# 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。

## 非root下

太极:

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

VirtualXposed

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

## Root下

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

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

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

## 需要刷机

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

需要安装Magisk，需要刷机

## 重新打包

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

使用脚本将APK重新打包，实现抓包

## Frdia

<https://github.com/CreditTone/hooker>

<https://bbs.pediy.com/thread-267387.htm>

上边两个是一起的

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

<https://github.com/WooyunDota/DroidSSLUnpinning>

逆向，寻找证书

https://blog.csdn.net/weixin\_44032232/article/details/111478298

## 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