1、将手机root；如果手机不root，关闭不了SELinux，IDA如果附加进程调试，则看不到运行的进程。

2、关闭SELinux

adb shell getenforce

adb shell setenforce 0 //设置成permissive 模式

adb shell setenforce 1 //设置成enforce 模式

注意此方法重启后失效

3、将IDA安装目录下的dbgsrv/android\_server拷贝到手机中，修改文件权限

adb push android\_server /data/local/tmp

adb shell chmod 777 /data/local/tmp/android\_server

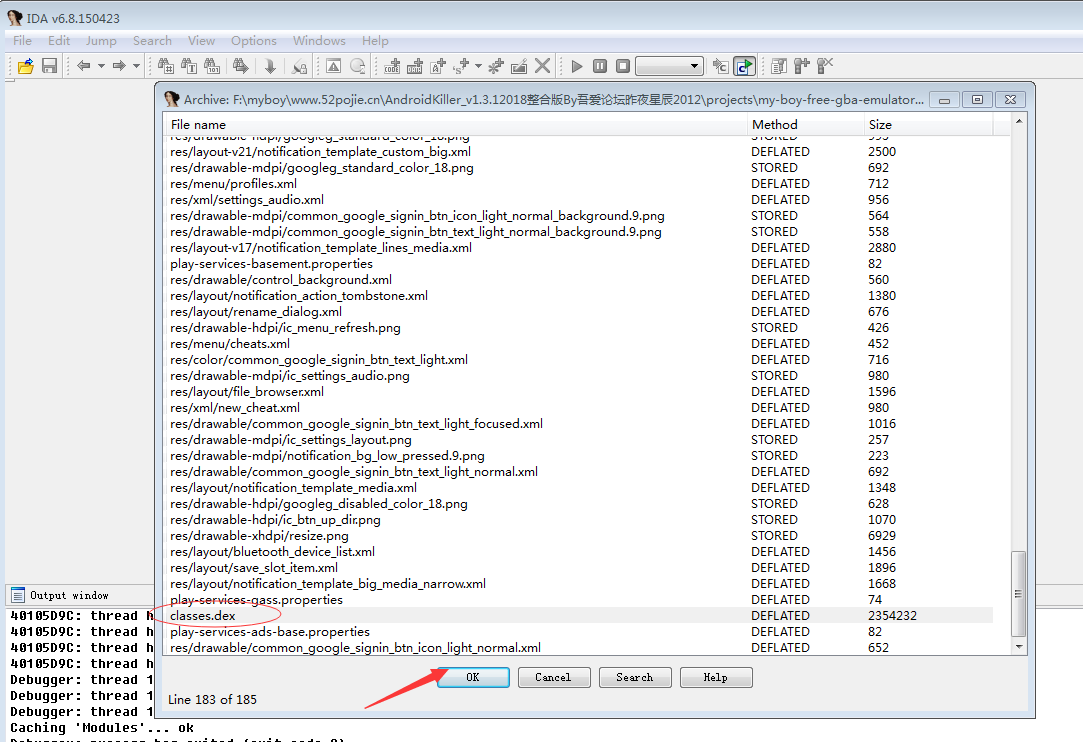
4、安装添加了android:debuggable="true"属性的apk到手机

在AndroidManifest.xml的application中添加android:debuggable="true"。

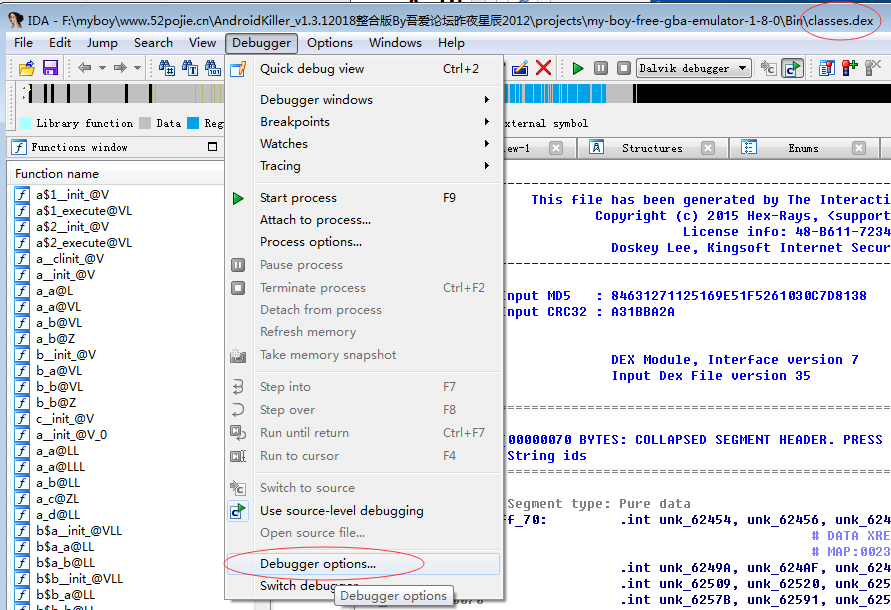
adb install my-boy-free-gba-emulator-1-8-0\_killer.apk

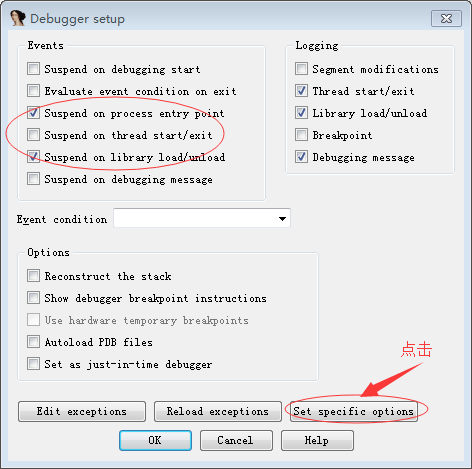
注意：使用的是Android\_killer v1.3.1.0对原apk进行反编译，注意bin/apktool/apktool/ShakaApktool.jar要是最新的，不然反编译会失败。

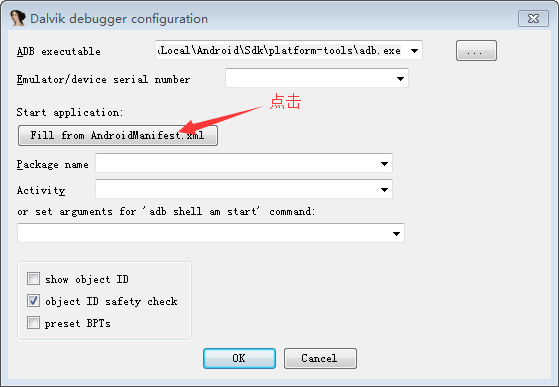
5、将反编译后的apk拖到IDA中，选择class.dex



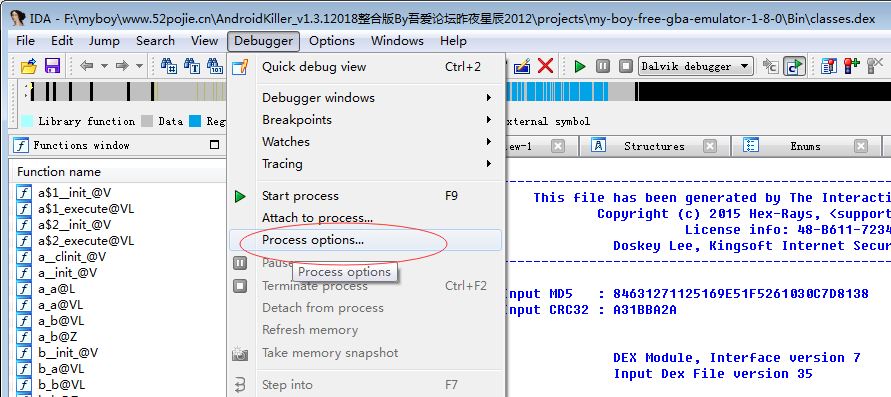
6、设置debug选项

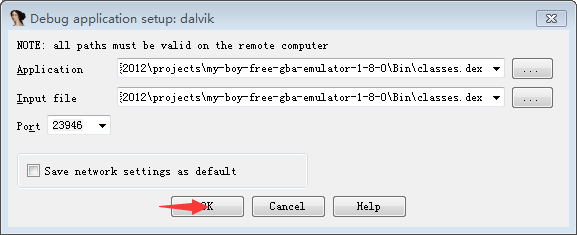






7、设置进程选项





8、启动android\_server



9、运行IDA

