# APP抓包方案总览

## 正常设置WLAN代理抓包

操作：高级选项中修改代理设置

问题：当开启拦截的时候，抓包工具无记录。APP可正常使用。APP不走代理。

解决：使用模拟器抓包或强制代理方式。强制代理方式本文不涉及。

## 模拟器抓包

操作：使用模拟器，使用Proxifier将整个模拟器流量抓包。

问题1：乱码。

解决：安装并信任证书。

问题2：无法抓包，显示网络连接断开。

原因1：协议问题，非正常协议。quic 或者 spdy。本文不涉及。

原因2：ssl-pinning验证。

解决：使用hook拦截验证。Xposed方案或frida方案。

## 重新打包

<https://github.com/levyitay/AddSecurityExceptionAndroid>

使用脚本将APK重新打包，实现抓包。不知道怎么用

## 非root下

### 将APP重新打包使用frida

### 太极:

<https://taichi.cool/zh/download.html>

### VirtualXposed

<https://github.com/android-hacker/VirtualXposed>

## Root下

### Xposed

使用模拟器，安装翻墙工具，安装xposed。

翻墙工具：<https://github.com/2dust/v2rayNG>

JustTrustMe++ ：<https://github.com/JunGe-Y/JustTrustMePP>

动态寻找hook点，解决混淆问题

JustTrustMe：<https://github.com/Fuzion24/JustTrustMe>

固定hook类名，APP混淆后失效

SSLUnpinning ：<https://github.com/ac-pm/SSLUnpinning_Xposed>

不知道效果。

<https://github.com/ac-pm/Inspeckage>

很强大，看项目readme

TrustMeAlready ：<https://github.com/ViRb3/TrustMeAlready>

据说很强大

其他工具集见

https://github.com/scopion/xposed-ssl-pinning

<https://github.com/JerryChenn07/AndroidReverseTool>

### EdXposed

<https://github.com/ElderDrivers/EdXposed> （Xposed升级版，支持安卓9）

需要安装Magisk，需要刷机

### Frdia

#### 安装

<https://pypi.org/project/frida/#files> 支持环境如列表所示。

不支持Python3.7 环境

Pip install wheel

pip install frida

pip install frida-tools

注意观察frida版本。

查看模拟器架构

adb shell getprop ro.product.cpu.abi

根据cpu架构及版本去下载相应 <https://github.com/frida/frida/releases>

frida-server-15.1.3-android-x86.xz

解压得到 frida-server-15.1.3-android-x86，移动到 adb 目录下

将文件推送到手机目录，放到/data/local/tmp/下，此目录目录权限比较方便

adb push frida-server-15.1.3-android-x86 /data/local/tmp/

进入模拟器

adb shell

切换到root权限

Su

赋予server权限

Cd /data/local/tmp

chmod 777 frida-server-15.1.3-android-x86

#### 启动服务

先关闭防火墙

setenforce 0

启动服务

./frida-server-15.1.3-android-x86

开启端口转发

adb forward tcp:27042 tcp:27042

查看模拟器进程

frida-ps -U

#### 开始调试

先进入目标包看能否连接

frida -U com.baidu.ipc

Exit 推出

#### 抓包示例

参考文章

<https://bbs.pediy.com/thread-222427.htm>

脚本地址

<https://github.com/scopion/frida-ssl-pinning>

注意文章中 cf = CertificateFactory.getInstance("X.509");

少了var声明，脚本中已修复。

导入证书

adb push cert.crt /data/local/tmp/cert.crt

开始抓包

frida -U -f com.baidu.ai -l .\frida-android-repinning\_sa1.js --no-pause

## 以下为历史不可用项目

Cydia Substrate

<http://www.cydiasubstrate.com/> 只支持安卓5以前，5.0不支持。

https://github.com/iSECPartners/Android-SSL-TrustKiller