stevens图形一样，该时序图的x轴表示的是时间，单位为秒，y轴表示的是TCP序列号。TCP序列号会按照每个数据包发送的字节数而递増。也就是说，如果当前序列号为1，而我们正在发送的数据大小为10字节，那么序列号也要相应地増加10。于是，下一个要发送的数据包的序列号就成了11。如果图中绘制的点的趋势比较陡，数据的吞吐量也就比较高。

一般来说，时序图的绘制点会从左下角发展到右上角。

每张时序图中会包含3条线。其中密密麻麻的那条线是TCP数据段，其中小选段越长，表示数据包中的载荷数据越多。TCP数据段下面的那条线表示的是发送数据的ACK数据流，而最上面的那条线表示的是计算出来的客户端接收窗口。



通过放大效果，数据段曲线图中有红色或深红色竖线，代表专家系统事件。关于专家系统介绍，会在今后的章节详细描述。



# TCP数据流分析技巧

使用TCP数据流图形分析，掌握以下规则，有助于更好更快的得到分析结果。

1. 所有斜线越陡越好，平坦的曲线代表传输平缓。
2. 数据段中出现的红色信息越少越好，代表专家系统中事件越少。
3. 客户端接收窗口的那条线和TCP数据段那条线之间的距离就是滑动窗口的大小，即接收方的缓冲区大小。这两条线之间的距离越近，表示可以使用的缓冲区越小，反之亦然。可以綬冲的数据越少。