免 root 脱腾讯御安全加固

相信大家在遇到需要破解软件时都遇到过软件被加固的情况, 但是被加固了, 不代表无法继续逆向了, 我们可以选择脱壳操作, 做到继续逆向工程的操作现在也有一些比较主流的脱壳 ... 免 root 脱腾讯御安全加固 , 吾.....

一只码农

相信大家在遇到需要

破解

软件时都遇到过软件被加固的情况,

但是被加固了, 不代表无法继续逆向了, 我们可以选择

脱壳

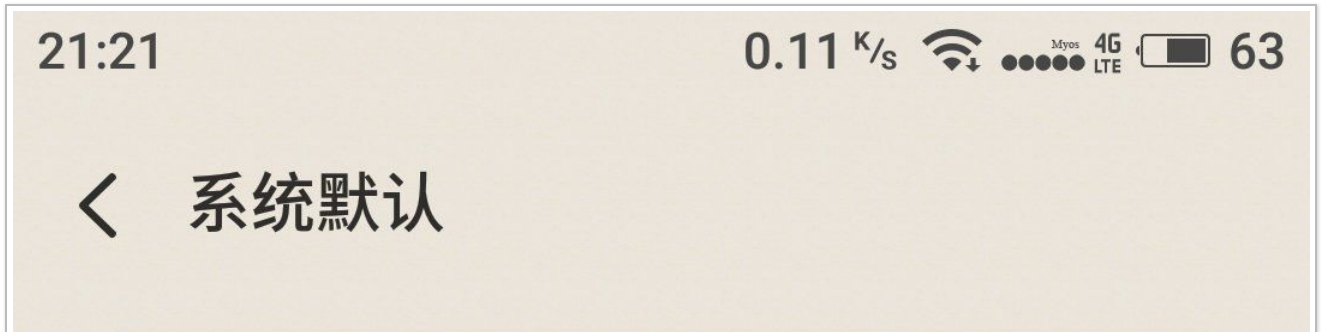
操作, 做到继续逆向工程的操作

现在也有一些比较主流的脱壳工具, 例如: 反射大师、Fdex2 等等这些都是比较优秀的脱壳工具, 但是他们都需要 root 和 XP 框架, 对于一些蓝绿厂的手机特别不友好

有人说可以用 VMOS, 但是现在的 VMOS 开启 root 和 xp 框架需要看广告, 贼烦

所以, 今天我来说一些不用 root 和 xp 框架脱壳, 但是相对的也不是特别完美

另外, 之前的帖子有人给我反馈说我手机字体有点花里胡哨, 所以本次教程我用系统默认字体




Flyme
极致源于梦想
因梦想而立，为极致而生
Flyme，born for dream，dedication
to perfection.

系统默认

好了, 废话不多说, 开始进入正题:

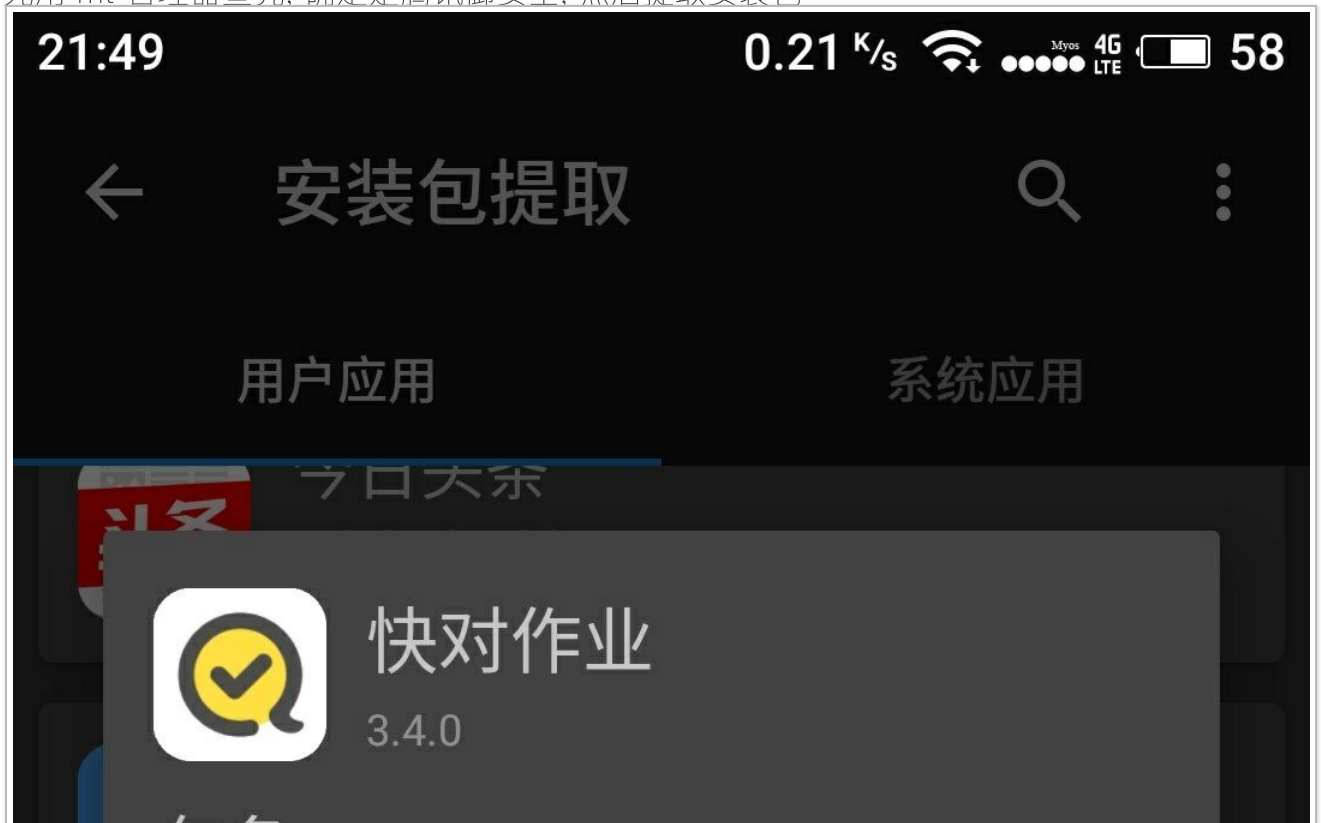
准备工具:

1、被腾讯御安全加固过的应用 (我这里以快对作业为例)

2、Arm Pro(因为作者不允许挂链接, 所以自己问度娘)

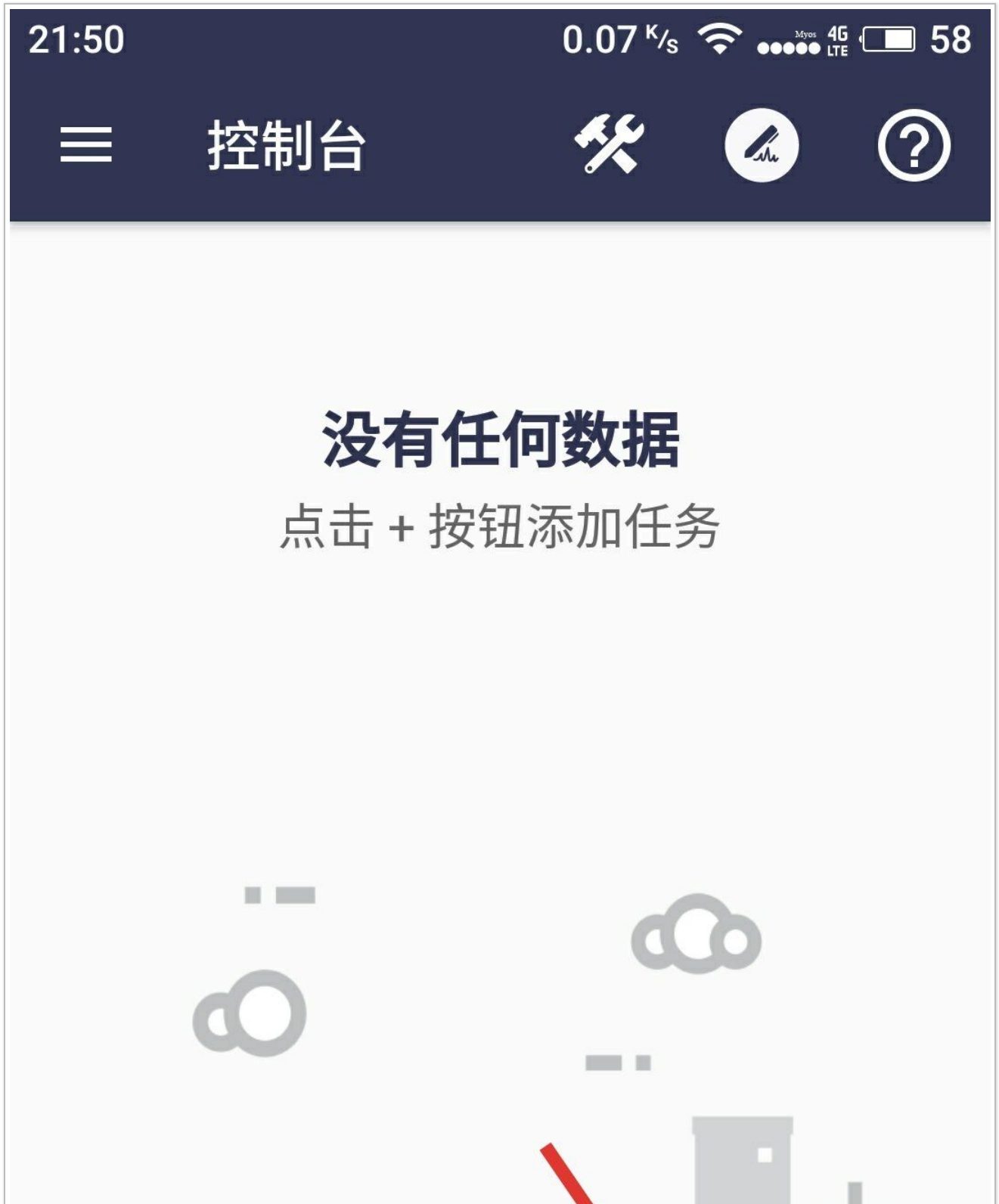
3、mt 管理器 (自备, 没有在问)

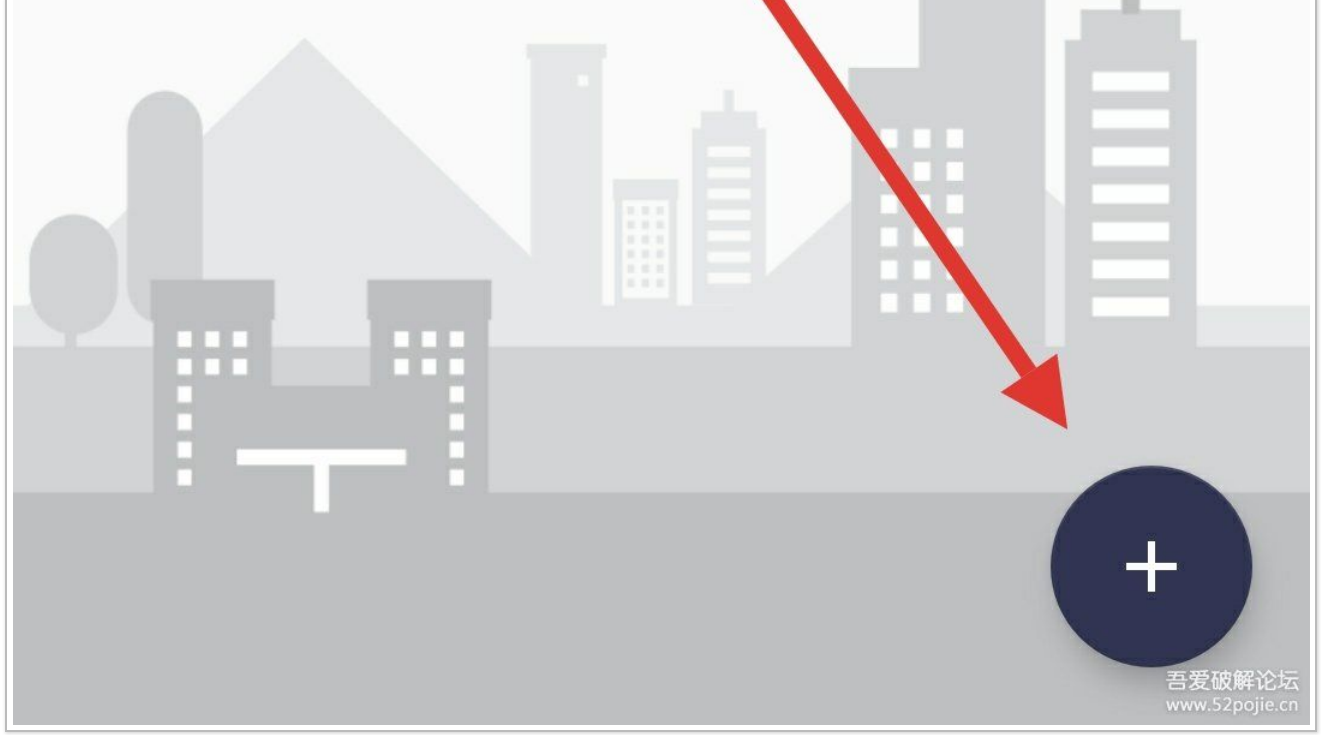
#1 首先用 mt 管理器查壳, 确定是腾讯御安全, 然后提取安装包

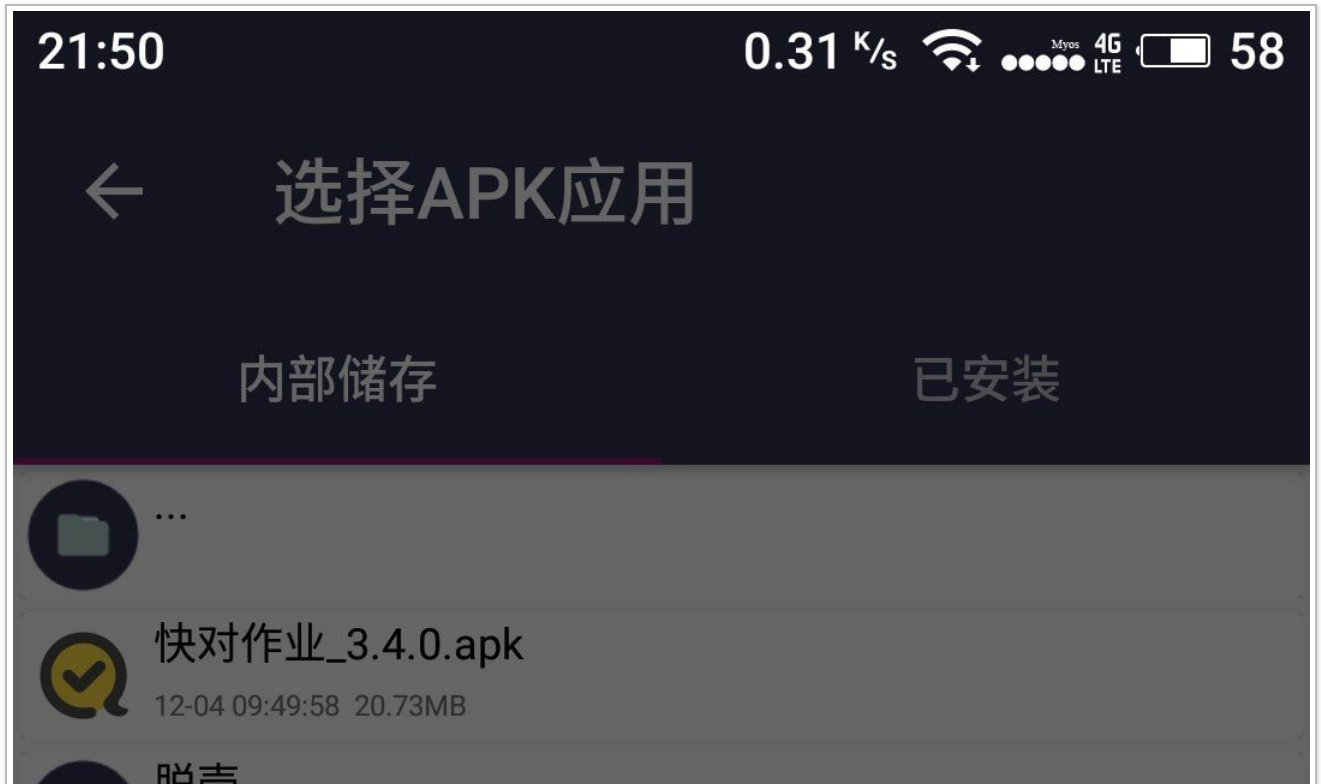


#2 打开 app.zip 选择脱壳软件（如果你没有修改 zip 管理器默认 apk 提取位置就在 MT2/Apks 里面）

#2 打开 arm pro, 选择脱壳软件 (如果你没有修改 mt 管理器默认 apk 提取位置就在 MT2/Apks 里面)

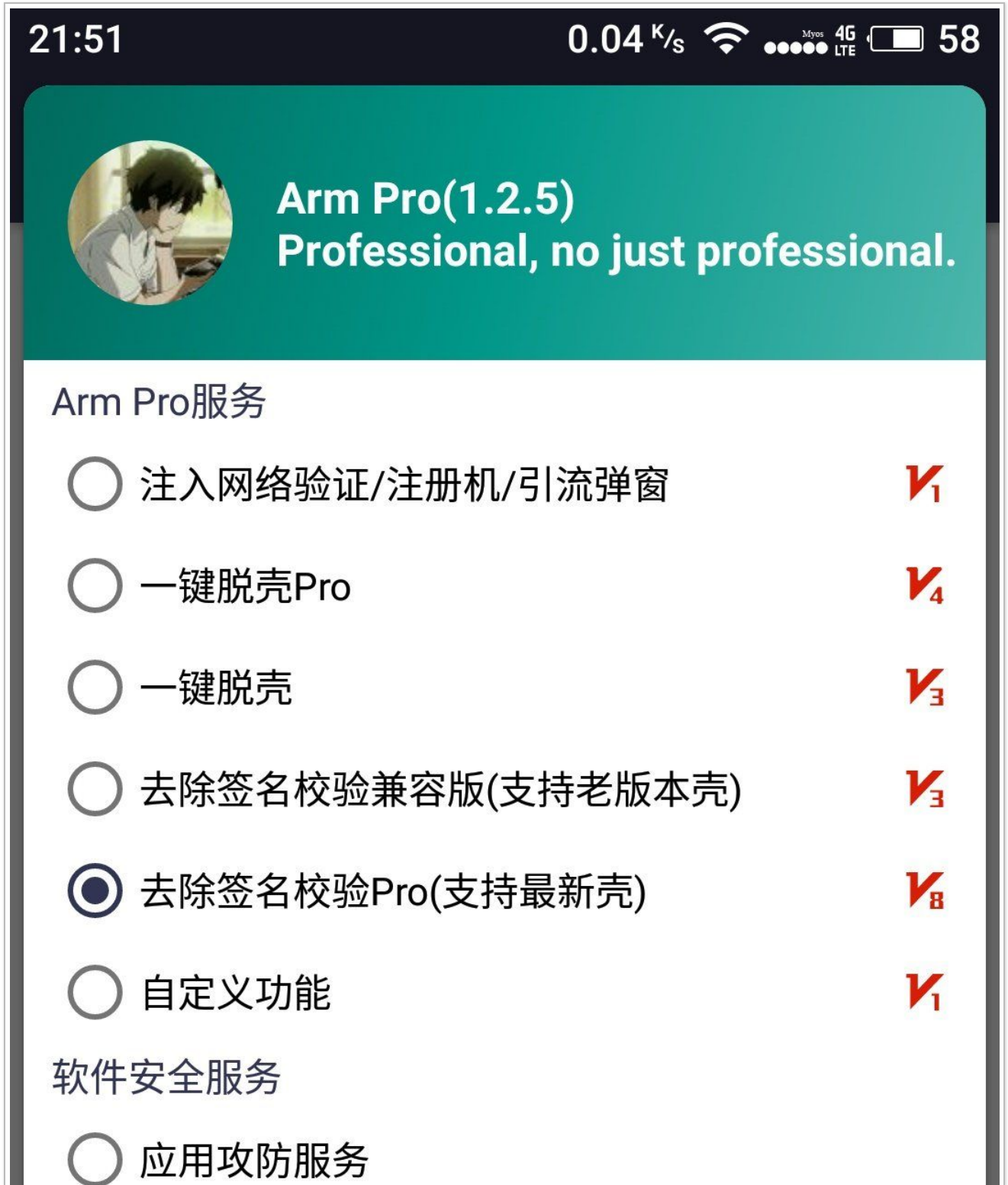


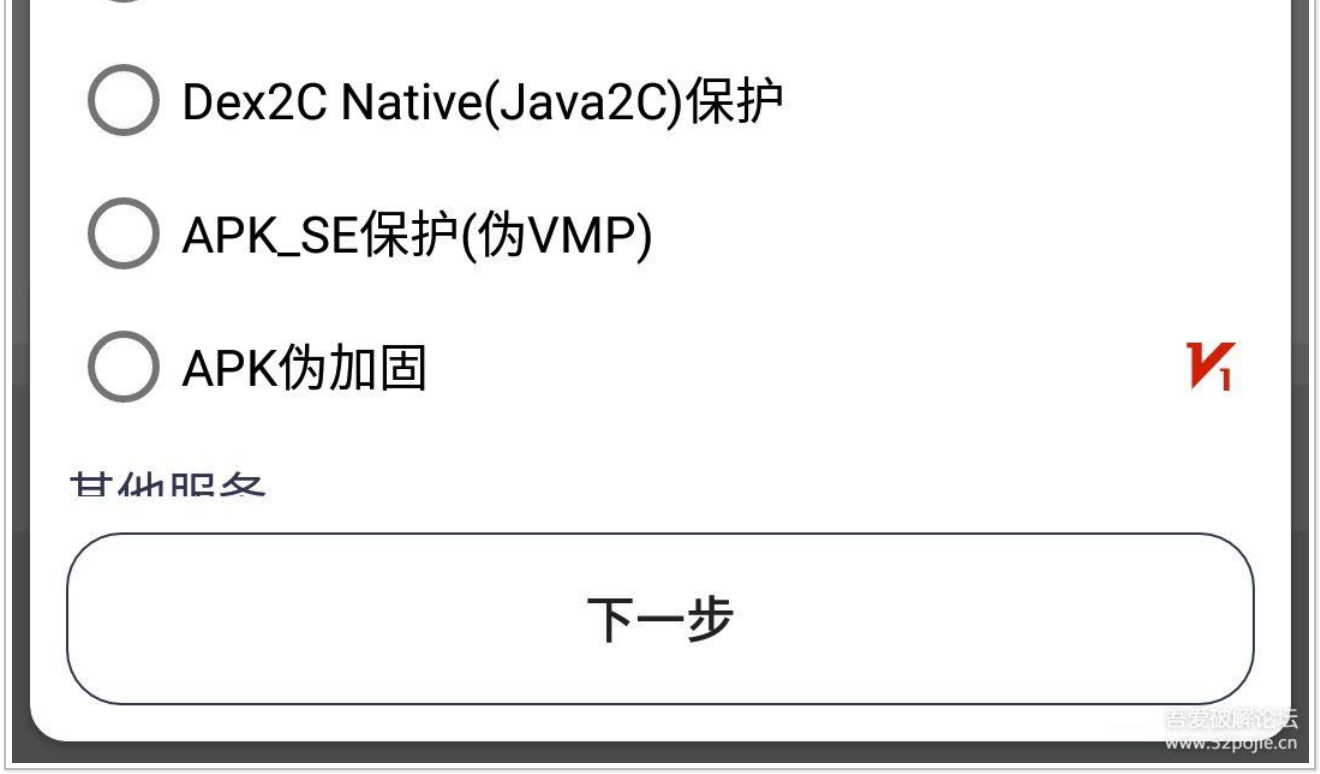

吾爱破解论坛
www.52pojie.cn


21:50
0.31 K/s
58
选择APK应用
内部储存
已安装
...
快对作业_3.4.0.apk
12-04 09:49:58 20.73MB

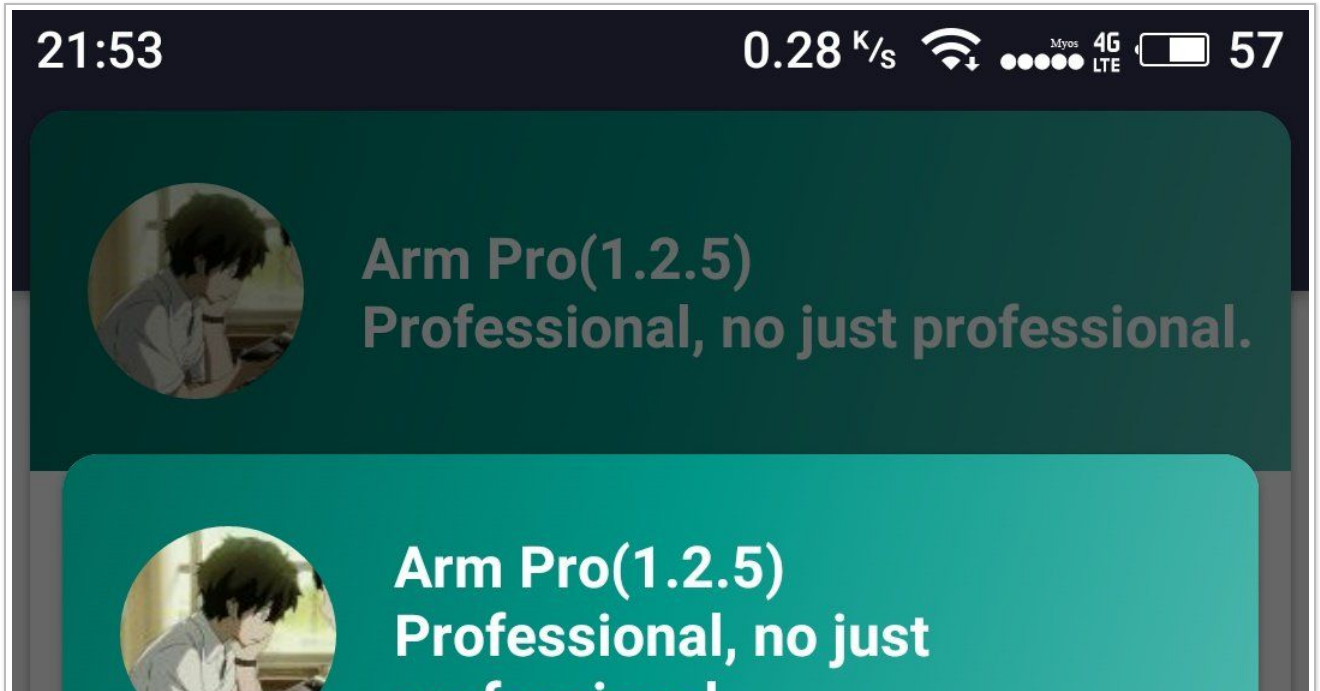

12-04 09:07:06 0B
没有更多数据了
是否选择:快对作业_3.4.0.apk
取消
确定
吾爱破解论坛
www.52pojie.cn

#3 选择完成后, 点击去除签名校验 Pro, 然后点击下一步

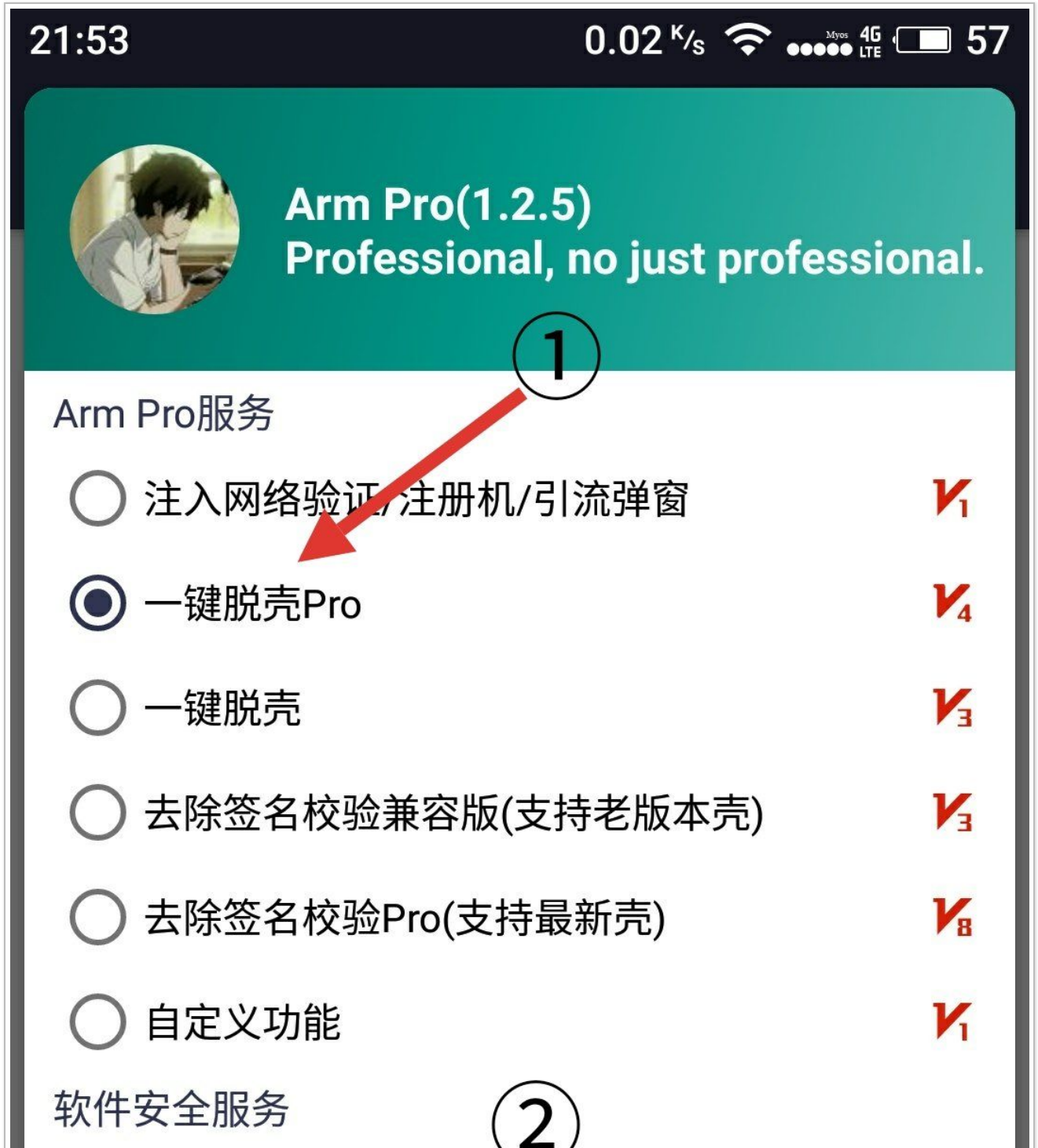


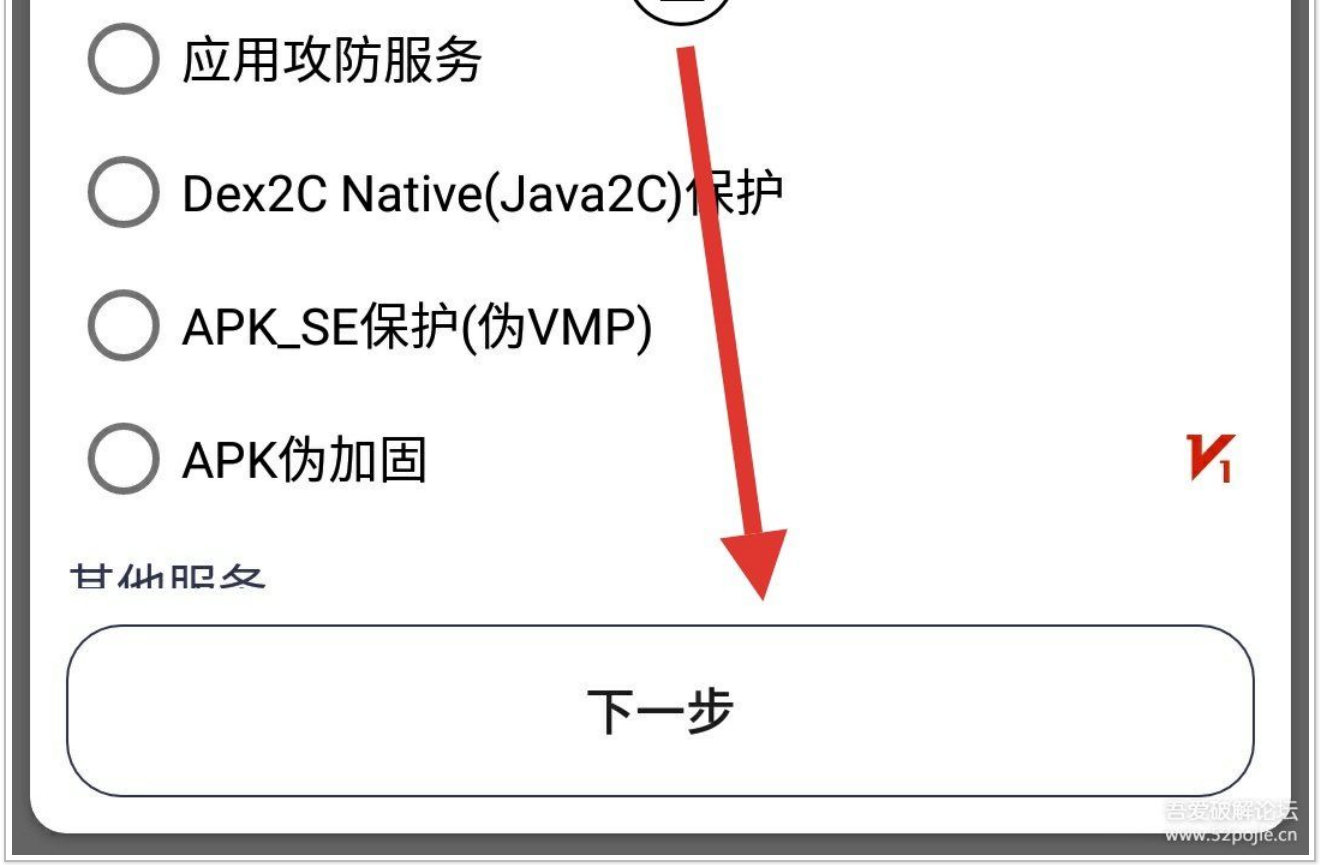


这里看情况选择, 按默认的就好

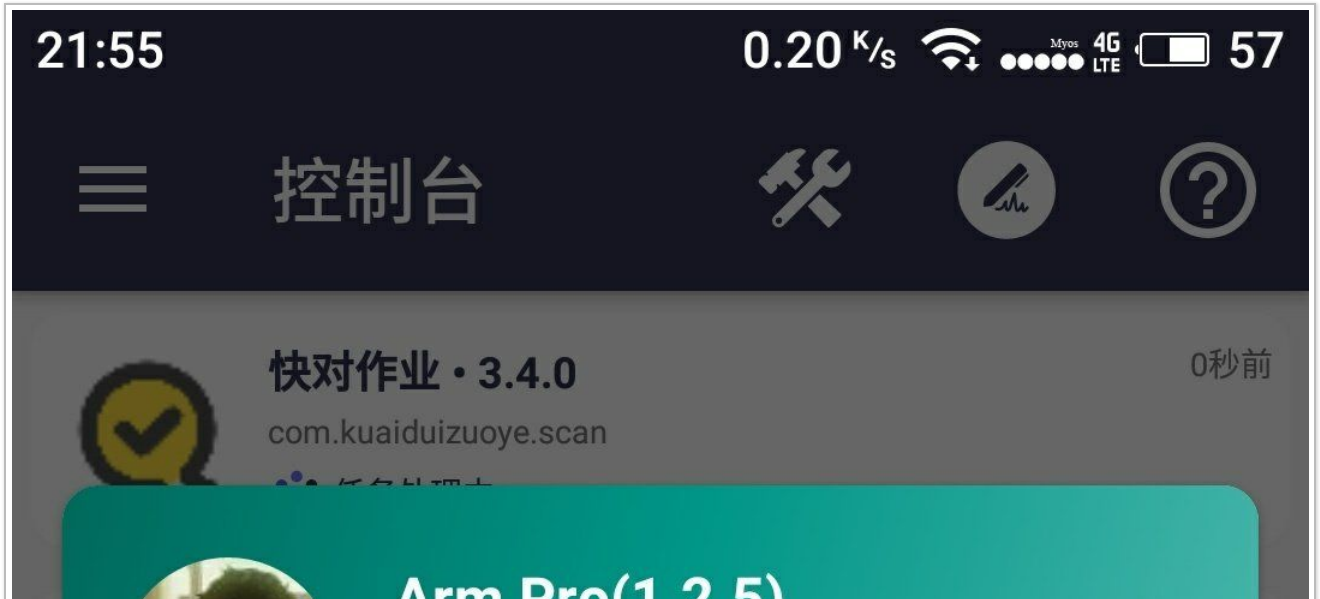


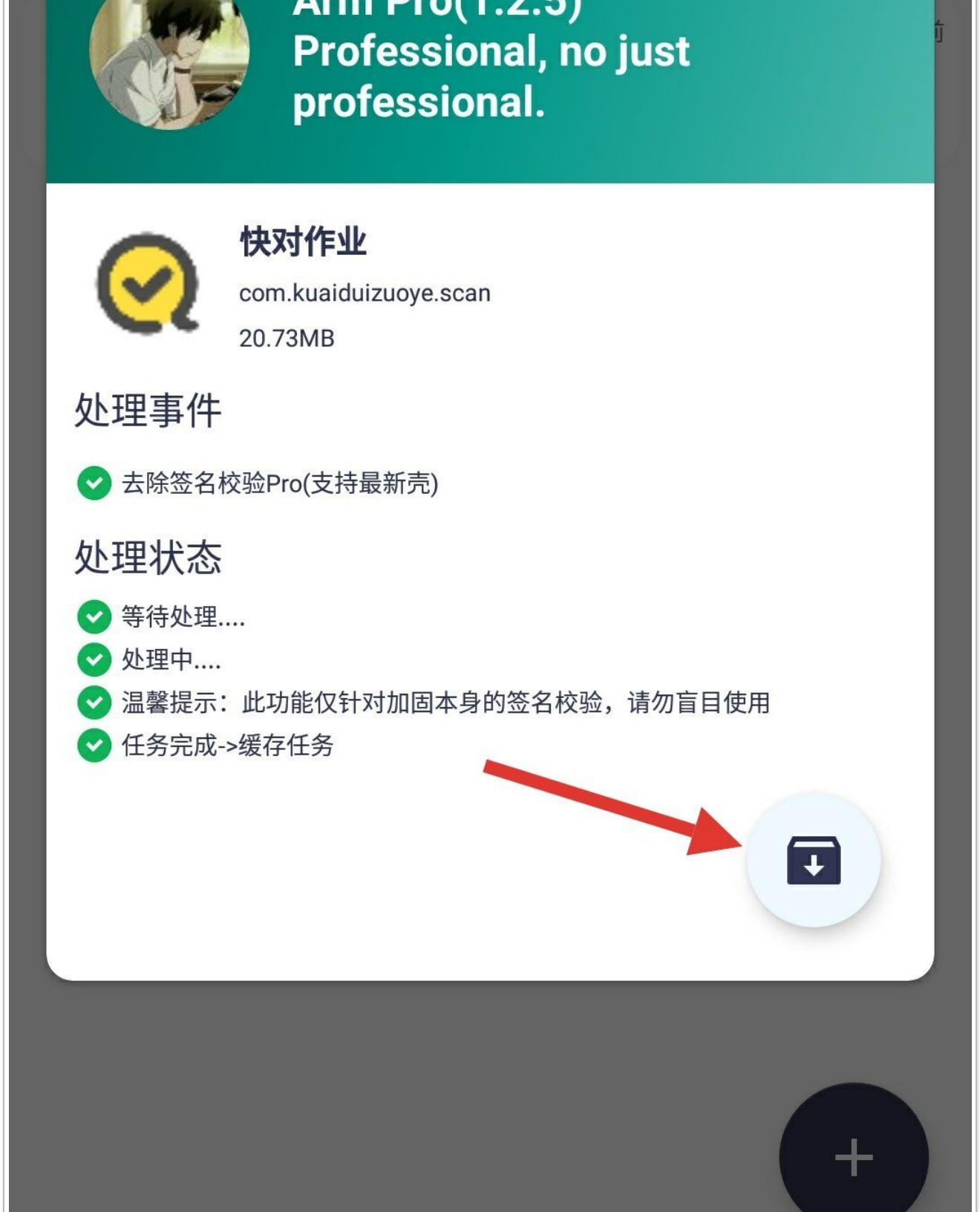
#4 然后继续重复 #2 的步骤，选择一键脱壳 Pro，然后点下一步



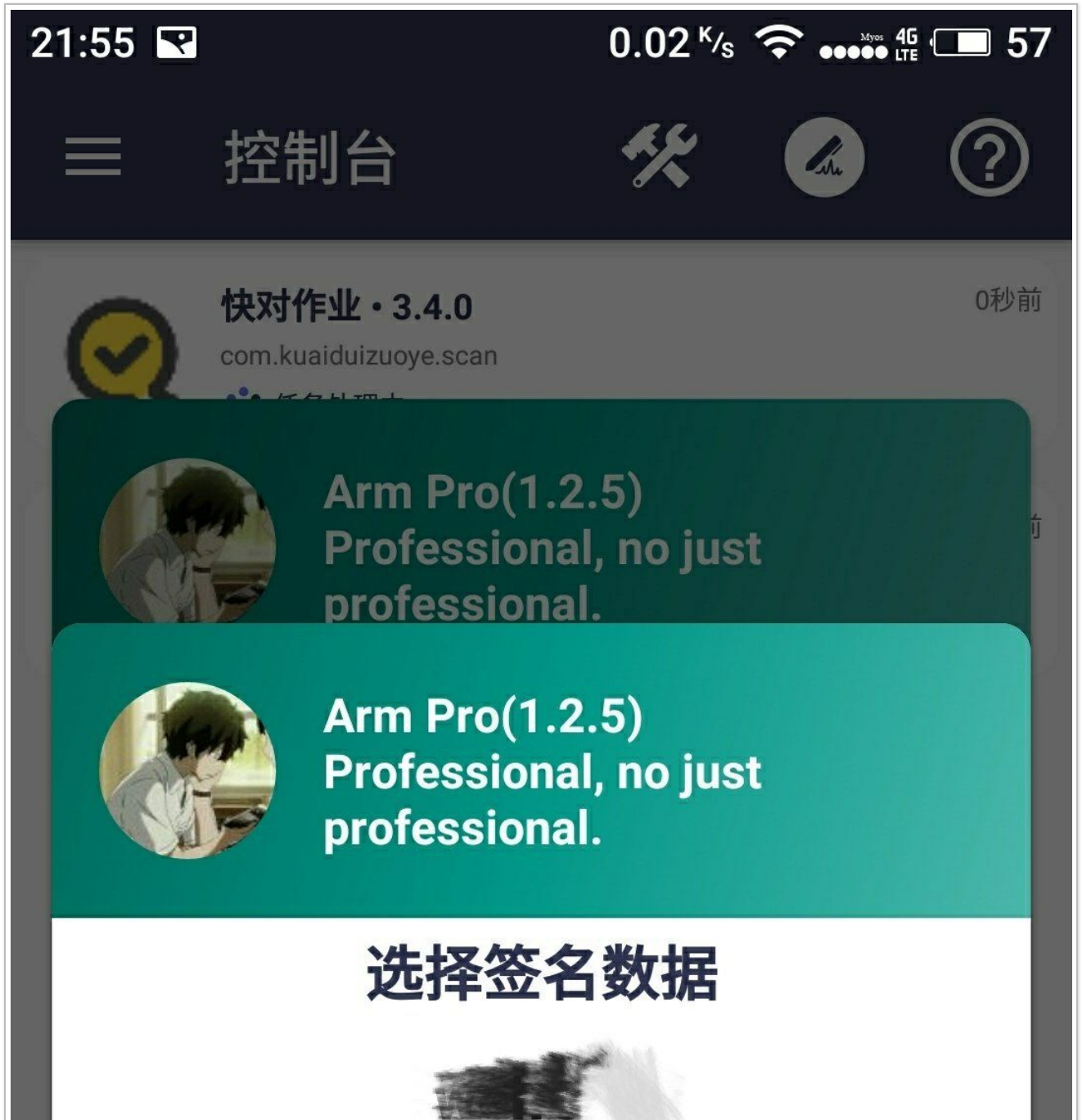


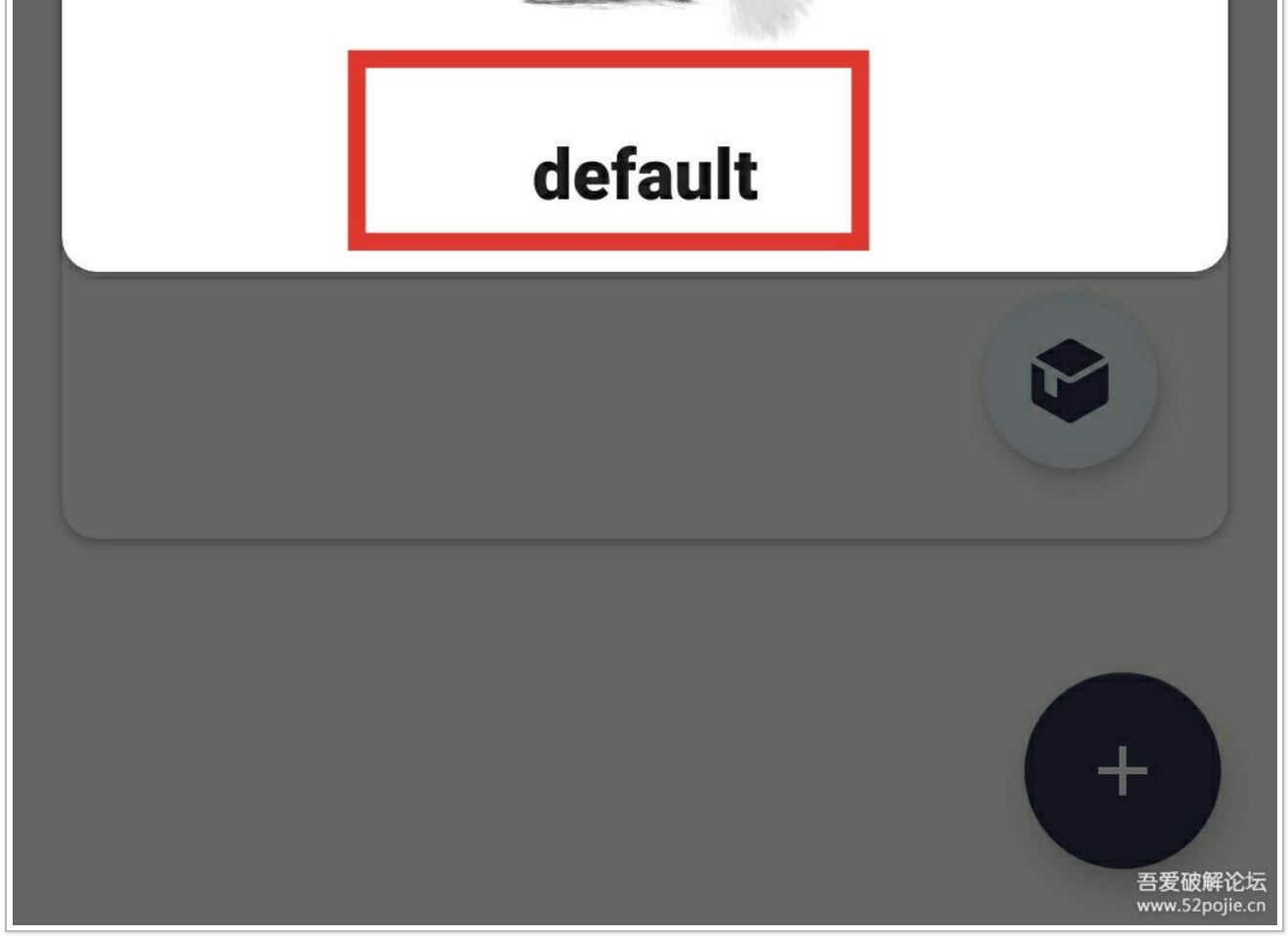
#5 点一下第一个去除签名校验的, 在点击一个像压缩包图标的按键 (如下图)



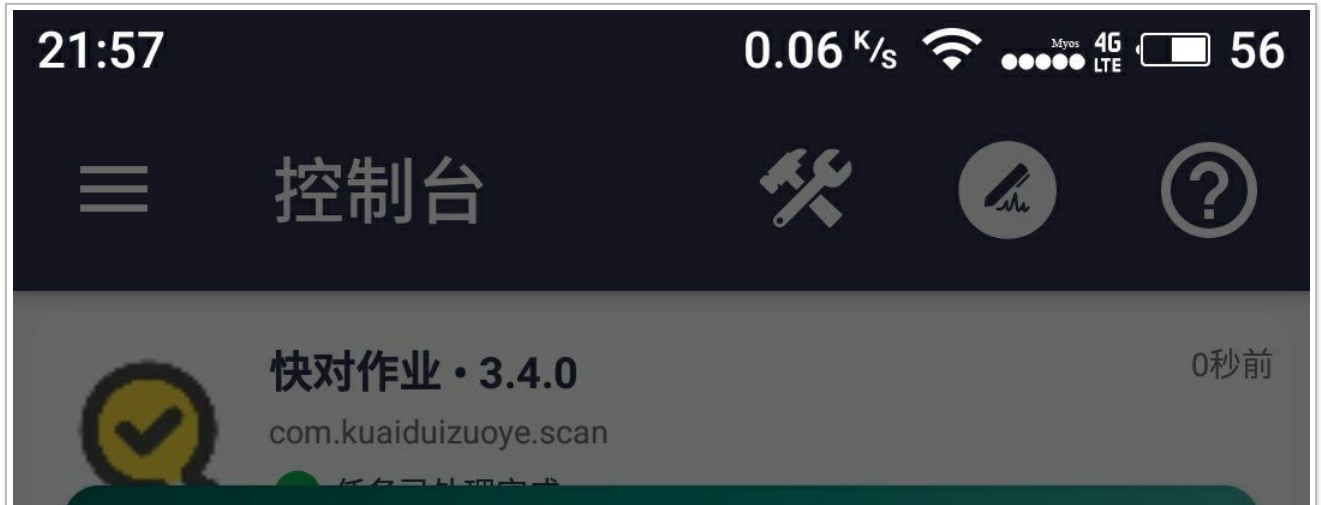

Professional, no just
professional.
快对作业
com.kuaiduizuoye.scan
20.73MB
处理事件
去除签名校验Pro(支持最新壳)
处理状态
等待处理....
处理中....
温馨提示：此功能仅针对加固本身的签名校验，请勿盲目使用
任务完成->缓存任务

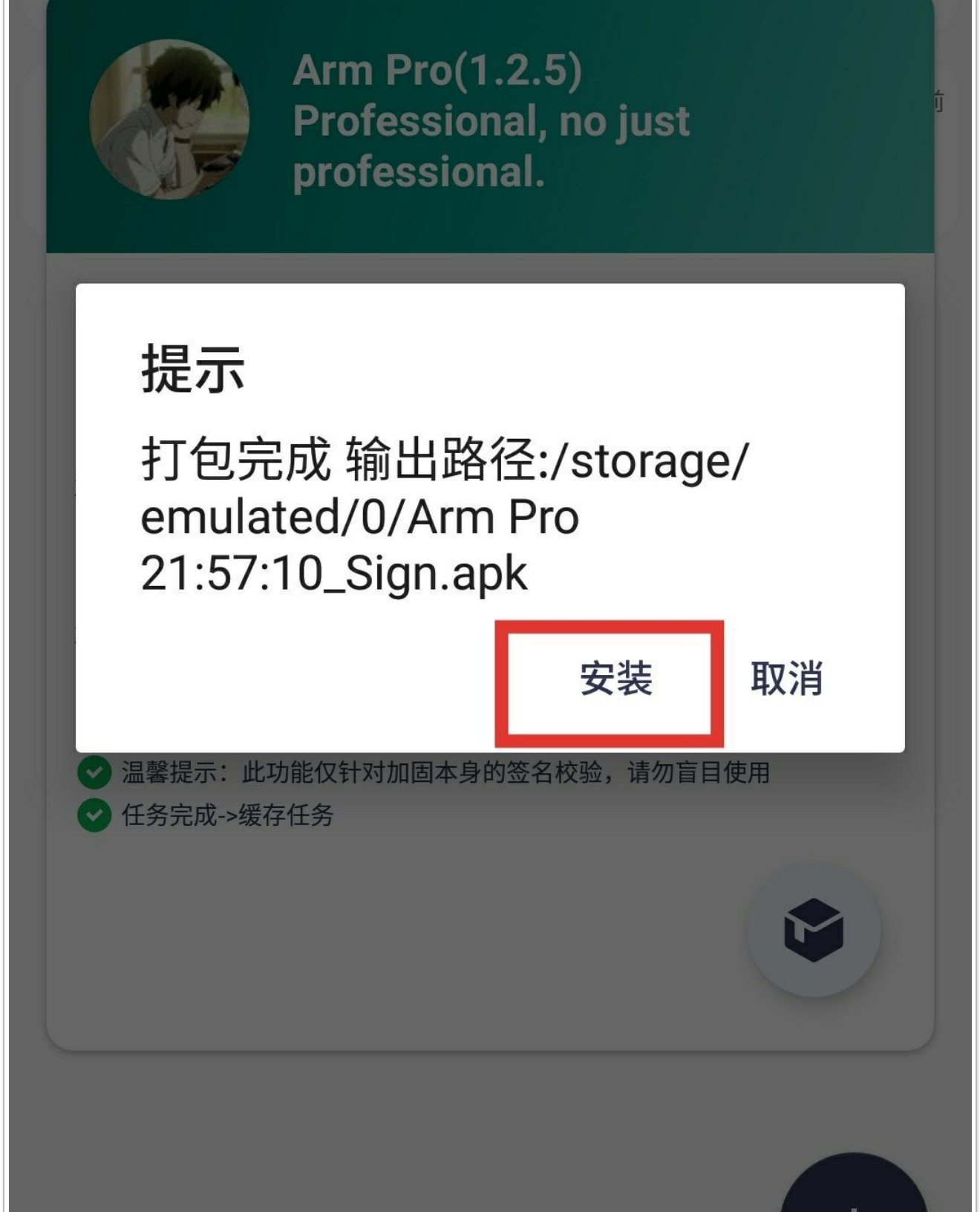
签名的话，按默认的来（打马赛克的是我自己设置的签名）

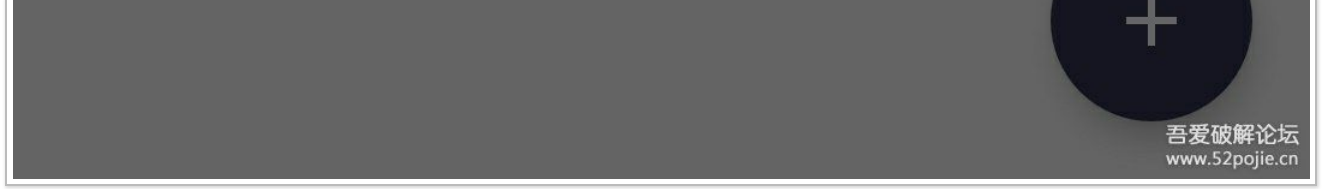




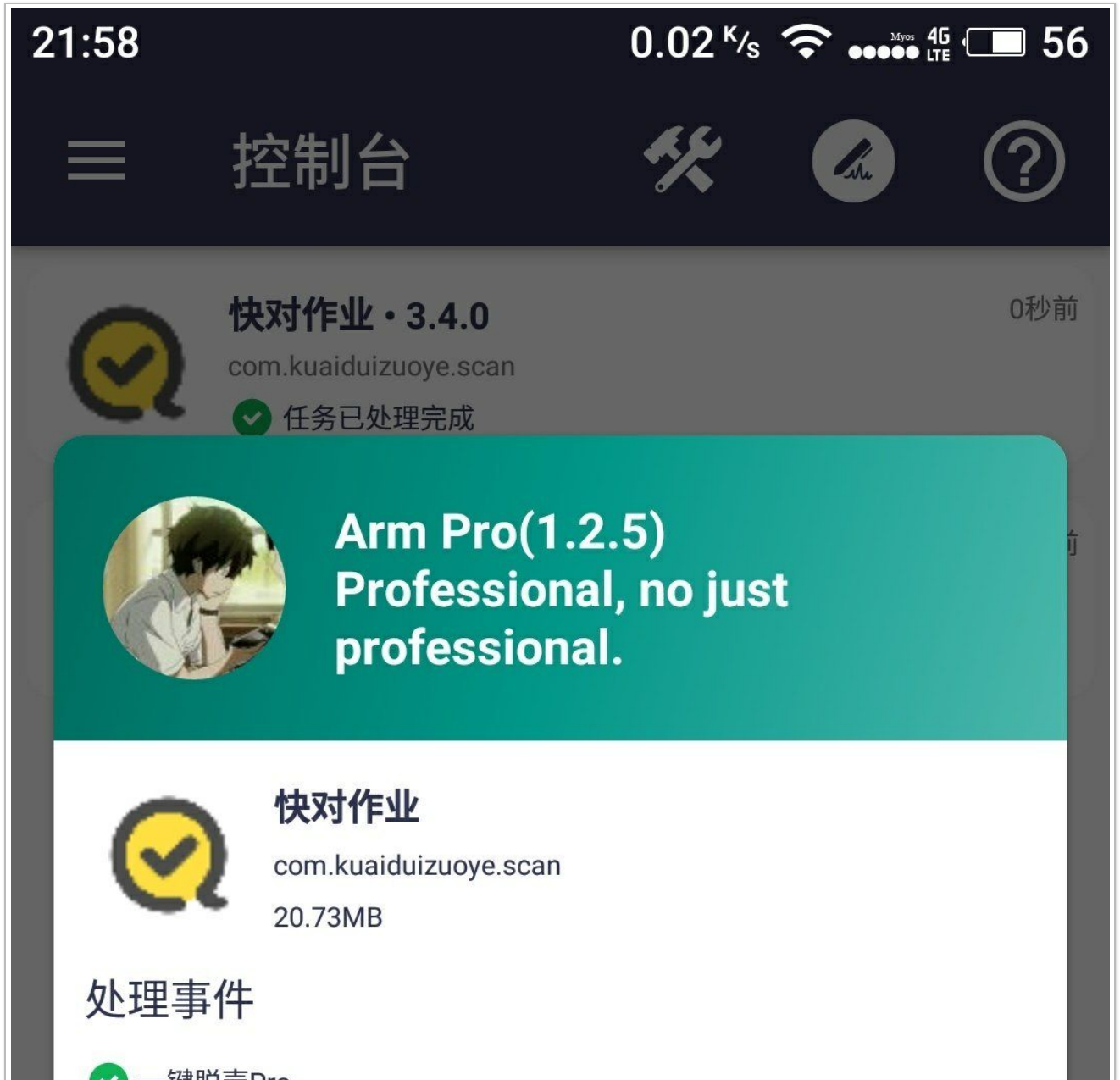
这里建议先安装看看会不会闪退, 如果闪退, 请看到 #3 换一个模式



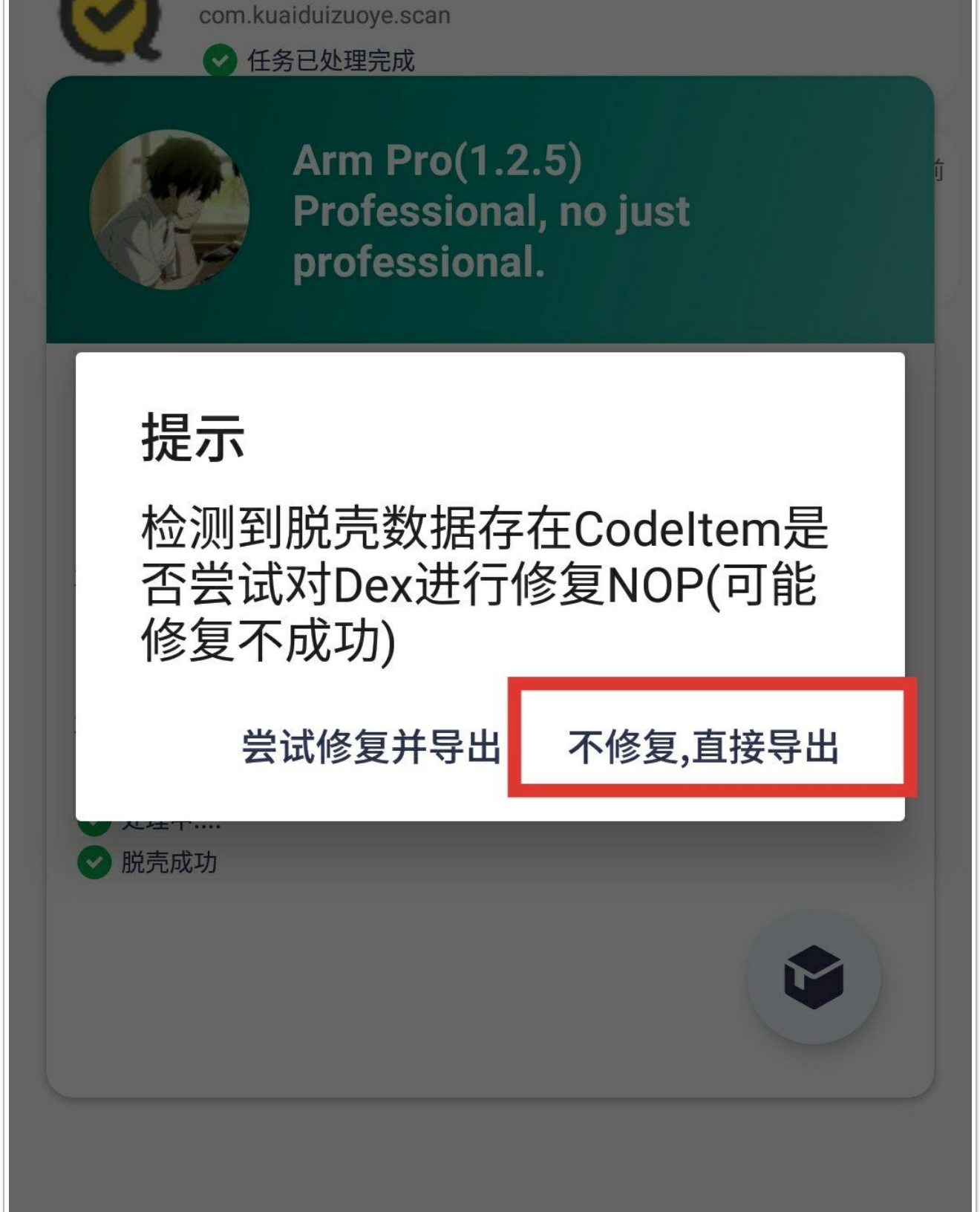

Arm Pro(1.2.5)
Professional, no just professional.
提示
打包完成 输出路径:/storage/emulated/0/Arm Pro 21:57:10_Sign.apk
安装
取消
温馨提示：此功能仅针对加固本身的签名校验，请勿盲目使用
任务完成->缓存任务



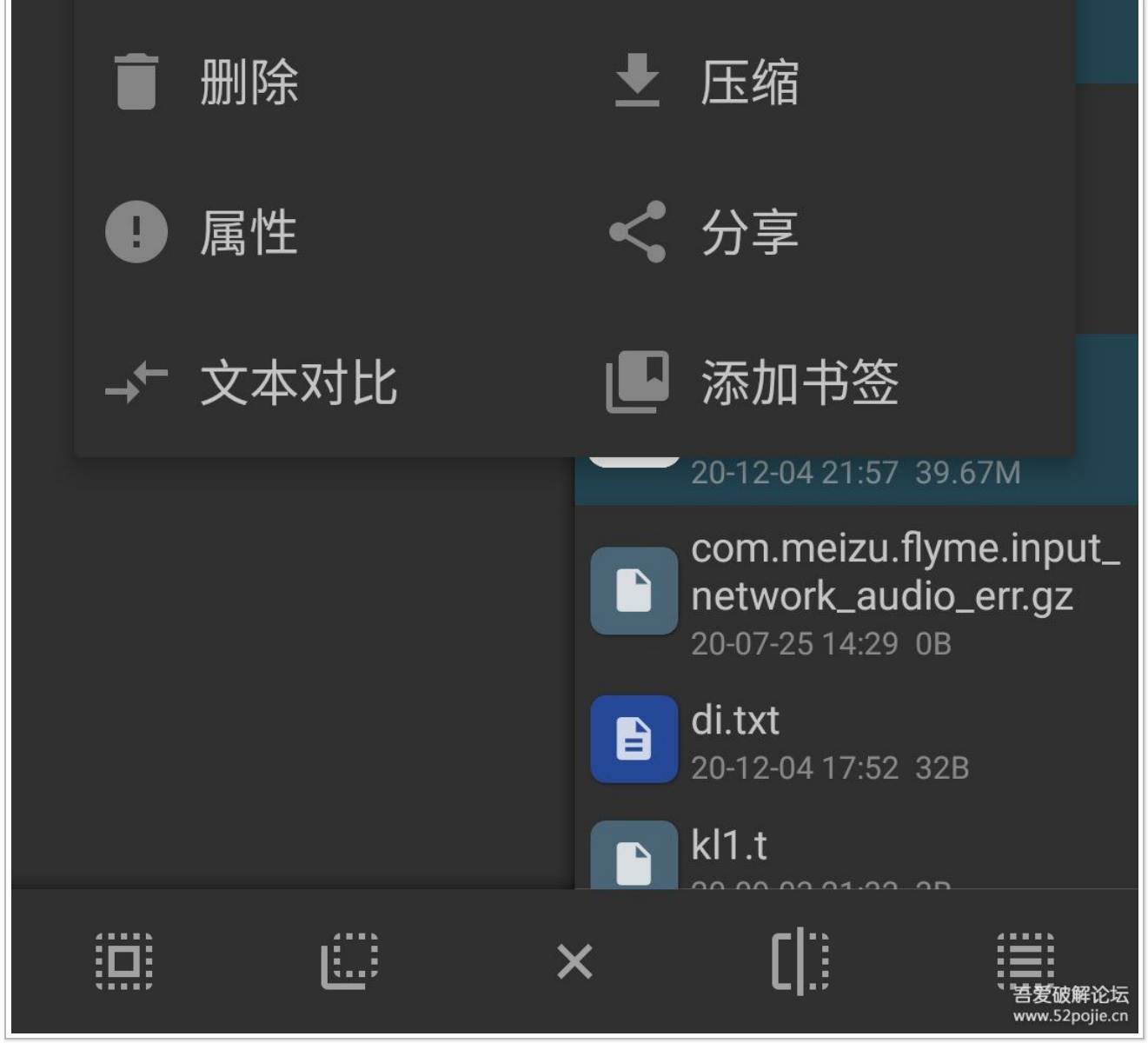
#6 点击一键脱壳 Pro 的那个, 步骤和 #5 差不多



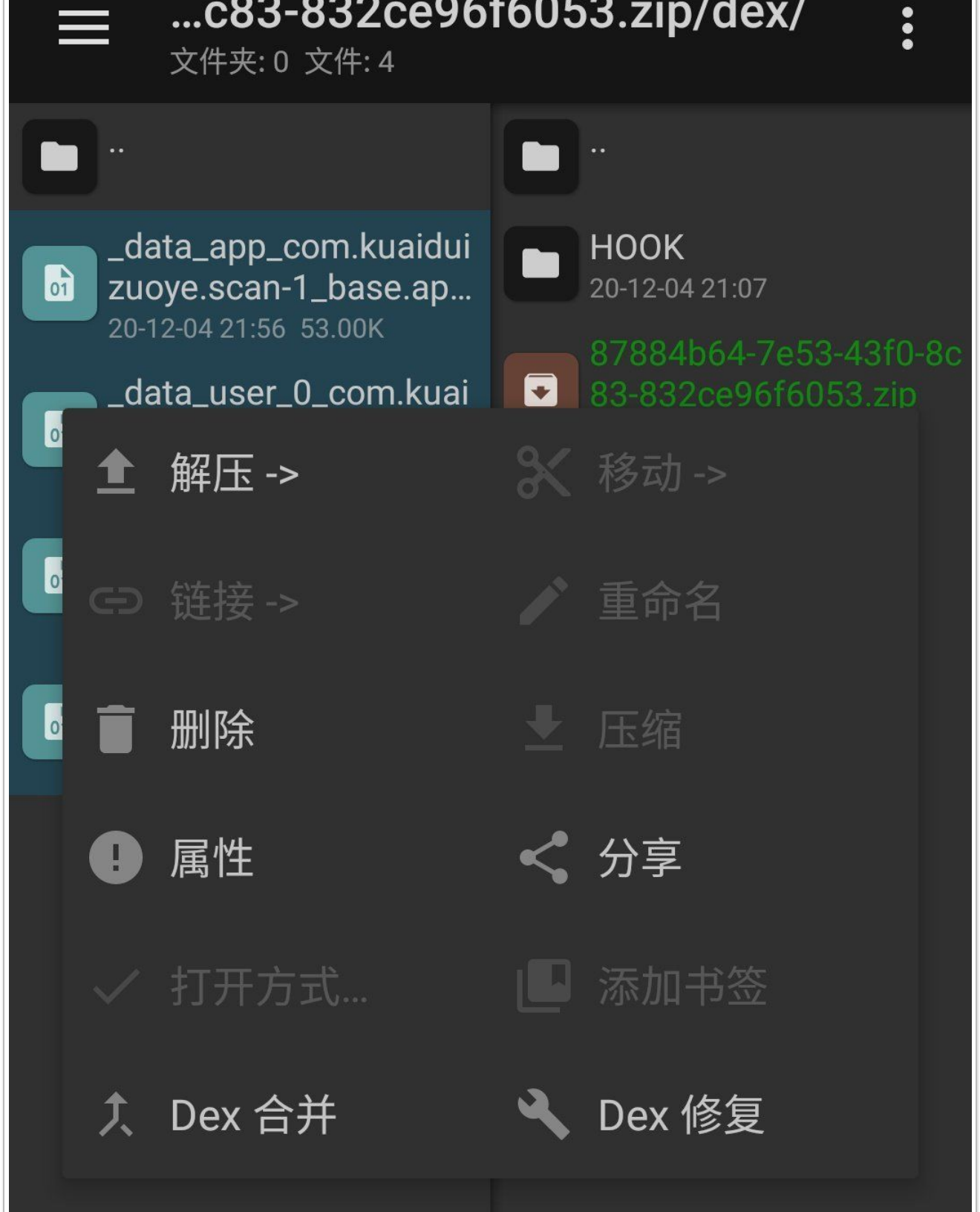
这里注意选择不修复，直接导出

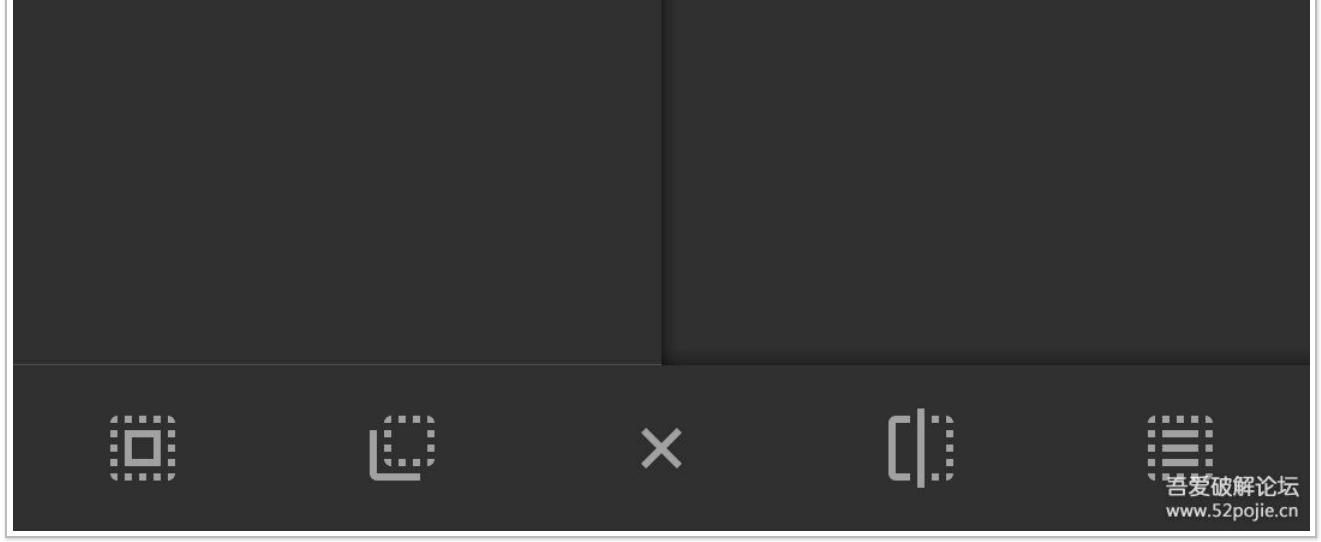

com.kuaiduizuoye.scan
任务已处理完成
Arm Pro(1.2.5)
Professional, no just professional.
提示
检测到脱壳数据存在CodeItem是否尝试对Dex进行修复NOP(可能修复不成功)
尝试修复并导出
不修复,直接导出
脱壳成功

#7 然后打开 MT 管理器, 到内部存储的根目录下找到导出的两个文件 (建议放在同一个文件夹里, 方便操作)

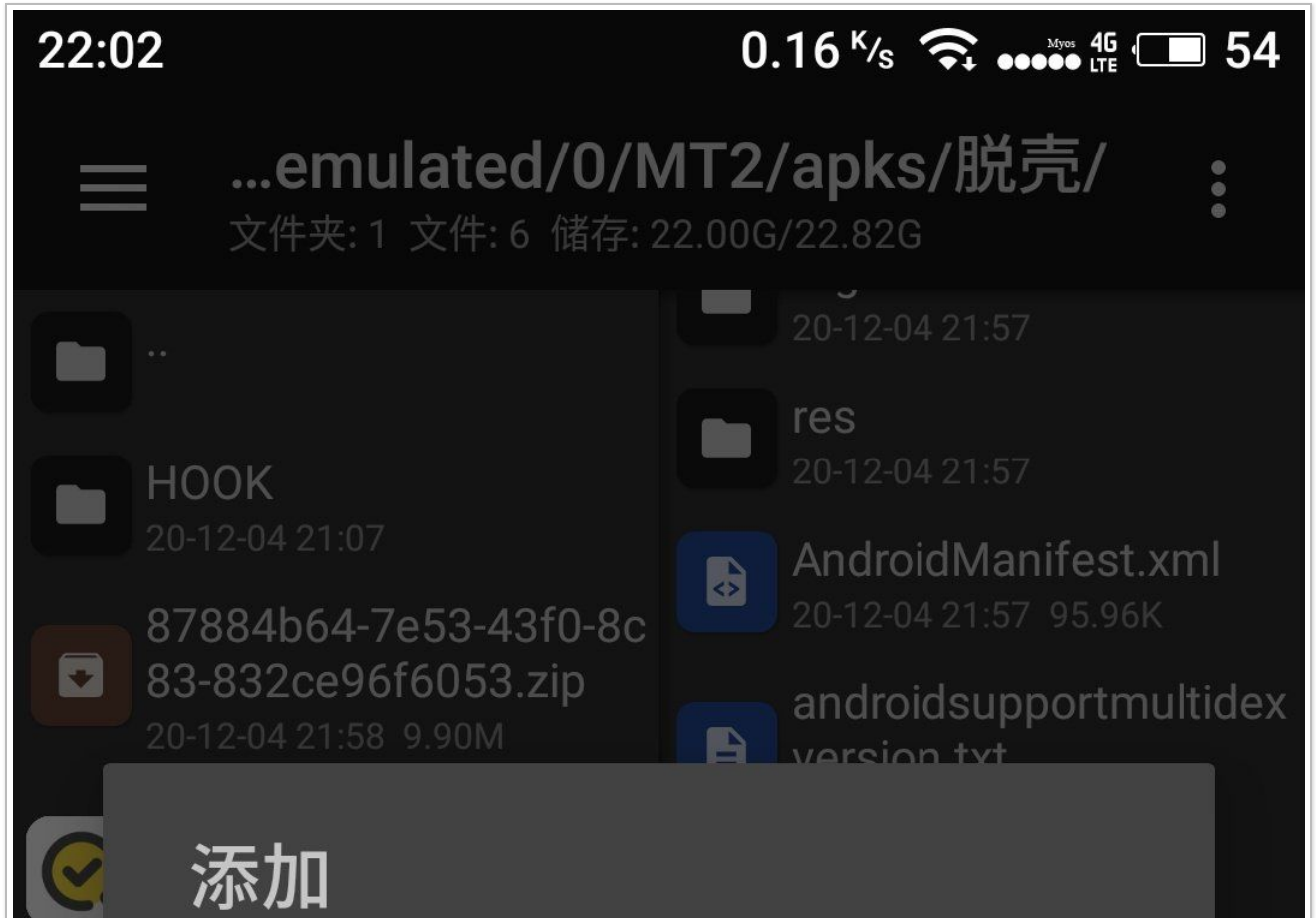


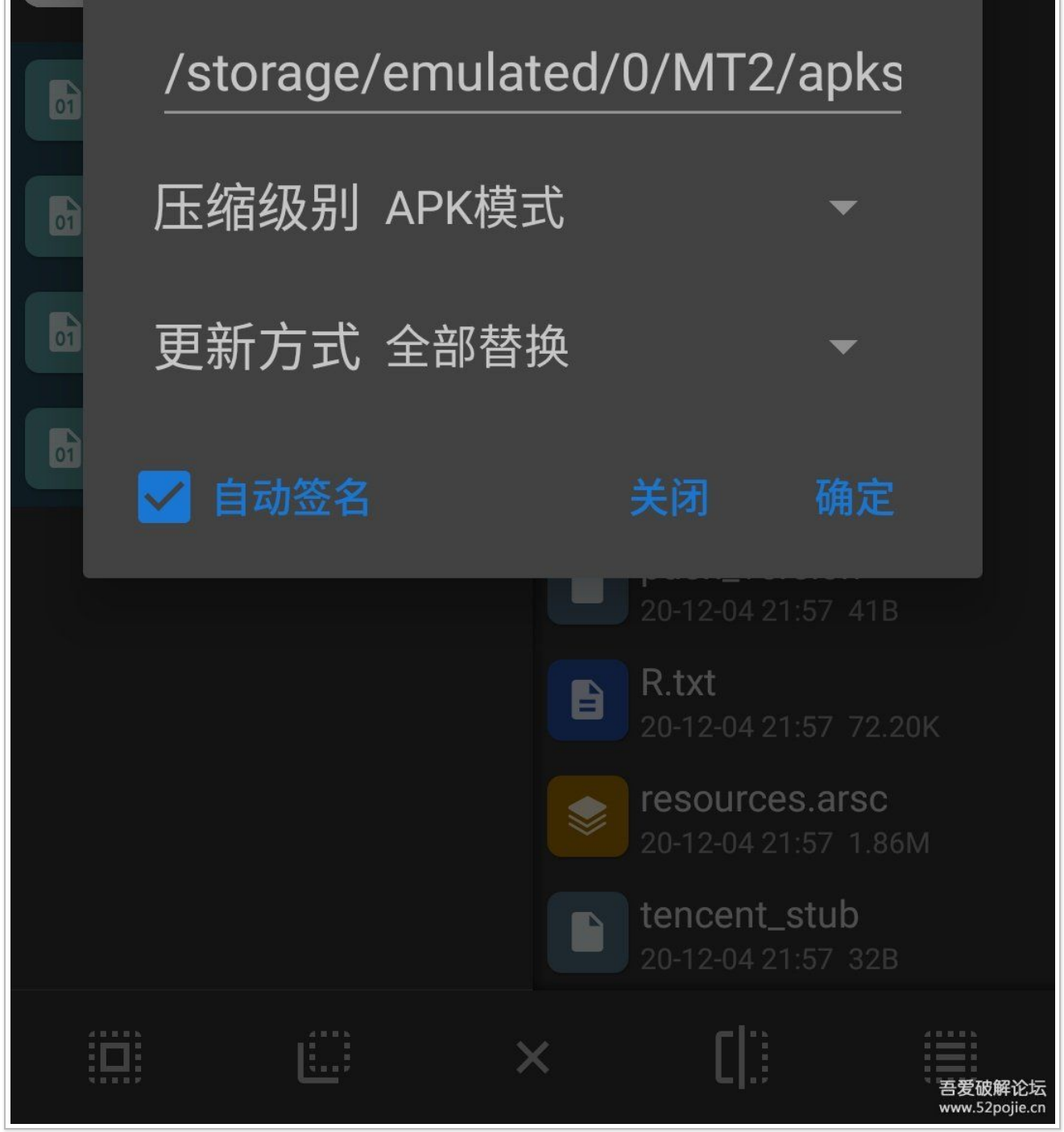
#8 打开压缩包, 把里面的全部 dex 文件解压出来, 然后把它们全部重命名 classes*.dex(其中,* 是去除签名校验软件里面的 classes.dex 数量 + 1 例如我这里最大是 classes3.dex, 则另外 4 个分别为 classes4.dex、classes5.dex 等等, 大家自己以此类推吧, 我这里不放图了)


...c83-832ce96f6053.zip/dex/
文件夹: 0 文件: 4
..
_data_app_com.kuaidui
zuoye.scan-1_base.ap...
20-12-04 21:56 53.00K
_data_user_0_com.kuai
..
HOOK
20-12-04 21:07
87884b64-7e53-43f0-8c
83-832ce96f6053.zip
解压 ->
移动 ->
链接 ->
重命名
删除
压缩
属性
分享
打开方式...
添加书签
Dex 合并
Dex 修复

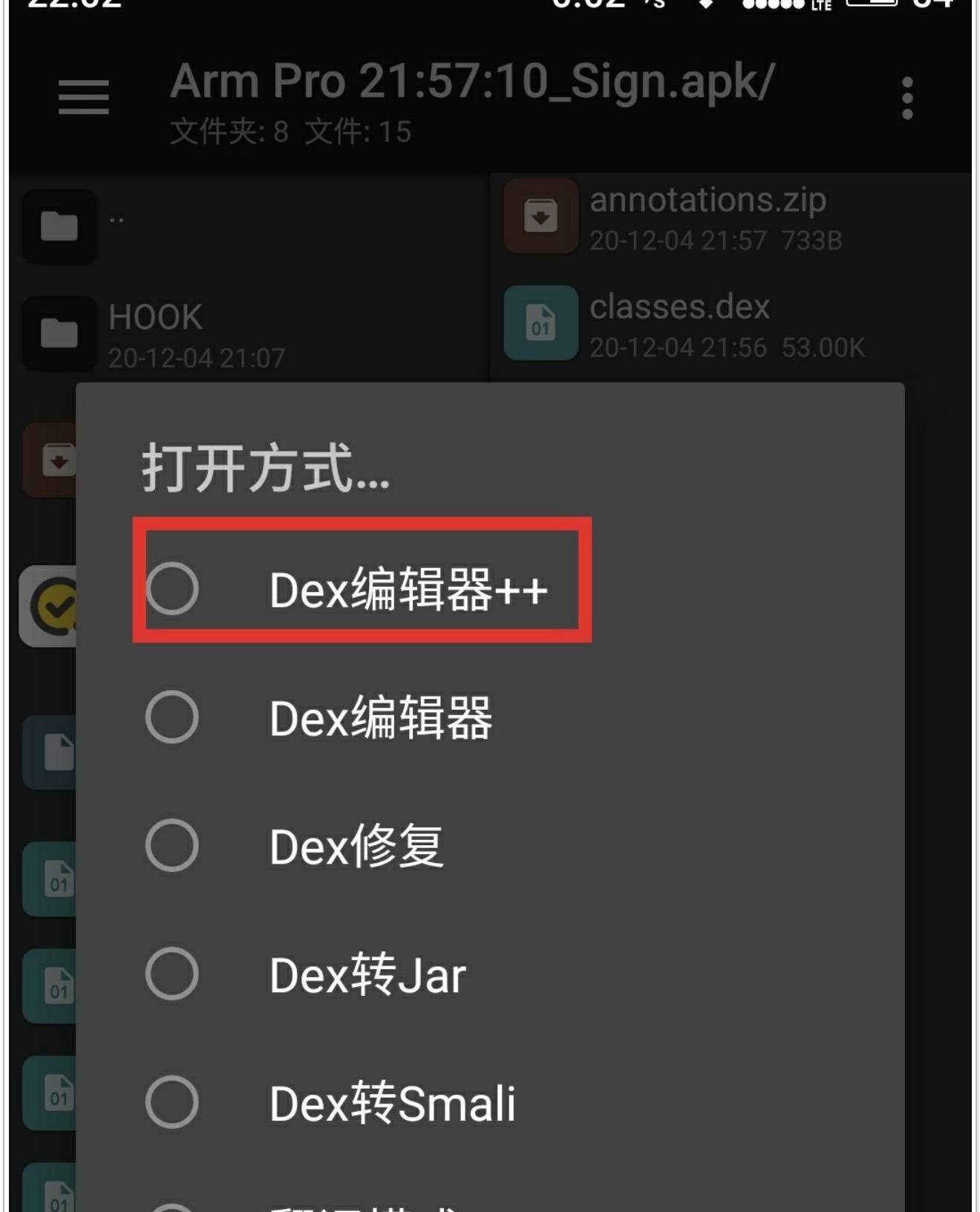


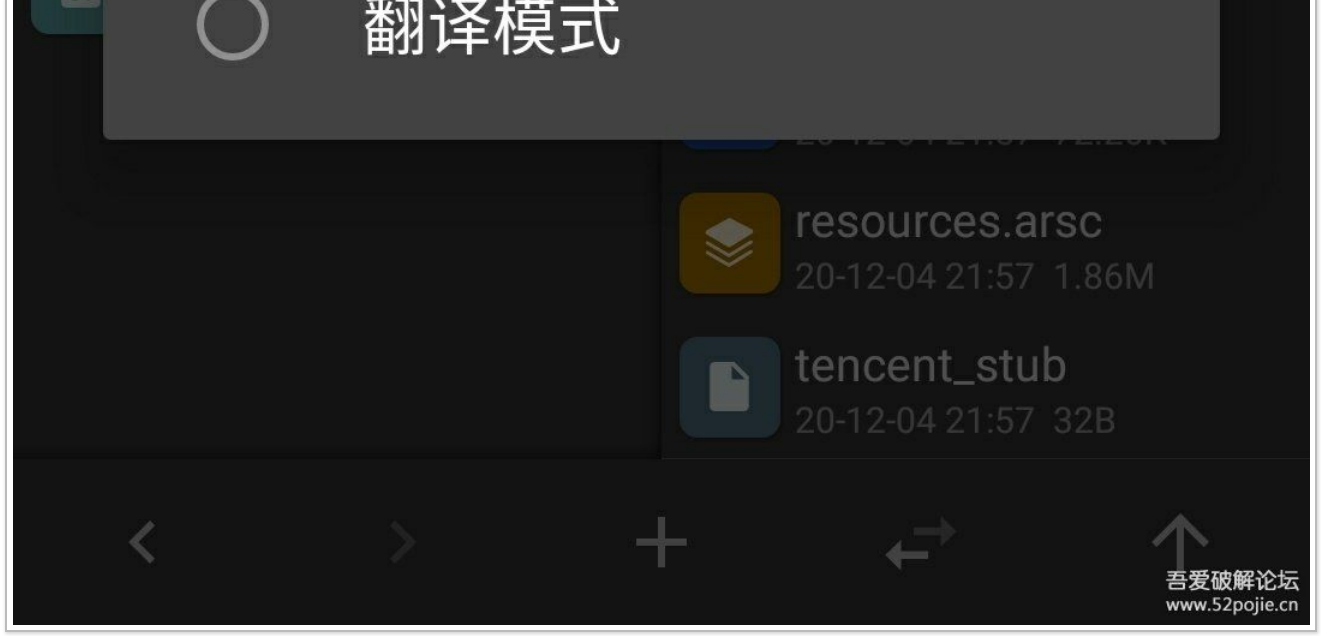
#9 重命名完成后, 把它们全部添加进去



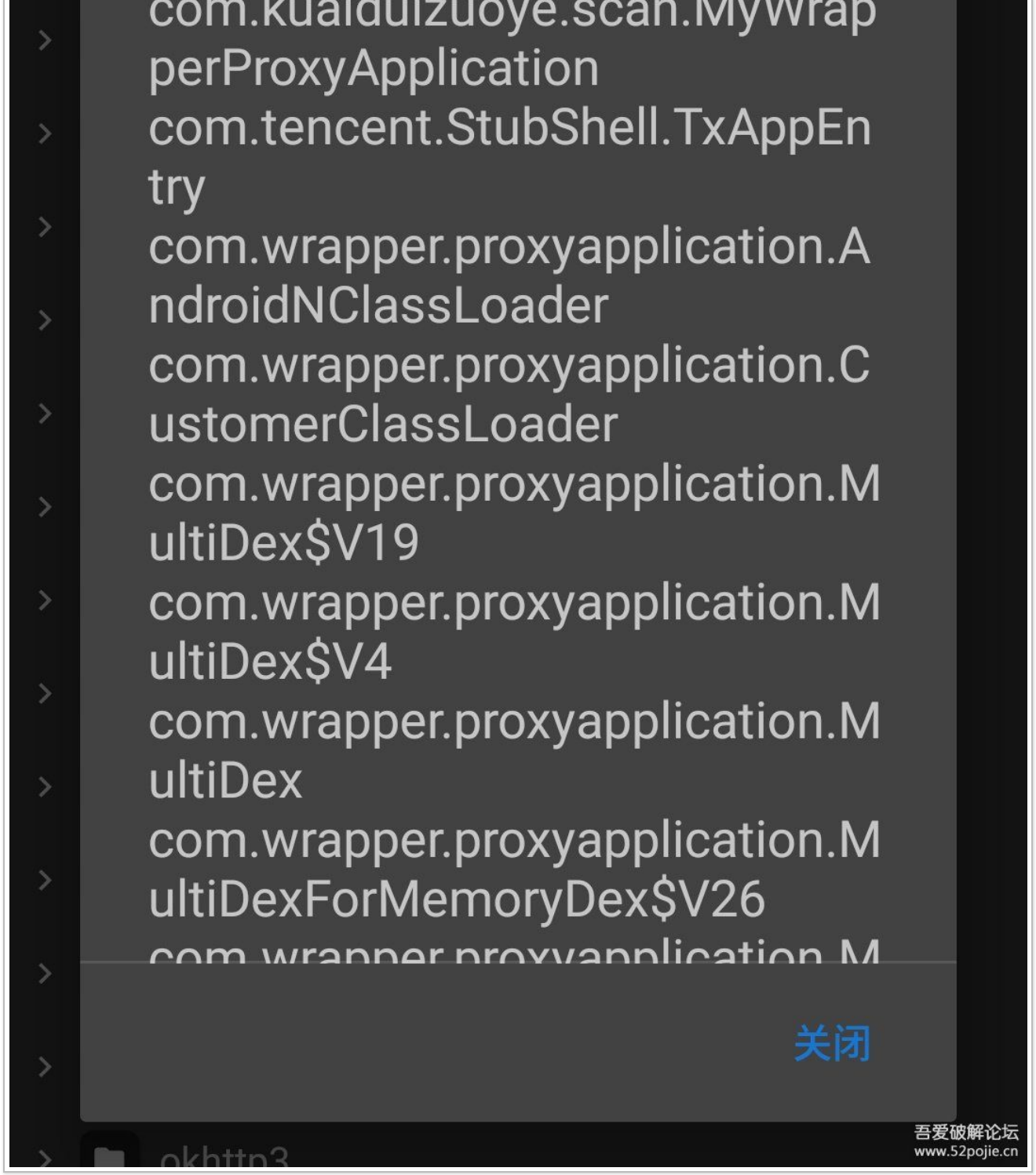


#10 然后选择 dex 编辑器 ++, 全选所有的 dex


Arm Pro 21:57:10_Sign.apk/
文件夹: 8 文件: 15
..
HOOK
20-12-04 21:07
annotations.zip
20-12-04 21:57 733B
classes.dex
20-12-04 21:56 53.00K
打开方式...
Dex编辑器++
Dex编辑器
Dex修复
Dex转Jar
Dex转Smali

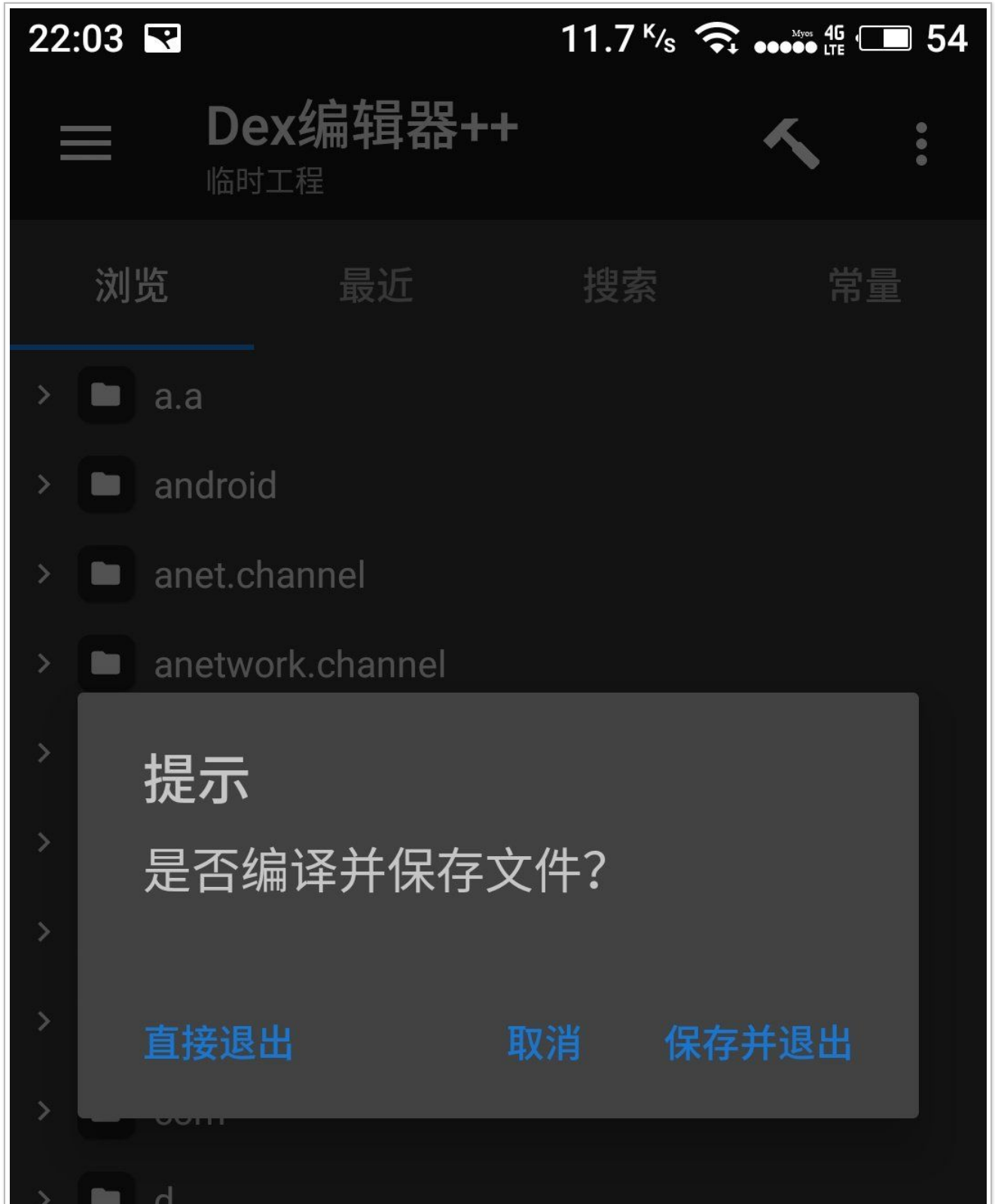


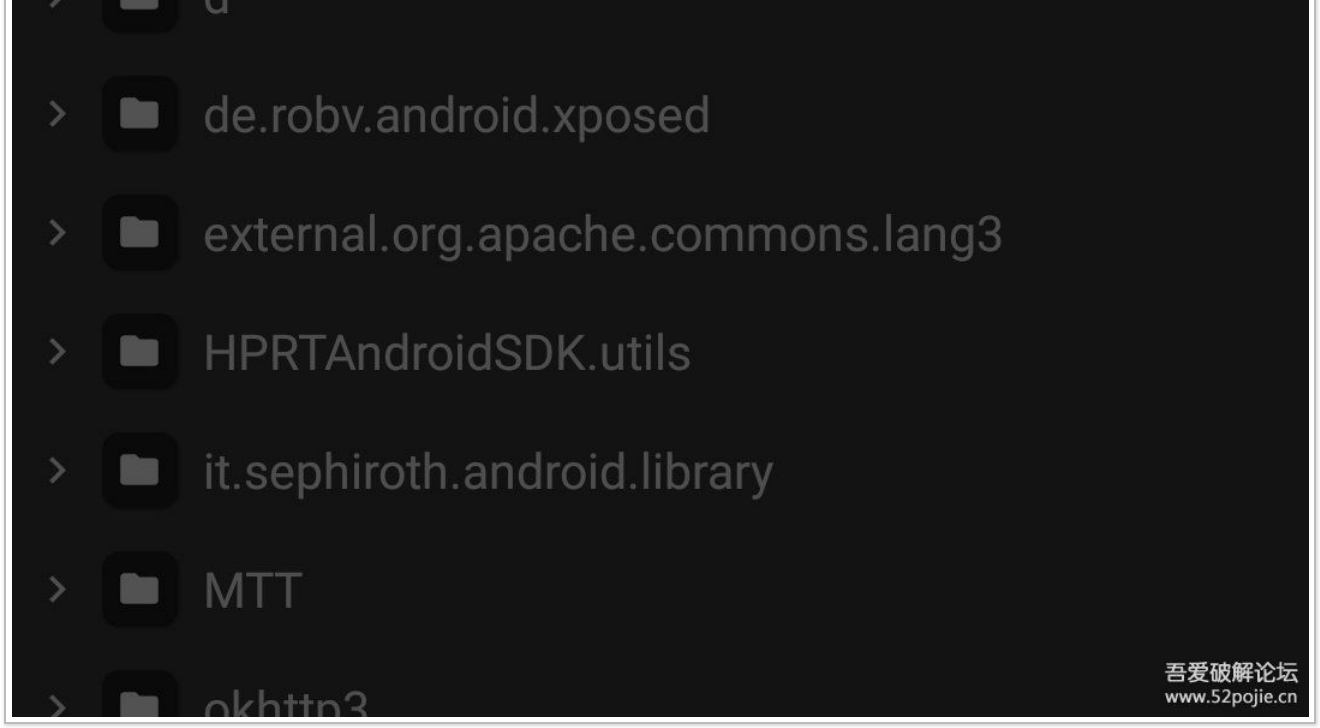
进来后, 有的可能会提示出这个



不要慌，它出来就对了，然后点击关闭，然后选择保存并退出即可

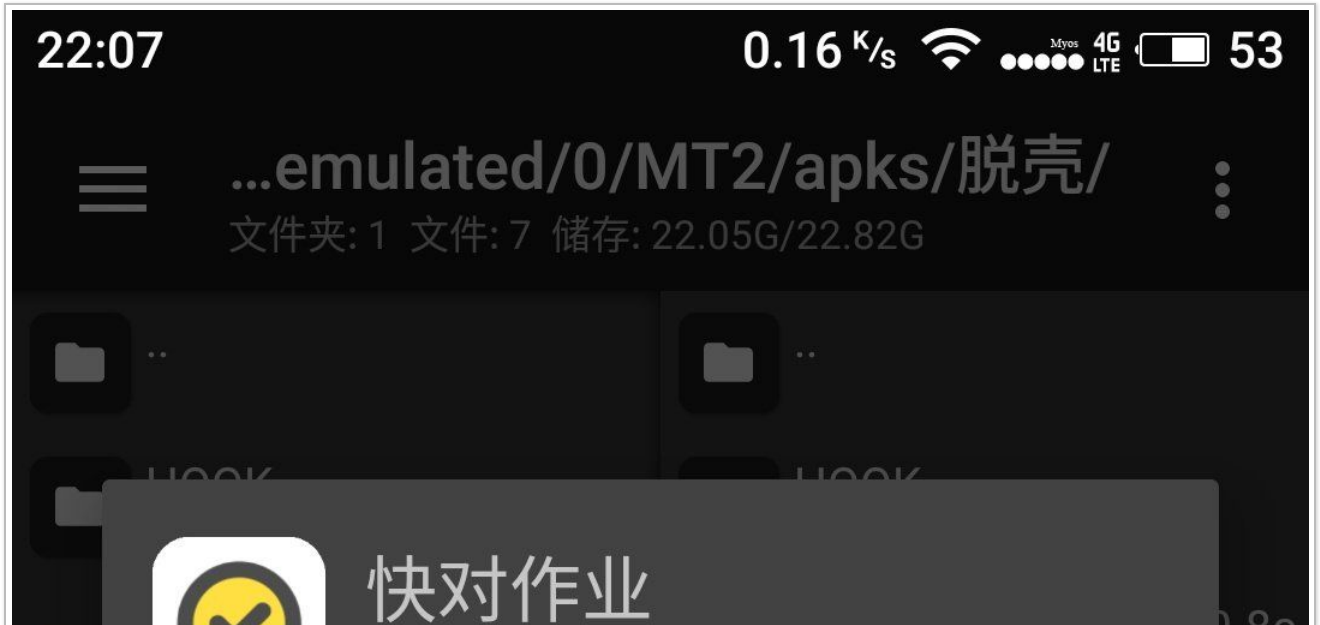
不要就，已经来就对了，然后点击关闭，然后选择保存并退出即可

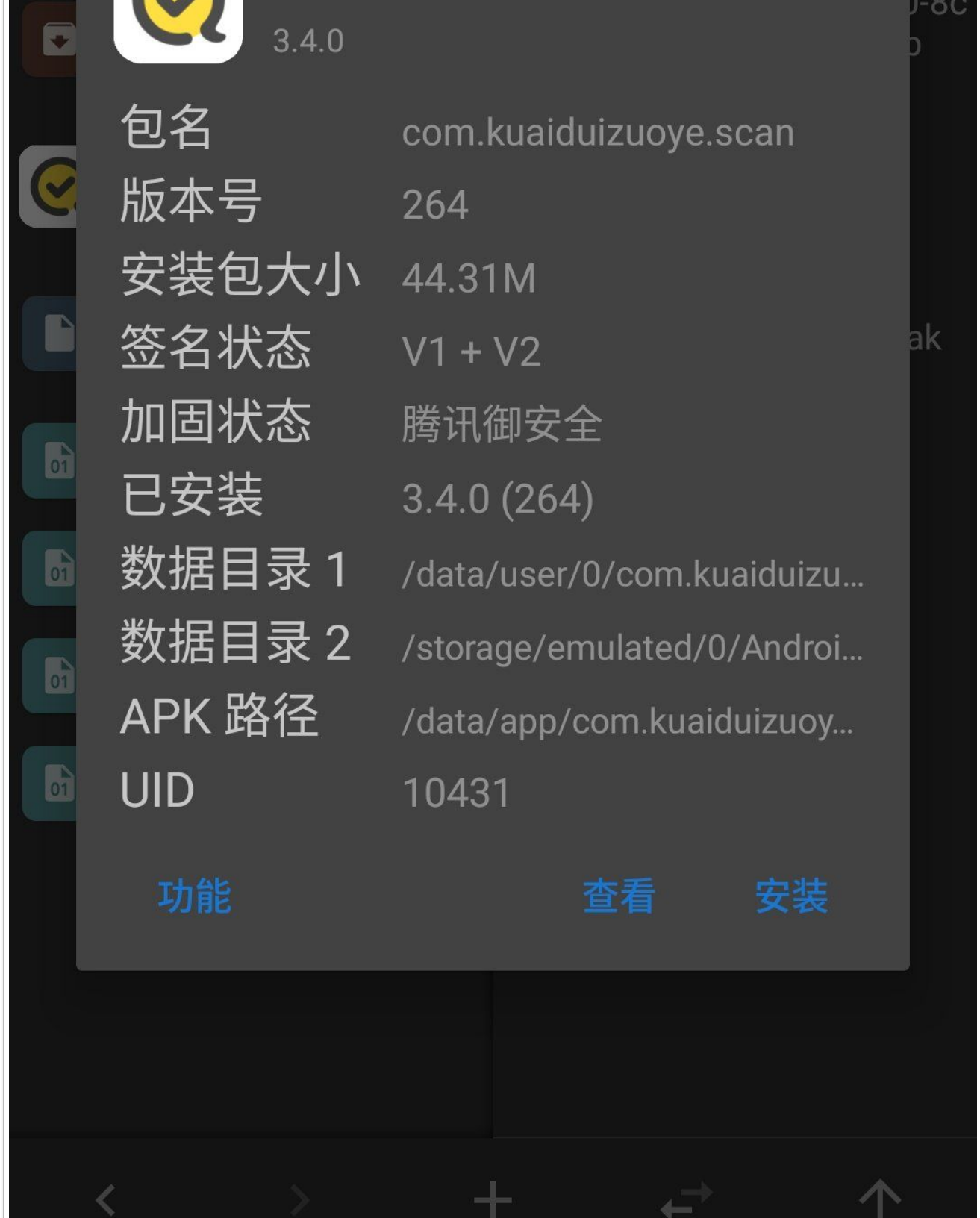




注意, 这部意义不大, 所以可有可无, 只是我有多年的强迫症晚期导致的

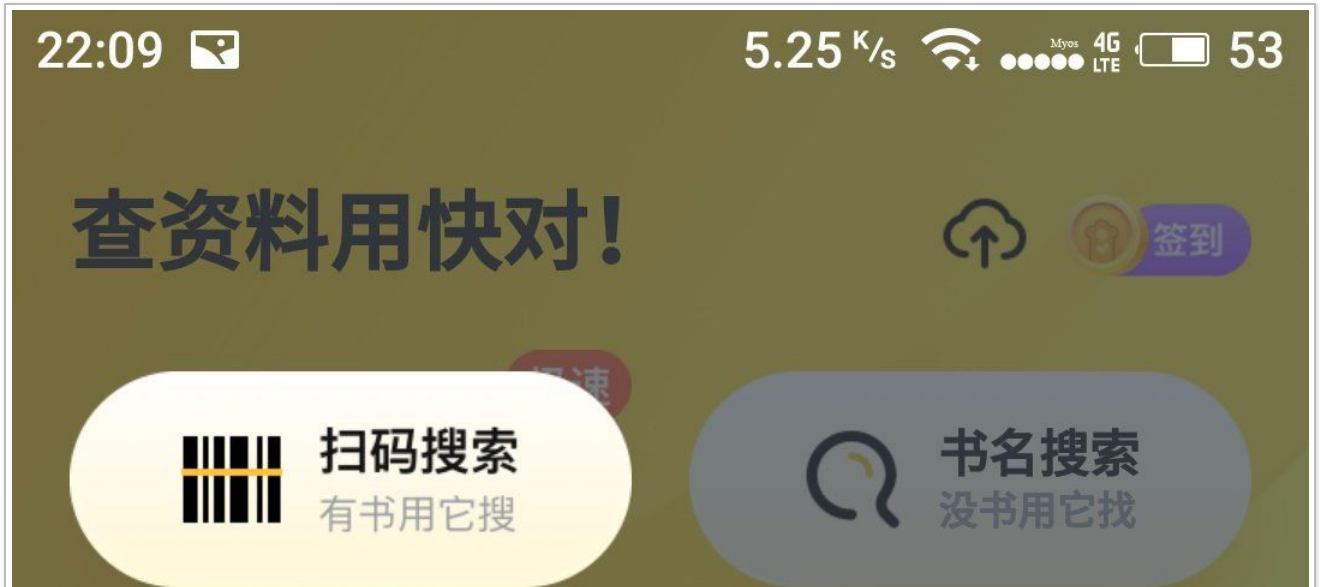
声明一下, 出来后, 虽然 mt 管理器还是会提示是腾讯御安全, 但实际上, 不会影响我们的逆向操作的, 在就是他的不完美之处

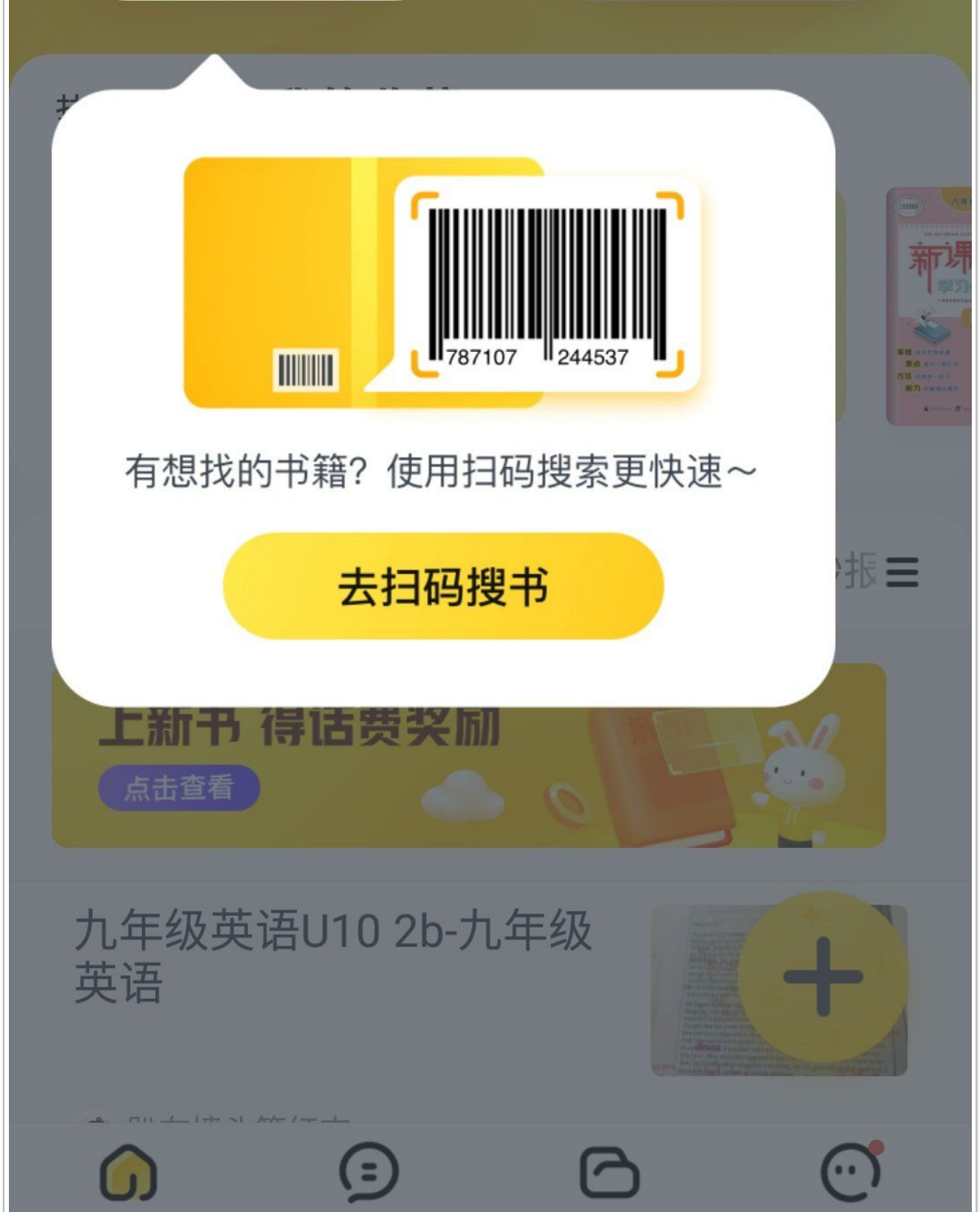



3.4.0
包名 com.kuaiduizuoye.scan
版本号 264
安装包大小 44.31M
签名状态 V1 + V2
加固状态 腾讯御安全
已安装 3.4.0 (264)
数据目录 1 /data/user/0/com.kuaiduizu...
数据目录 2 /storage/emulated/0/Androi...
APK 路径 /data/app/com.kuaiduizuoy...
UID 10431
功能
查看
安装

最后完美运行不闪退

登录即视为同意《用户服务协议》和《用户隐私政策》和《儿童用户隐私政策》




787107 244537
有想找的书籍？使用扫码搜索更快速～
去扫码搜书
上新书 得话费奖励
点击查看
九年级英语U10 2b-九年级英语

到此, 这篇帖子也该告一段落了, 如果大家有什么不懂的可以来问

最后: 小白瞎搞, 请大神勿喷

感谢楼主 我再也不水了

一只码农

回不去的时光 发表于 2020-12-5 02:37

能问下几个问题吗

这个能脱 360 吗，oncreate 的 native 可以还原吗

然后这款软件需要付费才能用吗，如果免费 ...

360 也可以脱,

正己

arm 脱腾讯不如反射，有概率闪退

这还不如反射好

米粒米粒

马割：兄弟别脱了 明天来上班，我们一起割

3404071

感谢分享

不跟蠢逼…

感谢分享

pdc9911

感谢分享

hongy…

總的方法就是替換類。

列明

感谢楼主分享

K.G 暗雪

哇，这个太实用啦

tanghen…

← 前一页

后一页 →