**Android下通过tcpdump进行抓包**

**准备工作**

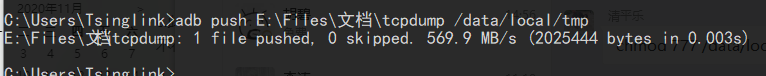
1. **设备要有Root权限.参考<<26A1设备获取Root步骤>>里面如何获取 ROOT 权限.**
2. **准备好tcpdump文件（见末尾附件）**

**抓包步骤**

1. **将tcpdump文件复制到设备/data/local/tmp目录下**

此步骤一般只需要执行一次，如果之后设备不格式化的话这个文件还会存在，就不需要再复制了

* 1. 打开cmd窗口，运行命令 adb push tcpdump /data/local/tmp

注意：tcpdump 处要换成这个文件在你电脑上的完整路径，如截图所示（有些电脑或者系统的adb可能不支持中文路径，要把文件放在英文目录下）

* 1. 修改文件的权限

运行命令 adb shell chmod 777 /data/local/tmp/tcpdump

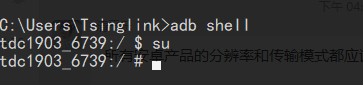


1. **抓包并导出抓包文件**
   1. 打开cmd窗口
   2. 运行命令 adb shell
   3. 运行命令 su （此时设备会出现Shell申请root权限的弹窗，点击允许，允许后下次执行就不会再次弹窗了）



申请权限成功后cmd窗口命令行的 $ 符号会变成 # 号，表示已经成功获取到root权限

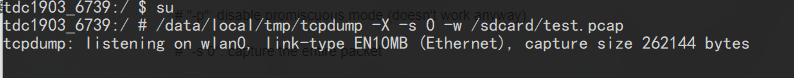
 →



* 1. 执行抓包程序,并将抓包文件存到设备的/sdcard目录下面

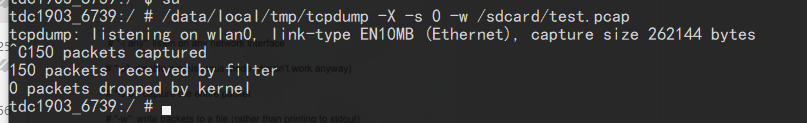
运行命令 /data/local/tmp/tcpdump -X -s 0 -w /sdcard/test.pcap

注：命令最后一部分test.pcap，其中的“test” 是抓包生存的文件名称，可以根据需求自己重命名区分



此时设备已经开始抓包，不要关闭cmd窗口

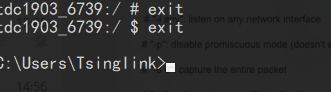
* 1. 操作设备，进行相关测试
  2. 操作结束之后，在cmd窗口按 Ctrl+C 来结束抓包



* 1. 导出抓包文件

先退出adb shell su模式，进入普通命令行模式

（可以直接关闭cmd窗口再重新运行cmd或者先执行exit 退出 su，再执行exit 退出adb shell，进入普通命令行模式）



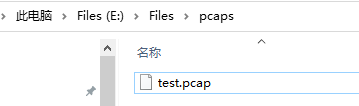
导出抓包文件

运行命令 adb pull /sdcard/test.pcap E:\Files\pcaps

（后面的路径改成想要导出到的目的文件夹路径）



抓包文件成功导出



f) 通过 wireshark 等第三方软件来分析抓包结果,参考网上有关wireshark 的使用说明.

**附件**

tcpdump文件：

