<https://jingyan.baidu.com/article/455a9950552d97a16627782f.html>

在Windows下我们一般抓包使用fiddler比较多一点。

但最近用Linux的次数比较多一点儿，fiddler软件并没有Linux的版本。

wireshark是一款Linux下的图形化抓包工具，其最大的好处就是直接是图形化的客户端不用繁琐的去输入命令，非常的方便。

方法/步骤

1. 使用命令

**sudo apt-get install wireshark**

来安装我们最新的wireshark软件版本

sudo是获取root权限，其输入密码并不会显示出来，输入完直接回车就好了。

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=1)

1. 待程序下载完成后进入安装界面是这样的。

用tab键选中“确定”按钮，回车确定

才可以继续安装

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=2)

1. 是否运行非root用户进行抓包

这里我选择的是

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=3)

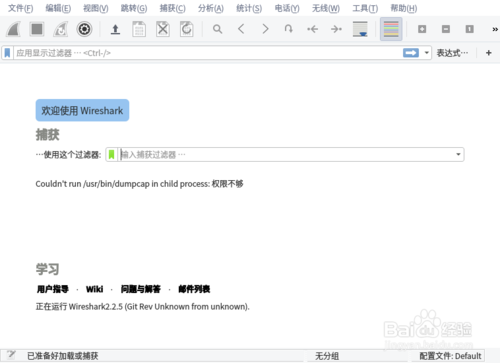
1. 安装完成后可以看到软件的启动图标

双击就可以直接启动了

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=4)

1. 如果出现下面这种提示，则代表权限不够。

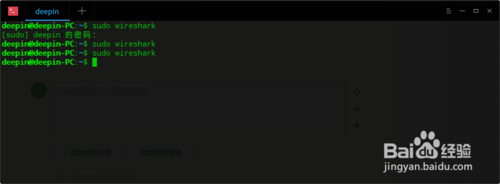
我们需要在root权限下去执行这个软件

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=5)

1. 打开终端我们输入以下命令

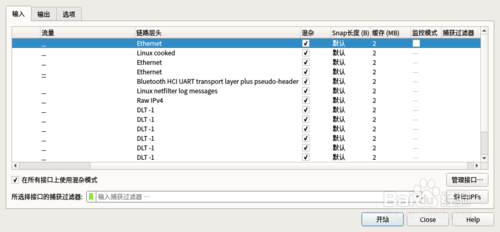
sudo wireshark

使程序运行在root权限下

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=6)

1. 这时启动程序已经正常了，我们选择自己需要捕获的设备

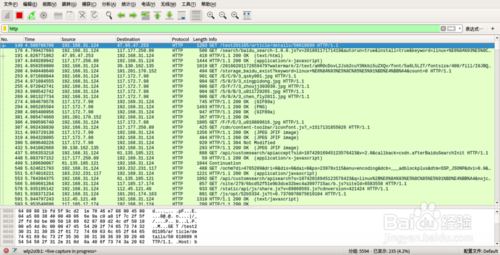
也可以全选即混合模式，然后利用过滤来得到自己需要的东西

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=7)

1. 这里我设置的是http过滤

只进行http信息的捕获

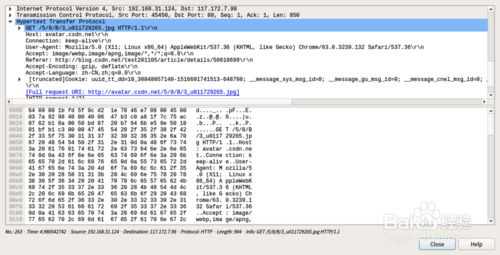
下面的内容为浏览器进行访问web网页的信息

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=8)

1. 9

双击某条信息，即可以查看详细信息。

这里查看详细的get或post内容主机等信息

[](http://jingyan.baidu.com/album/455a9950552d97a16627782f.html?picindex=9)