**Android逆向（反编译一个APK）**

一、反编译未加固的apk

**1、反编译用到的工具**

[apktool](https://links.jianshu.com/go?to=https%3A%2F%2Fbitbucket.org%2FiBotPeaches%2Fapktool%2Fdownloads)：资源文件获取，可以提取出图片文件和布局文件进行使用查看 [dex2jar](https://links.jianshu.com/go?to=%255Bhttp%3A%2F%2Fsourceforge.net%2Fprojects%2Fdex2jar%2Ffiles%2F%255D%28http%3A%2F%2Fsourceforge.net%2Fprojects%2Fdex2jar%2Ffiles%2F%29)：将apk反编译成java源码（[classes.de](http://classes.de)x转化成jar文件）

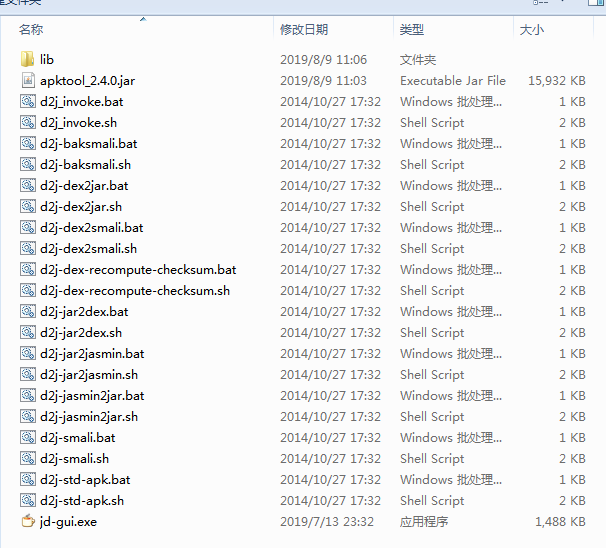
[jd-gui](https://links.jianshu.com/go?to=http%3A%2F%2Fjd.benow.ca%2F)：查看APK中[classes.de](http://classes.de)x转化成出的jar文件，即源码文件

**2、使用apktool反编译资源文件和Manifest文件**

为了方便操作，首先将下载好的3个工具统一放到1个文件夹中



将gui和dex2jar分别解压到当前文件夹

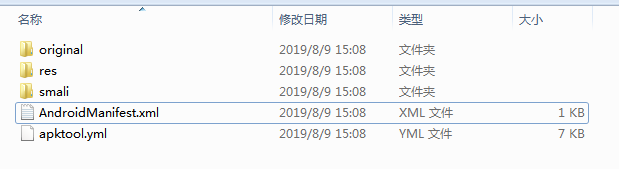


[image.pn](http://image.pn)g

使用apktool反编译apk得到图片、xml、maifest等文件 运行CMD.exe,进入Demo.apk路径下 运行apktool对apk进行反编译 使用如下命令将Demo.apk反编译到【Demo】文件夹下：

java -jar apktool\_2.4.0.jar d -f Demo.apk -o Demo

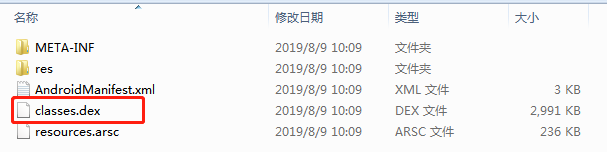
打开Demo文件，就可以看到反编译后生成的文件



这时候可以看到【res】和Manifest文件了；

**3、使用dex2jar反编译java源码**

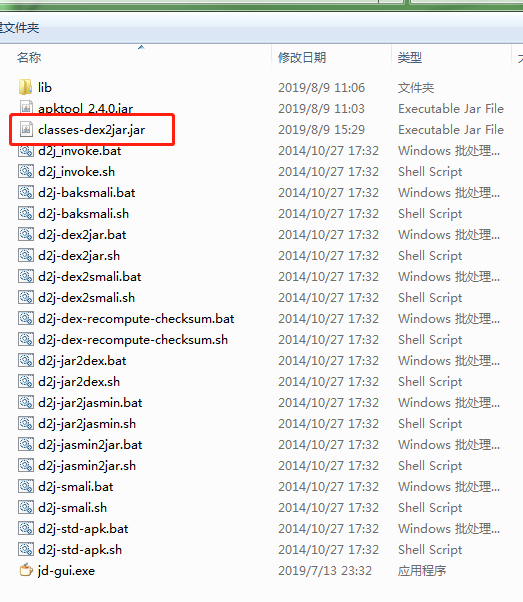
将Demo.apk直接修改后缀，改为[Demo.zip](http://Demo.zip)，并解压 解压后的文件夹中，[classes.de](http://classes.de)x 就是java源码打包后的文件



将命令行定位到[dex2jar.ba](http://dex2jar.ba)t所在目录 使用命令行：

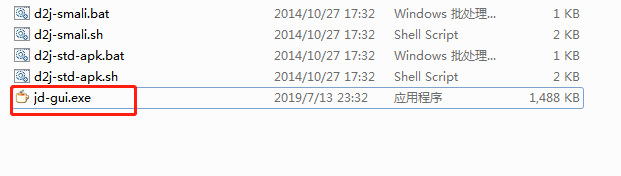
d2j-dex2jar classes.dex

会生成classes-dex2jar文件，该文件就是反编译后的java源码文件

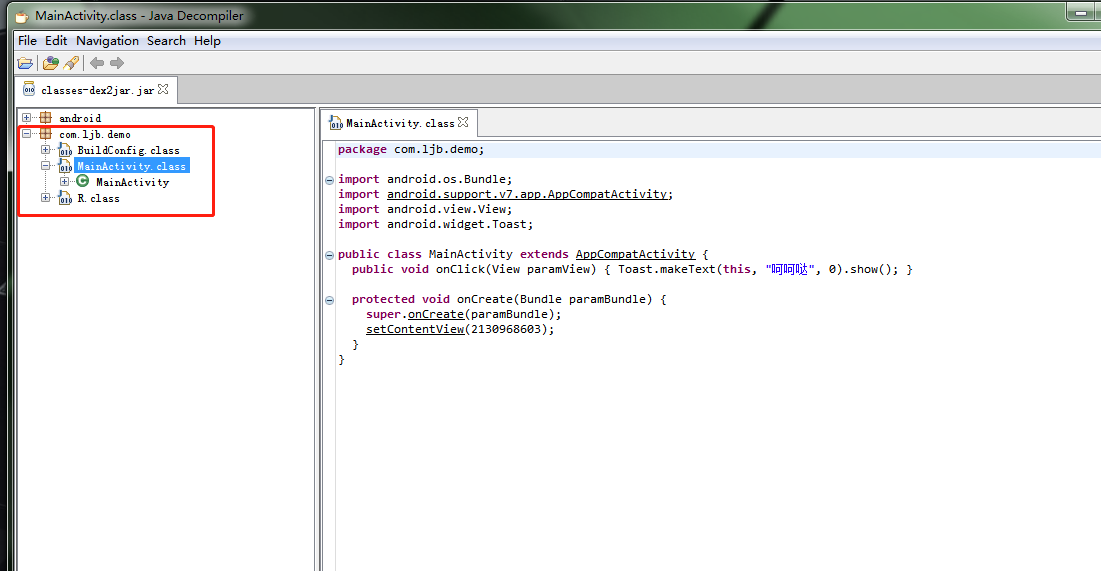


**4、使用gui查看反编译后的java源码**

双击jd-gui.exe,运行gui，



选择刚刚生成的classes-dex2jar，打开后就可以看到源码（图中的Demo为了容易阅读没有加混淆，正常上线的应用会加混淆来加大阅读难度）

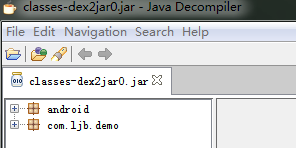


至此，一个没有加壳的apk已经被反编译完成了。

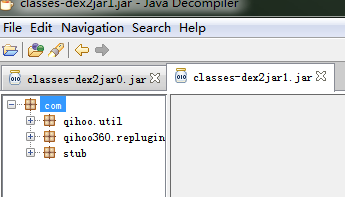
二、脱壳

实际工作中，上线的apk包大多数都会进行加固，有些应用市场甚至后要求加固，例如360，应用宝等，下面会介绍一中常见的脱壳技术。

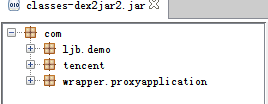
加固后的apk在通过以上的反编译流程后，无法得到正常的java源码，如下图



未加固



360加固保



乐加固

从上图可以看出，经过加固后的apk，通过常规方法反编译无法获取到源码。

**1、脱壳用到的工具**

[FDex2](https://links.jianshu.com/go?to=https%3A%2F%2Fbbs.pediy.com%2Fthread-224105.htm) ：通过Hook ClassLoader的loadClass方法，反射调用getDex方法取得Dex([com.android.dex.De](http://com.android.dex.De)x类对象)，再将里面的dex写出。

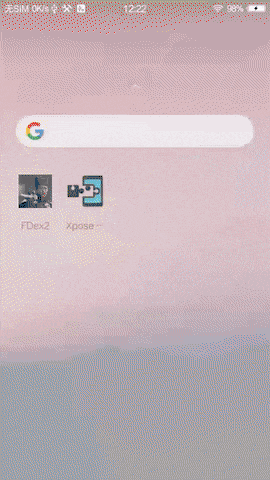
[VirtualXposed](https://links.jianshu.com/go?to=https%3A%2F%2Fvxposed.com%2F)：无需root手机即可使用的xp框架。

**2、脱壳**

Step1、将 【VirtualXposed】、【FDex2】和需要脱壳的apk都安装到手机上 Step2、启动【VirtualXposed】，并在【VirtualXposed】中安装【FDex2】：

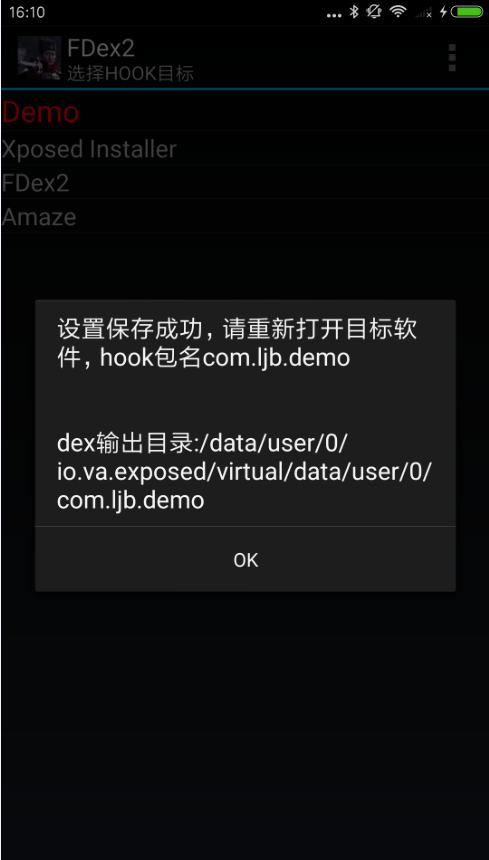


Step3、在【VirtualXposed】中激活【FDex2】:



Step4、在【VirtualXposed】中安装要脱壳的应用，方法和Step2一样。

Step5:启动【VirtualXposed】中的【FDex2】，并配置要脱壳的应用。



Step6：在【VirtualXposed】中运行要脱壳的应用。

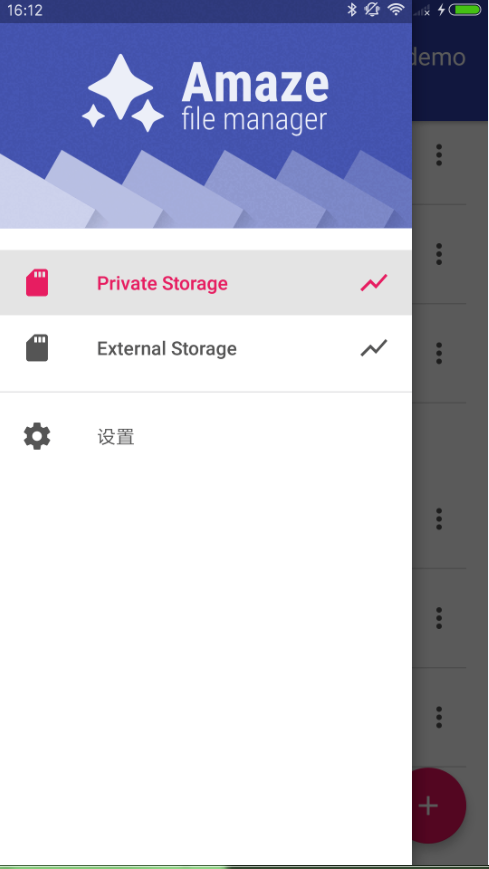
Step7：在上【VirtualXposed】安装文件管理器，方便将生成的dex文件导出 在【VirtualXposed】选中【高级设置】

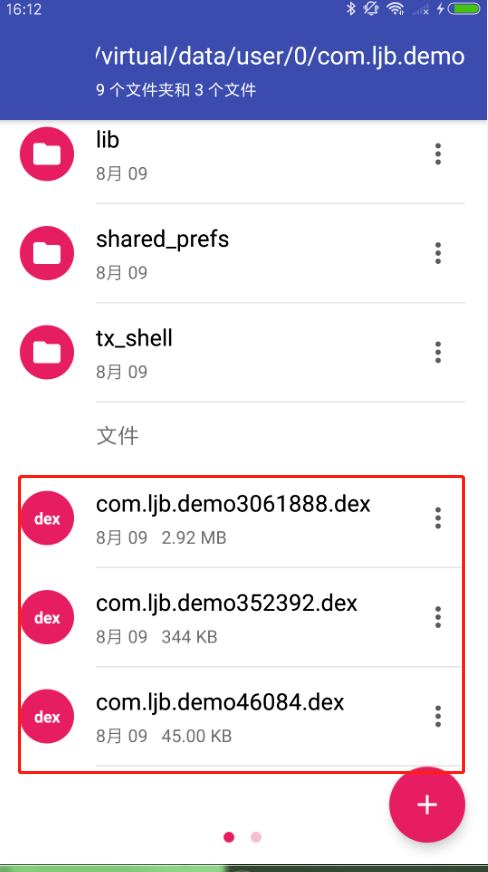


选中【文件管理】，会提示安装【Amaze】文件管理器

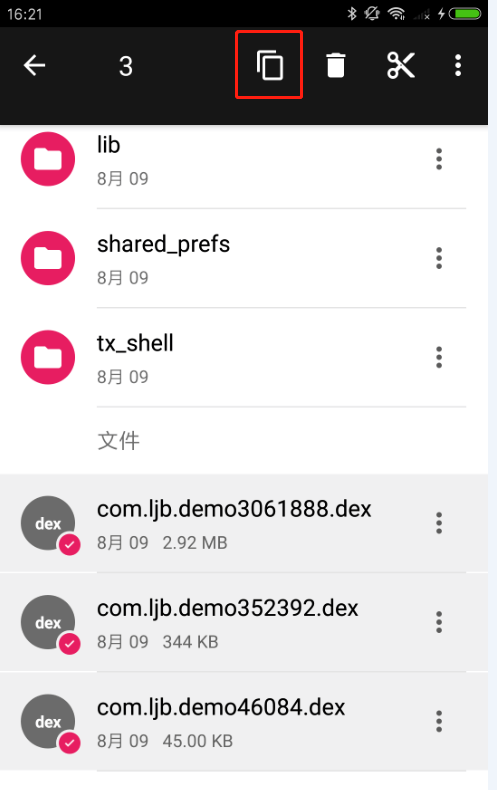


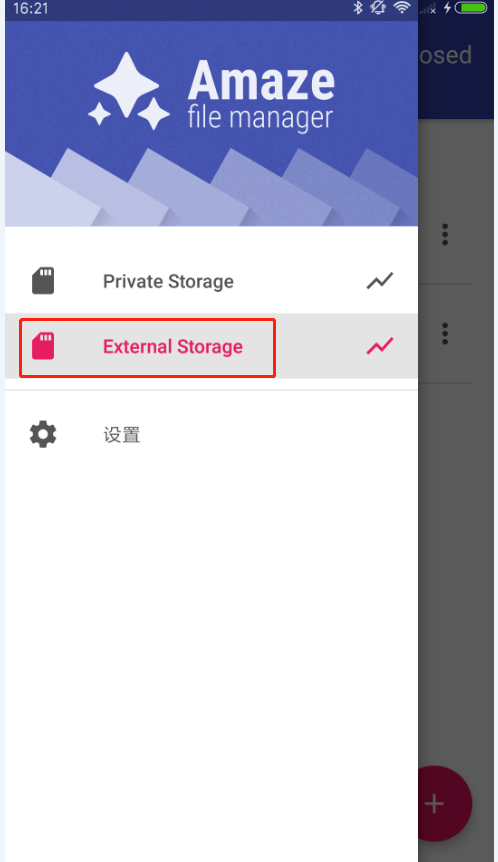
Step8：查看脱壳后的dex文件，打开【Amaze】,选中【Private Storage】，定位到FDex2设置的dex输出路径下，可以看到脱壳后的dex文件

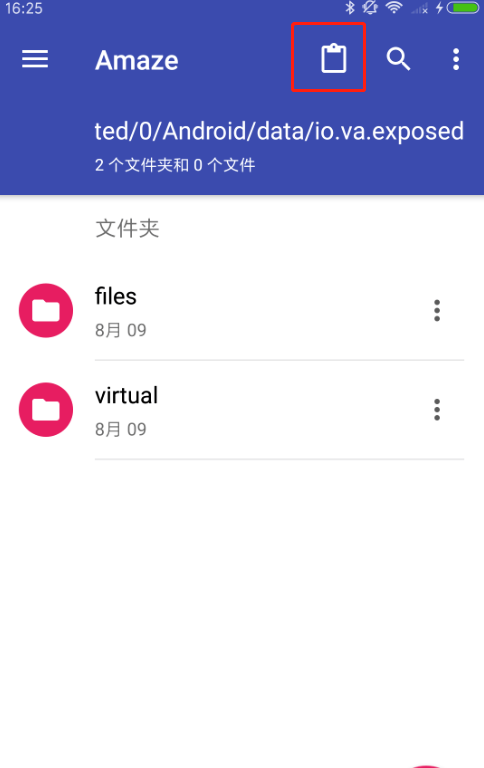




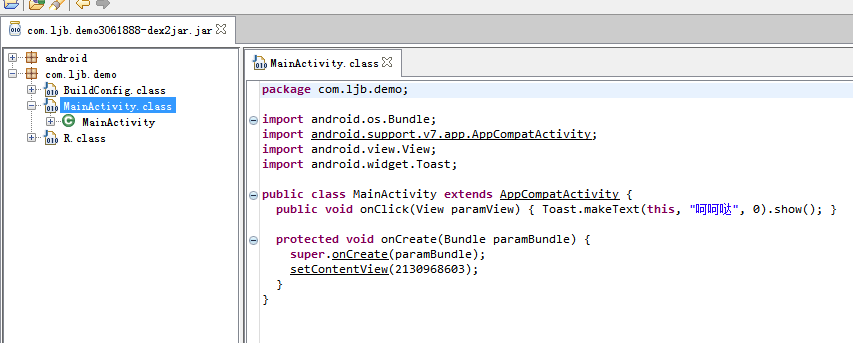
Step9：将dex文件导出：长按dex文件，点击顶部的复制按钮，然后回到选中【External Storage】并选择一个路径，点击顶部的粘贴按钮，将文件粘贴到外部存储，这时，在手机自带的文件管理器中就可以找到刚刚的dex文件了







Step10：通过dex2jar对脱壳的dex文件进行反编译，得到的3个dex文件中，有的是无用的文件，可以依次打开看看，最后可以看到，脱壳后的dex文件被成功反编译后



至此，脱壳完成

源代码和相关工具类已上传码云

[https://gitee.com/xiaobug/XpDemo](https://links.jianshu.com/go?to=https%3A%2F%2Fgitee.com%2Fxiaobug%2FXpDemo) [https://gitee.com/xiaobug/reverse\_tool](https://links.jianshu.com/go?to=https%3A%2F%2Fgitee.com%2Fxiaobug%2Freverse_tool)

本文出处:

<https://www.jianshu.com/p/dbe579f6cc84>

参考链接，

1、[APK反编译](https://links.jianshu.com/go?to=https%3A%2F%2Fblog.csdn.net%2Fs13383754499%2Farticle%2Fdetails%2F78914592)

2、[Android APK脱壳--腾讯乐固、360加固一键脱壳](https://www.jianshu.com/p/138c9de2c987)

3、[【Xposed模块开发入门】](https://links.jianshu.com/go?to=https%3A%2F%2Fblog.csdn.net%2Fmrglaucusss%2Farticle%2Fdetails%2F50963542)

4、[Xposed 热更新（干货，建议收藏）](https://www.jianshu.com/p/360edca021bb)

5、[android apk编译打包过程](https://links.jianshu.com/go?to=https%3A%2F%2Fblog.csdn.net%2Fbrycegao321%2Farticle%2Fdetails%2F79127159)

6、[Android工程师，如何简单高效的学会smali语法](https://www.jianshu.com/p/b23782460f61)

7、[使用baksmali及smali修改apk并打包](https://links.jianshu.com/go?to=https%3A%2F%2Fblog.csdn.net%2FMoonDroid%2Farticle%2Fdetails%2F44224111)

8、[MT管理器](https://links.jianshu.com/go?to=http%3A%2F%2Fbinmt.cc%2Fdoc%2Findex.php%3Fs%3D%2F1%26page_id%3D1)

9、[Oo0代码混淆实现方法](https://links.jianshu.com/go?to=https%3A%2F%2Fmp.weixin.qq.com%2Fs%2FT8CFMjQ5_te1fIHzwzTpUg)

10、[修改AndroidStudio混淆配置文件](https://links.jianshu.com/go?to=https%3A%2F%2Fblog.csdn.net%2Fu014476720%2Farticle%2Fdetails%2F85112374)