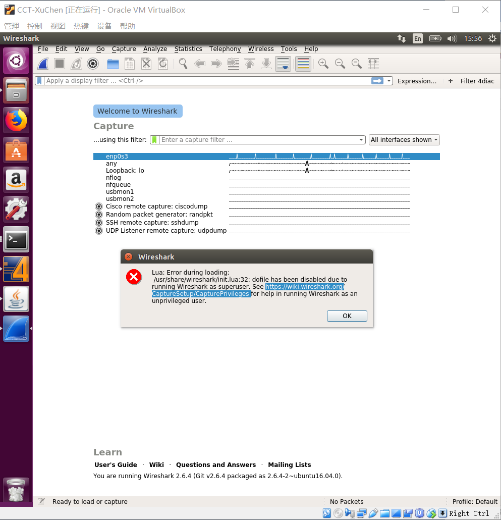
# 一、Linux下的安装

在终端执行sudo apt-get install wireshark即可。

# 二、使用过程

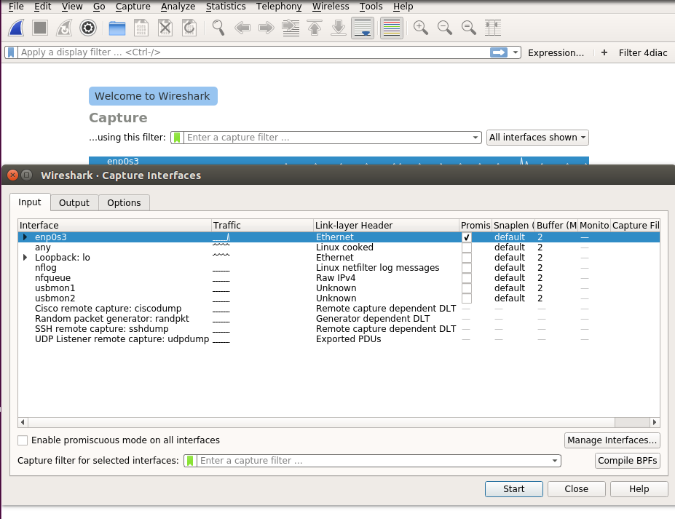
1、因为wireshark抓包需要一定的权限，所以最简单的运行方法是执行sudo wireshark，当然其他方法参考[wireshark权限设置](https://wiki.wireshark.org/CaptureSetup/CapturePrivileges)。

图：sudo wireshark执行后的界面

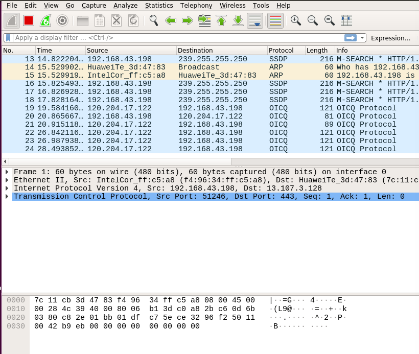


2、点击选项Capture->Options,然后选择对应的网卡点击start开始捕捉数据包。

图：网卡选择界面



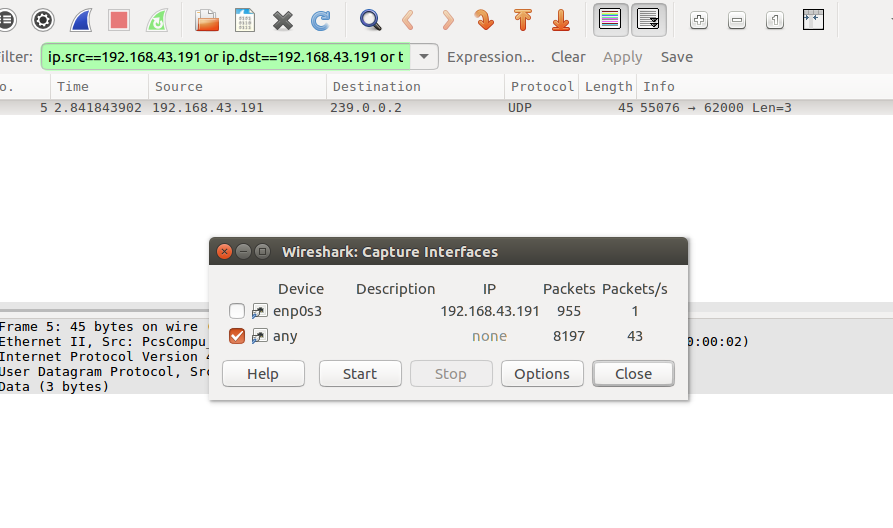
图：开始抓包的界面



3、设置条件选择

条件选择可以分为过滤规则和显示规则两种，其中过滤规则可以在开始抓包之前通过Capture->Interfaces设置。

图：过滤规则设置界面



图：显示规则设置位置



参考[过滤方法解析](https://blog.csdn.net/wojiaopanpan/article/details/69944970)。常见的几种条件：

ip.src==192.168.43.191 or ip.dst==192.168.43.191 or tcp.port==62001 or tcp.port==62000 or tcp.port==64004

图：设置过滤条件后捕捉到的包

