完全公开/内部公开/秘密/机密/绝密

手机抓包探究



南京奥闪迪信息技术有限公司

Nanjing oooo3d Information Technology Co., Ltd.

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **修订版本** | **修改描述** | **作者** |
| 2013-4-3 |  |  | LUNA |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目 录

1.1 笔记本做为热点，手机直接连接笔记本抓包 1

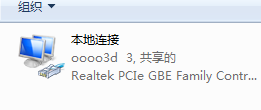
1.2 ANDROID手机安装抓包软件直接抓取 3

1.3 用TCPDUMP命令直接抓包方法 4

## 笔记本做为热点，手机直接连接笔记本抓包

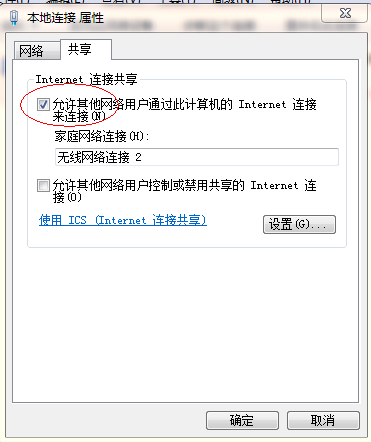
1. 将网线插入到笔记本的网口
2. 设置连接的网口如下：

在[控制面板\网络和 Internet\网络连接]下配置本地网络，为DHCP自动获取



注：此时需要将本地连接共享，共享如下：

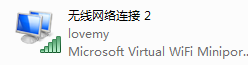
右击[属性]---[共享]—选择[允许其它网络用户共享此连接]



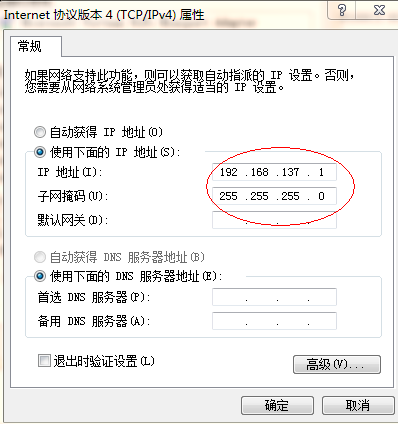
1. 保证WIFI开关为打开状态
2. 打开青青草原WIFI热点工具：



在[控制面板\网络和 Internet\网络连接]中，新增一个无线连接2



此处不能采用DHCP自动获取，需要自己配置静态IP地址，注意与本地联接不能在同网段：



1. 打开手机，在WLAN中找到LOVEMY，刚才在青青草原软件中设置的无线接入点，自动获取IP。

好了，在手机上试下，可以上网了。

1. 在PC上安装WIRESHARK等抓包工具：

打开手机应用APP，可以抓到应用APP上所有与互联网交互的包了。



## ANDROID手机安装抓包软件直接抓取

1. 直接安装androidmobiletcpdump.apk软件
2. 运行该软件



1. 填写抓包后的文件名称：

存储路径在mnt/sdcard/XXX.PCAP

点击[启动悬浮窗]



1. 可以看到在屏幕中间启动一个悬浮按钮，在打开所要测试的APP前，开启此按钮
2. 可以根据用户随意关闭抓包



此时，在mnt/sdcard/路径中可以看到XXX.PCAP文件，将文件拷贝出来后，用PC的WIRESHARK抓包就可以开始分析了。

## 用TCPDUMP命令直接抓包方法

前提：1）需要提前开放手机的ROOT权限

2）电脑需要安装ANDROID开发环境（具体安装方法见《ANDROID开发环境搭建》）

1. 在开发环境上，直接用CMD连接到SDK上，并且输入/data/local/

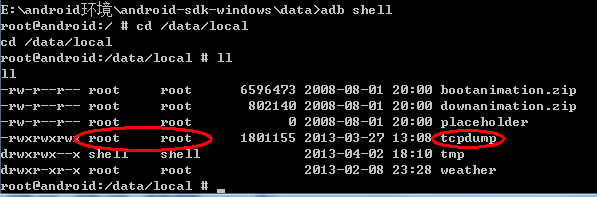


1. 输入adb shell  
   进入到asb shell模式下





1. 直接进入到/data/local/里面可以看到tcpdump文件，如果没有的可以从网上下载，并且赋于root操作权限



1. 执行如下命令：



1. 按着CRTL+C可以退出抓包模式
2. 用91手机助手或豌豆荚直接连接手机，找到capture1.pcap

在电脑上直接用wireshark抓包就可以看到了。

