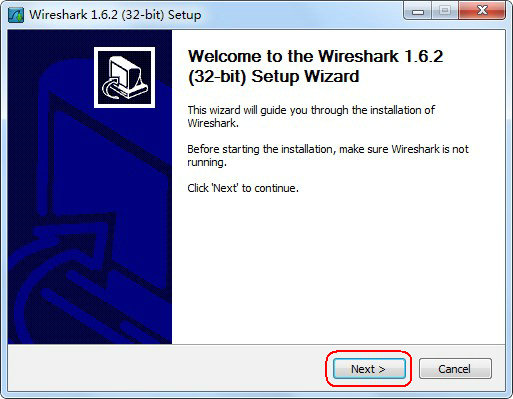
# 原文地址：https://blog.csdn.net/tennysonsky/article/details/45841591

# Wireshark环境搭建

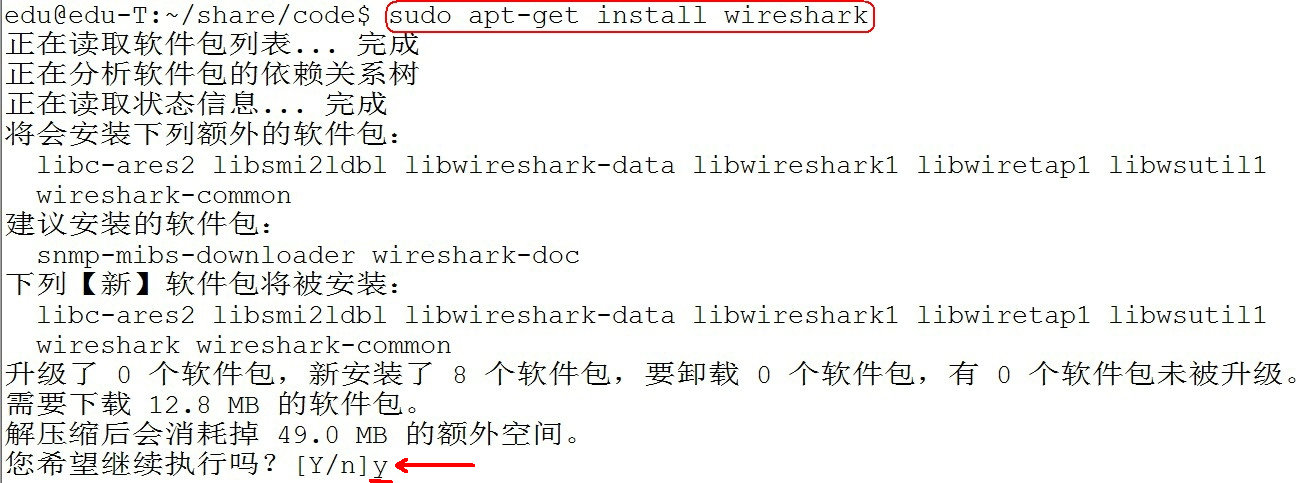
1）Windows环境

下载一个安装包，默认配置，一路 next 即可完成安装



2）ubuntu环境（这里测试环境为 ubuntu 12.04(32位)，不同版本有所差异，使用方法却差不多）

在终端敲安装命令：sudo apt-get install wireshark



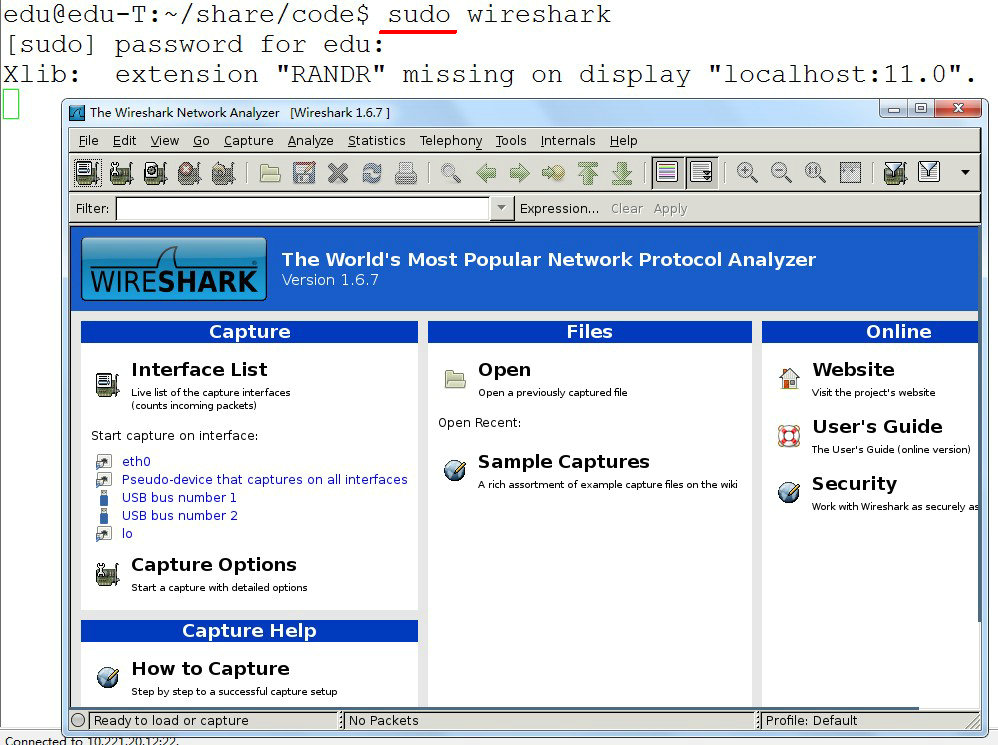
# Wireshark使用简单流程

**1）打开 Wireshark**

Windows 双击即可打开 Wireshark。

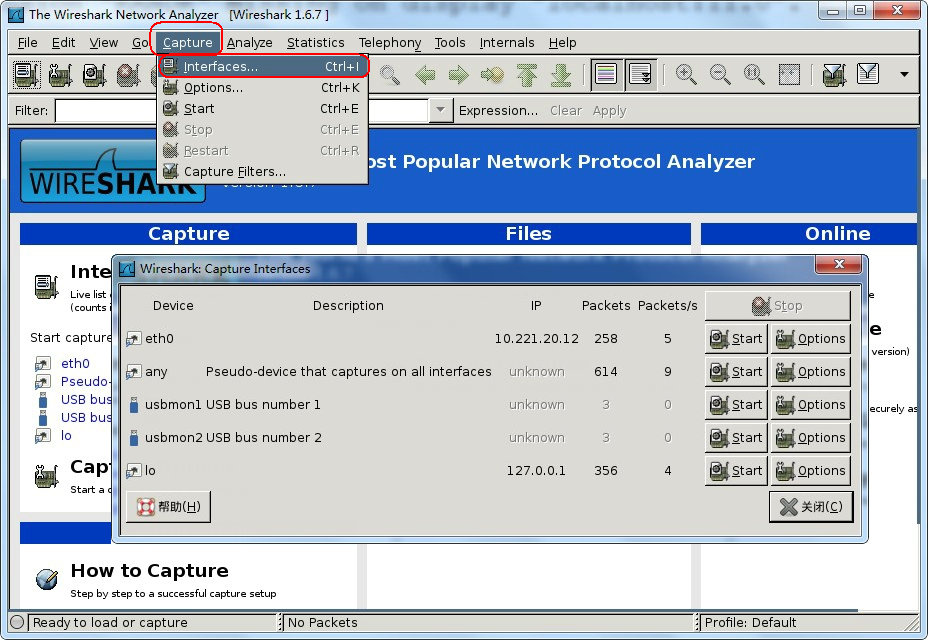
ubuntu 如何启动 wireshark ?

需要超级用户打开，在终端上敲：sudo wireshark

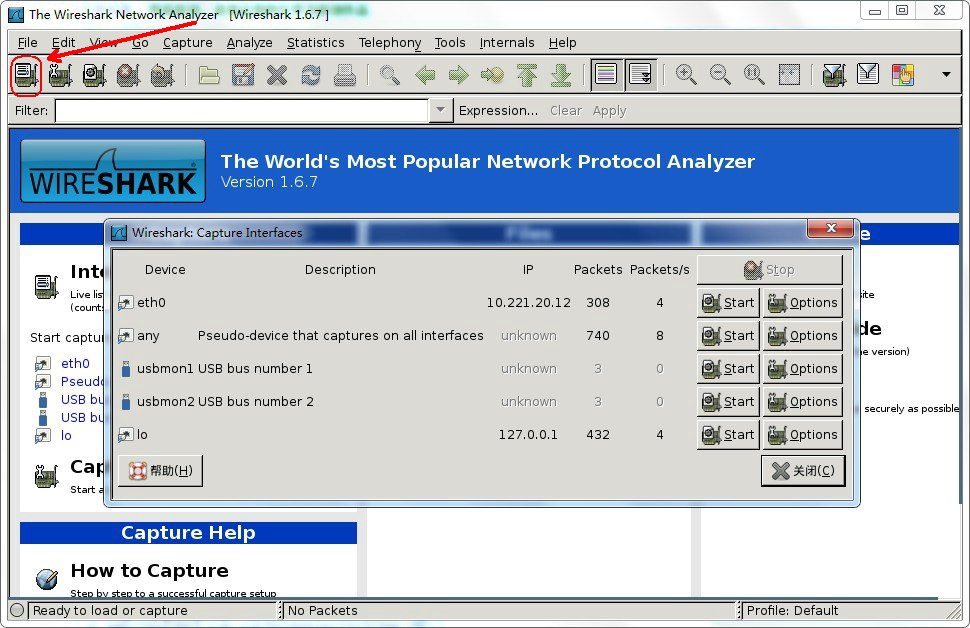


**2）如果没有接口列表，打开接口列表**

方法1：

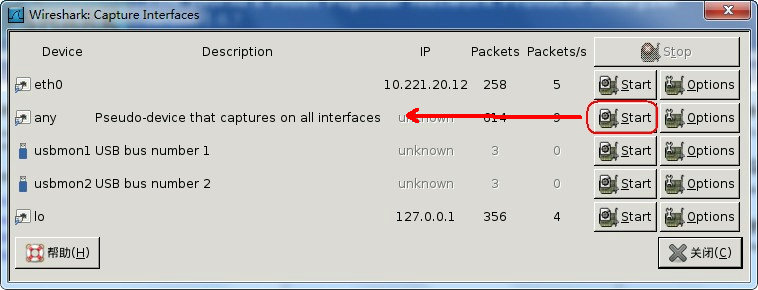


方法2：

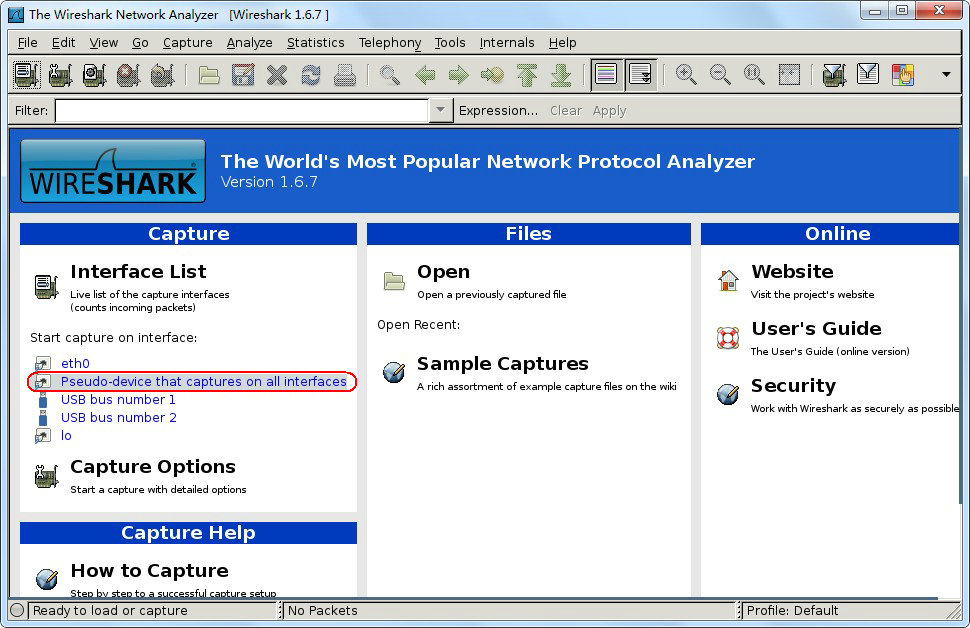


3）**选择合适网卡**，这里抓所有网卡的的数据。

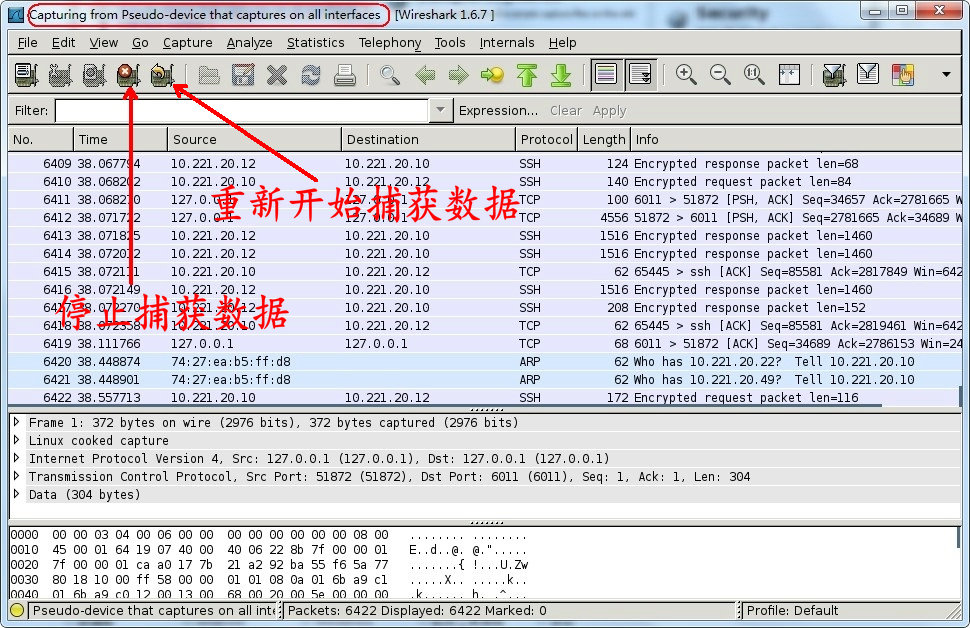
方法1：



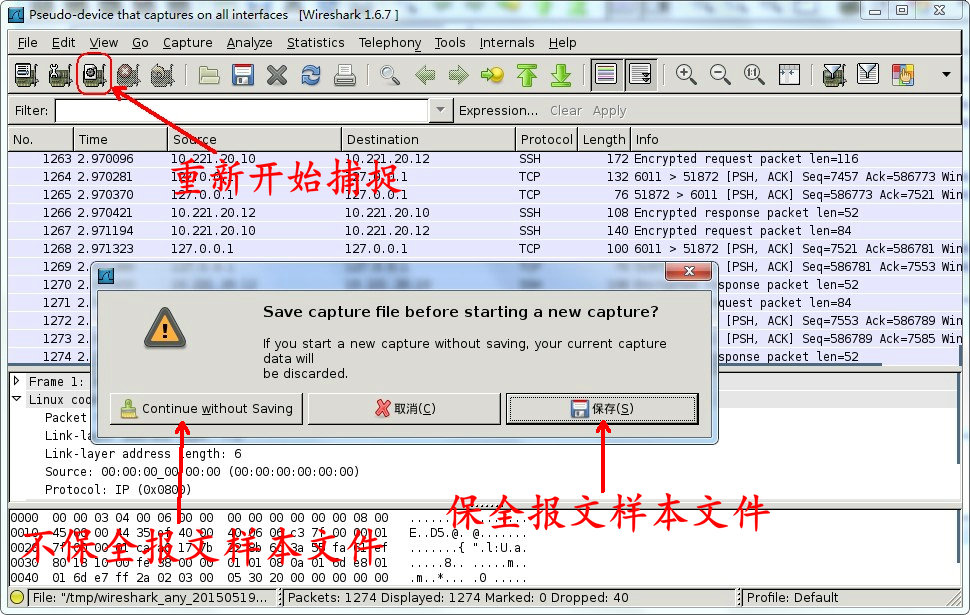
方法2：



4）已经开始捕捉数据包（ Wireshark 会捕捉系统发送和接收的每一个报文），捕捉到需要的数据包后可以停止捕捉

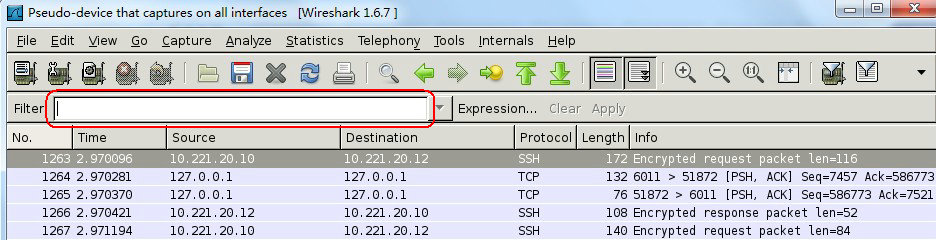


停止抓包后，如何重新开始？

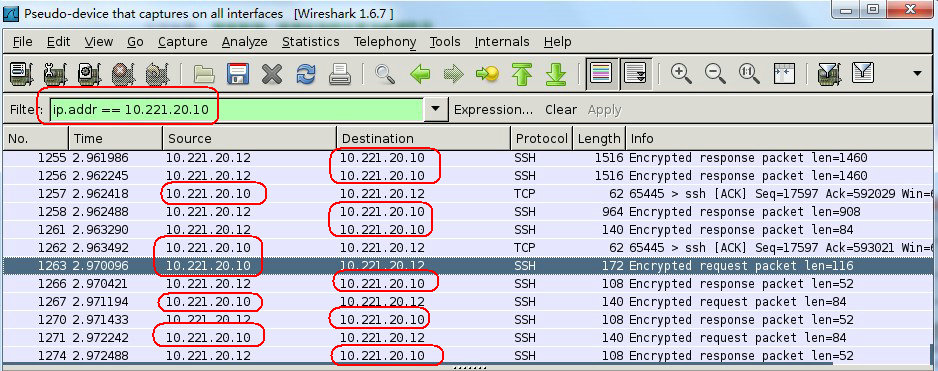


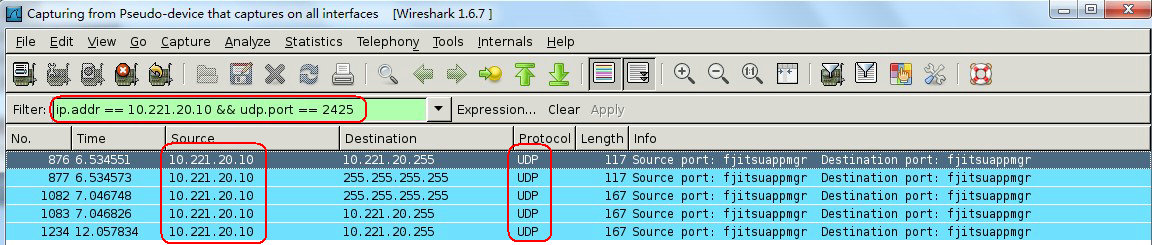
**在捕捉报文时，往往需要过滤数据包，这样可以更准确捕捉到我们所需要的报文**。

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。

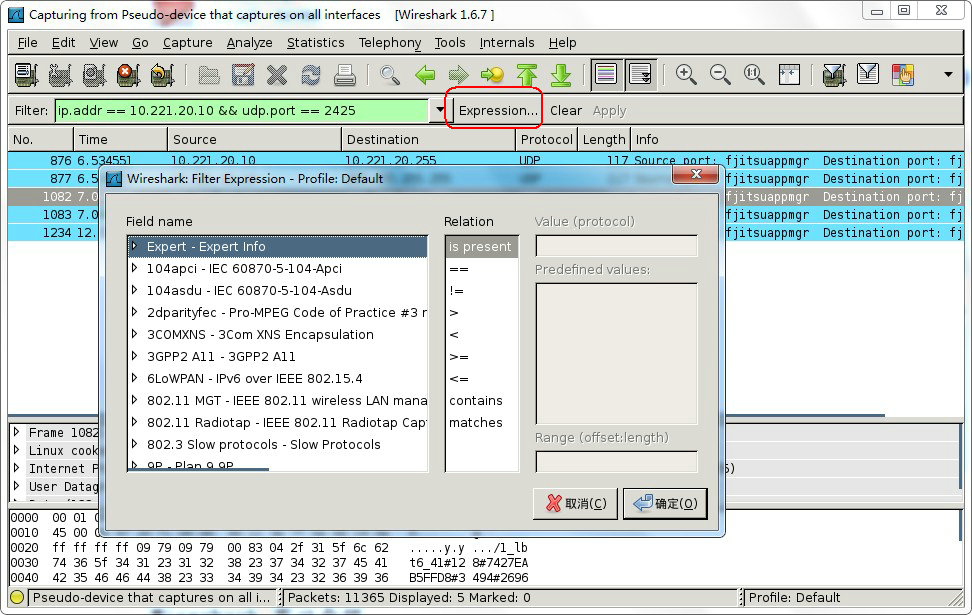


这些规则可以通过“或”、“且”、“非” 来连接，进行更详细的过滤。



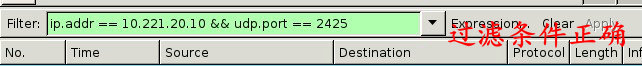


也可以点击 Expression 进行选择，这个过滤法则多去尝试，就能应用的更熟练。

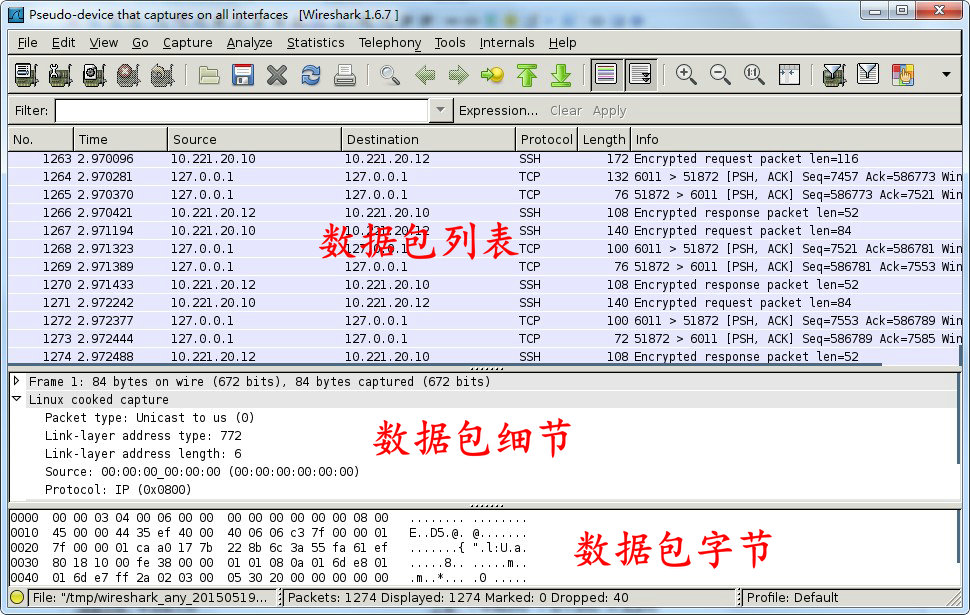


如果过滤语句不对，背景色会呈现粉红色，正确呈现浅绿色。

IMG_269



# Wireshark 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。**点击某一行可以在下面两个窗口看到更多信息。**

IMG_272  
  
**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。

