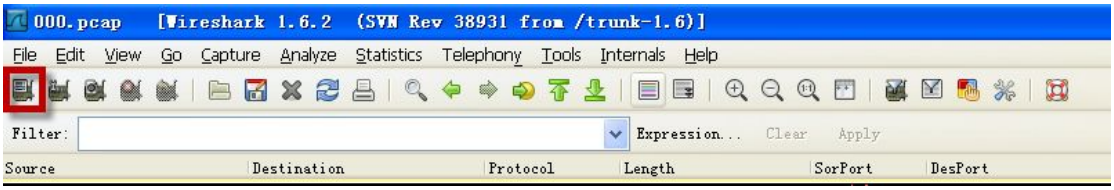
Wireshark 使用说明

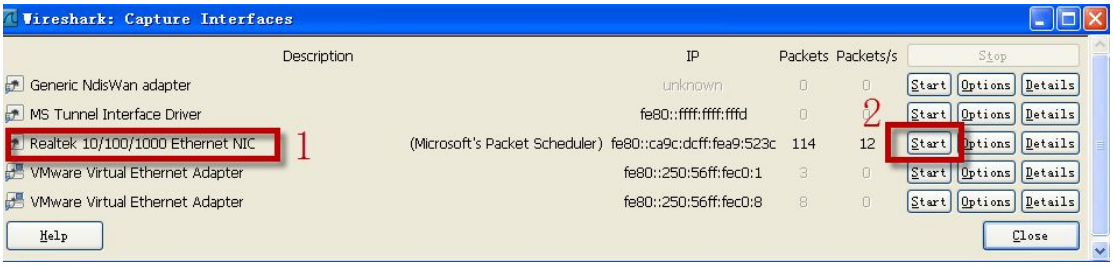
1.打开 Wireshark

2.选择主菜单中的 Capture ——> Interface

或者点击

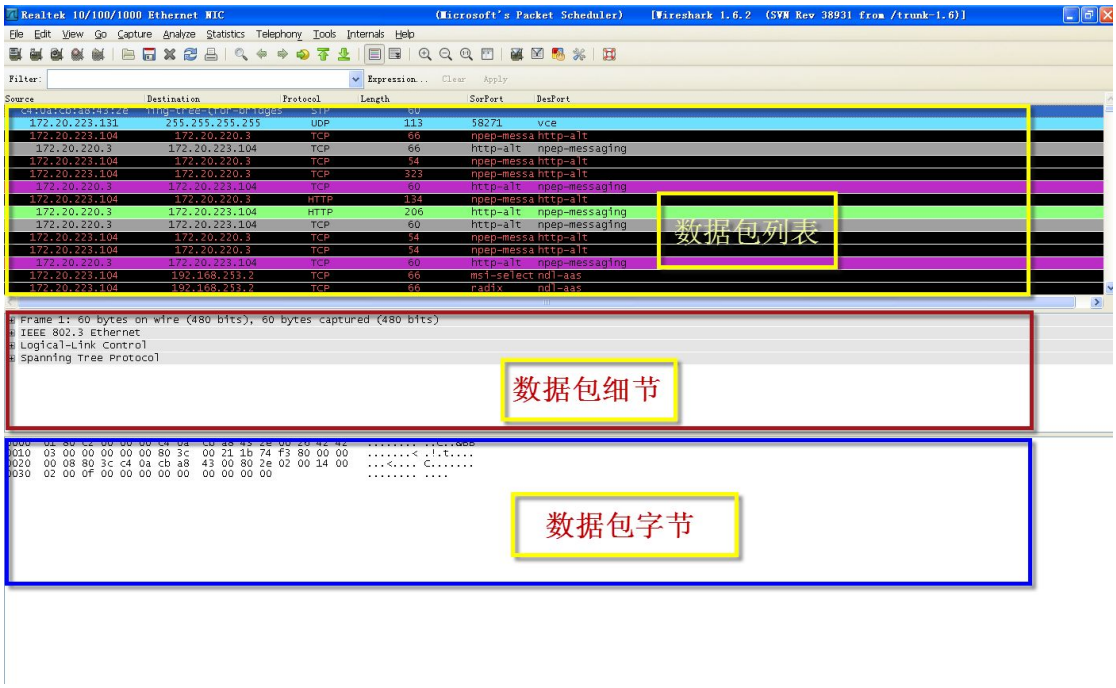


3.选择网卡



4.已经开始捕捉数据包，捕捉到需要的数据包后可以停止捕捉

Wireshark 主窗口介绍



数据包列表(Packet List)：用表格显示了当前捕获文件中的所有数据包，其中包括了数据包序号、数据包被捕获的相对时间、数据包的源地址和目标地址、数据包的协议以及在数据包中找到的概况信息等列

数据包细节（Packet Details）：用分层大的方式显示了一个数据包中的内容，并且可以通过展开或是收缩来显示这个数据包中所捕获到的全部内容

数据包字节（Packet Bytes）：显示了一个数据包未经处理的原始样子，也就是其在链路上传播时的样子

数据包颜色高亮

数据包列表中的彩色，不是随机分配给每个数据包的，这些颜色对应着数据包使用的协议，举例来说，所有的 DNS 流量都是蓝色，而 HTTP 流量都是绿色。将

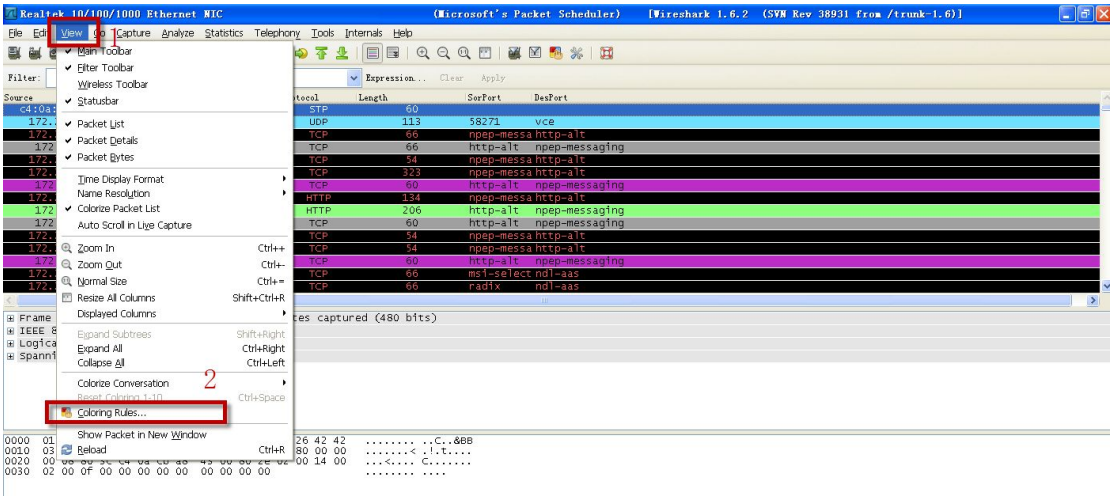
数据包进行彩色高亮，可以让我们很快地将不同协议的数据包分开，而不需要对每个数据包都查看数据包列表面板中的协议列，可以节省很多时间。

是否可以根据自己的喜好，设置不同的颜色呢？答案是肯定的！

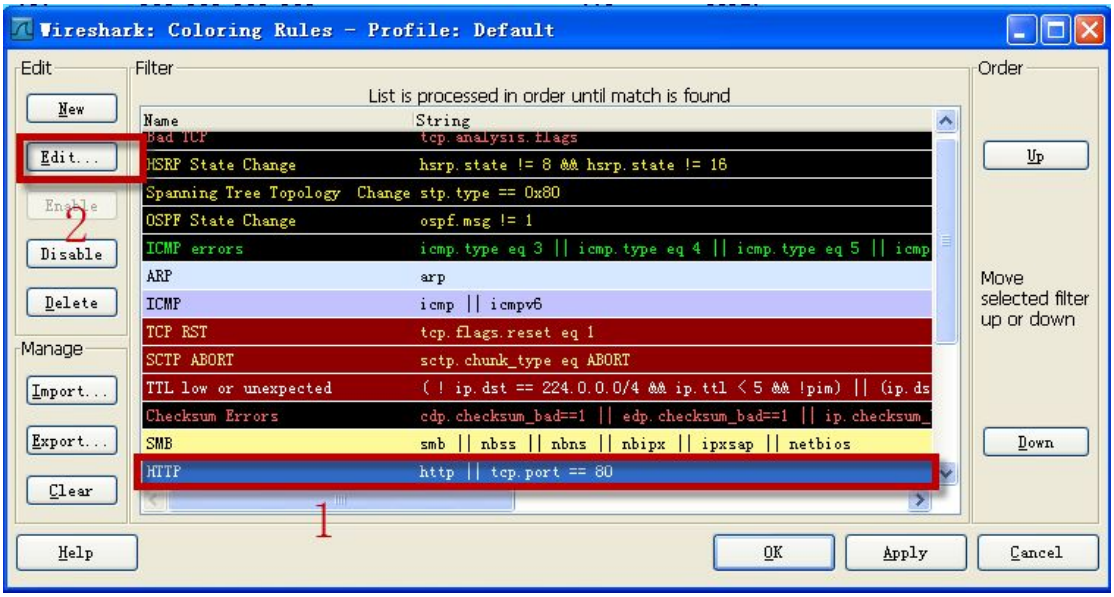
如何做？Follow me ！

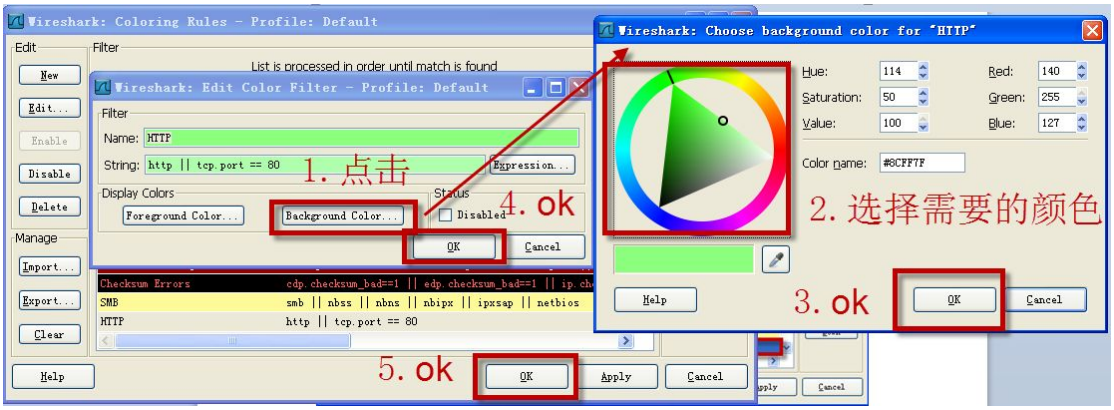
“以更改 http 协议的数据包颜色为例，将绿色更改为深紫色”

1.打开 Coloring Rules



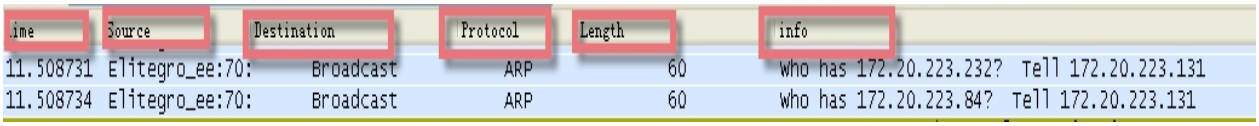
2.找到 http 协议，点击，再点击 edit



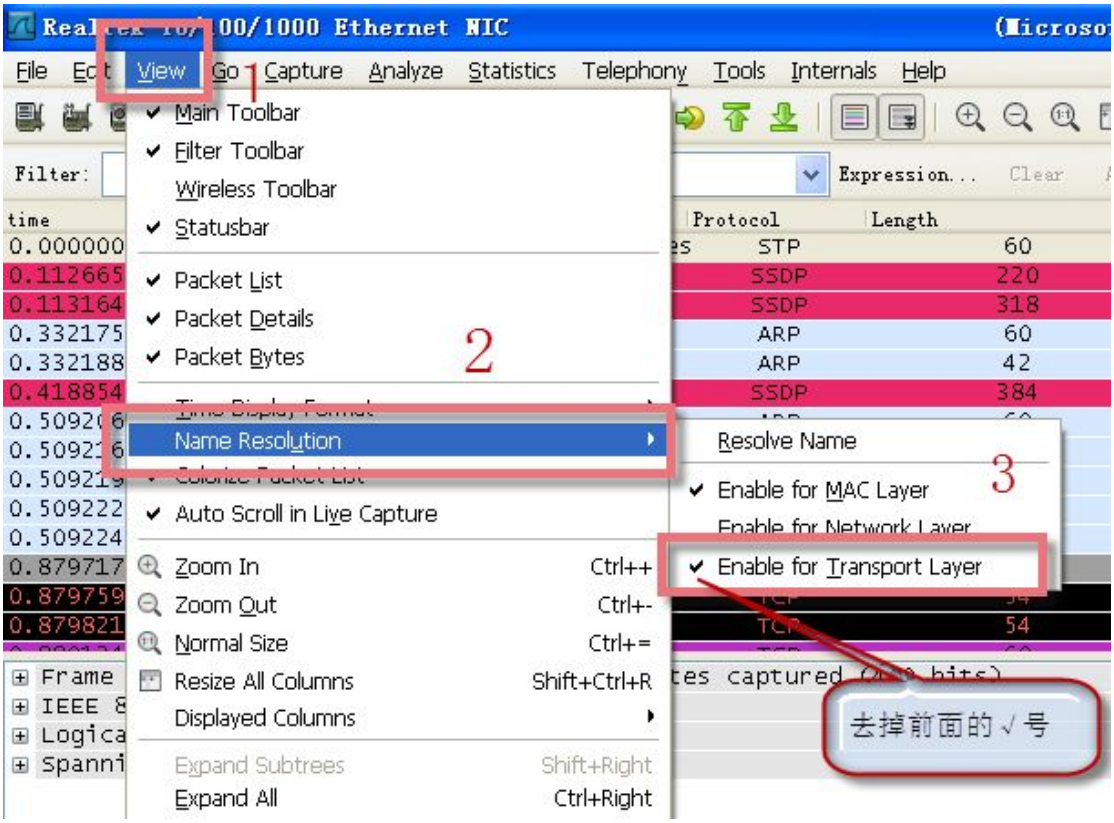


5.显示出端口号

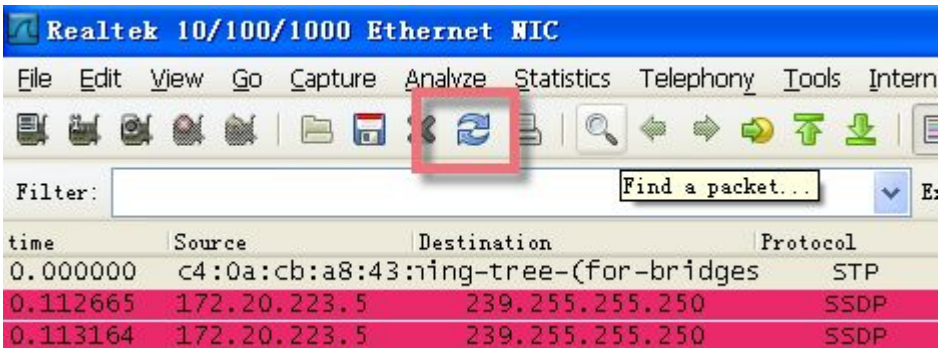
当安装好 Wireshark 后，默认会显示以下内容

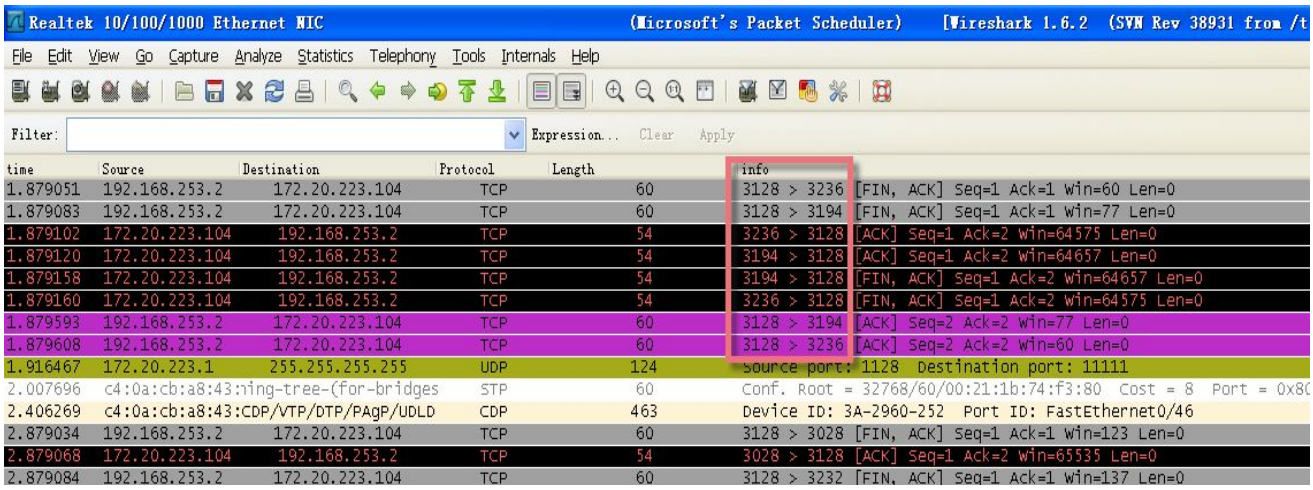


某些数据包在 info 这一栏包含了源端口号和目的端口号，但是是字符形式，我们可以将其调成习惯看的数字形式。



然后刷新一下

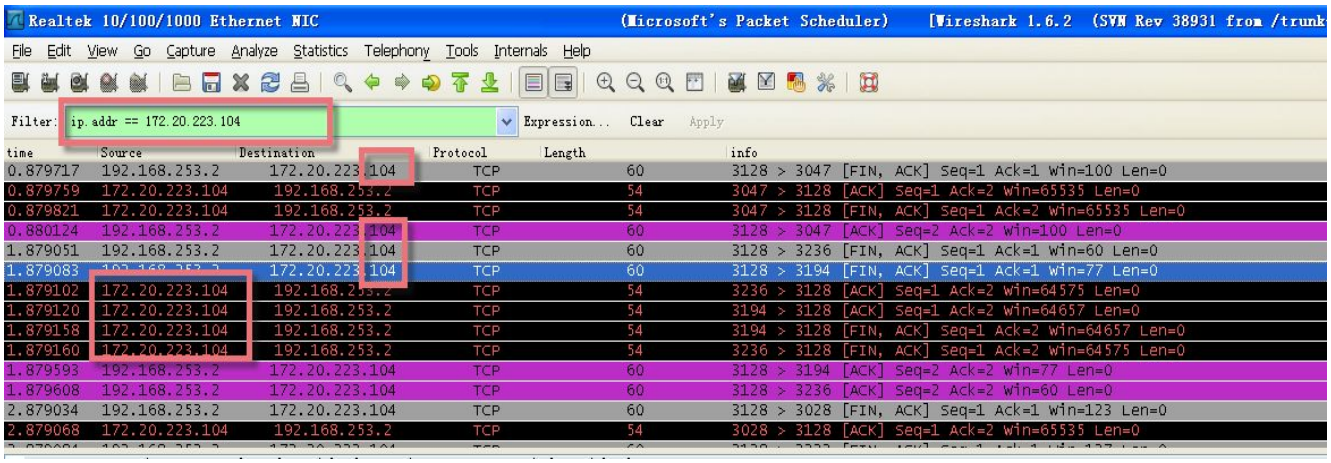


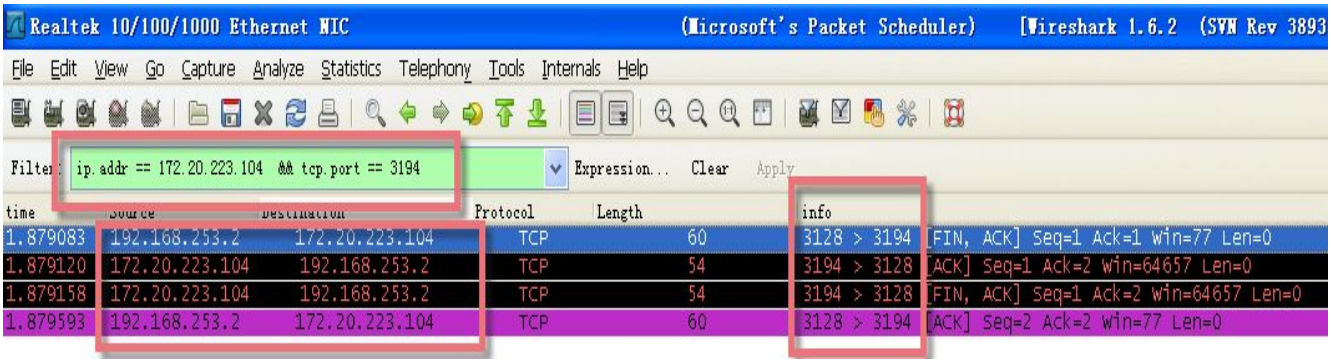


6.过滤数据包

在 Filter 这个框里 写上过滤的规则，回车即可过滤出想要的数据包

这些规则可以通过“或”\“且”\“非” 来连接，进行更详细的过滤





也可以点击 Expression 进行选择，这个过滤法则多去尝试，就能应用的更熟练，如果过滤语句不对，背景色会呈现粉红色，正确 呈现浅绿色