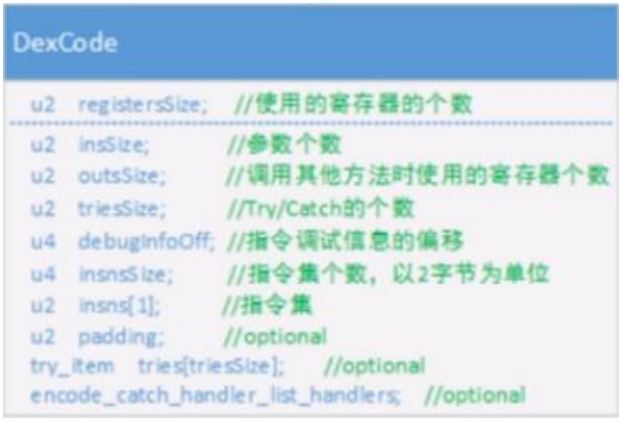
1. **classes.dex**

DexClassDef -> DexClassData -> DexMethod -> DexCode



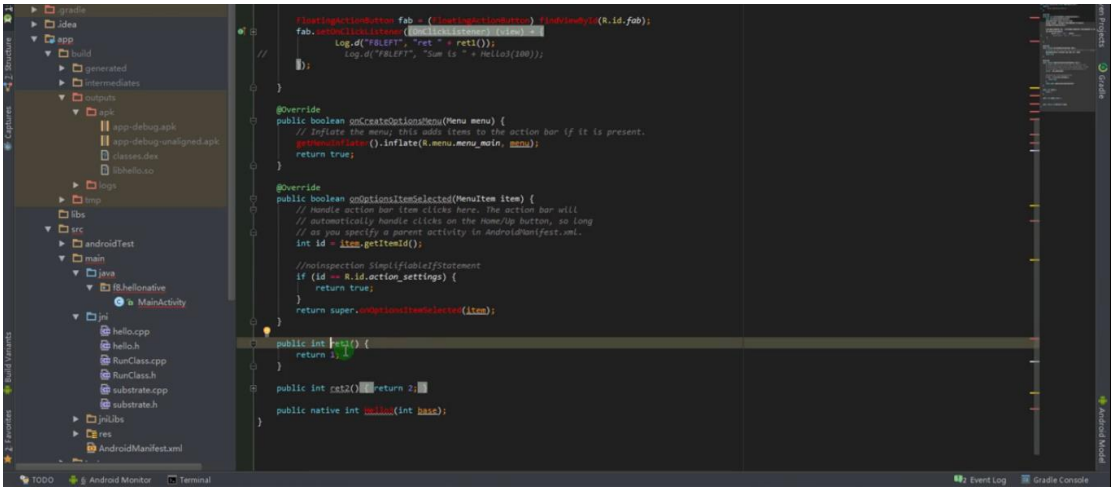
里面的 u2 insns 的值便是用于存放程序实现代码的地方。

程序执行时候会把整个 dex 文件加载到内存中，然后动态地解析执行 insns 中的内容。

只要修改了里面的数据，就相当于修改了程序执行流程和方法。

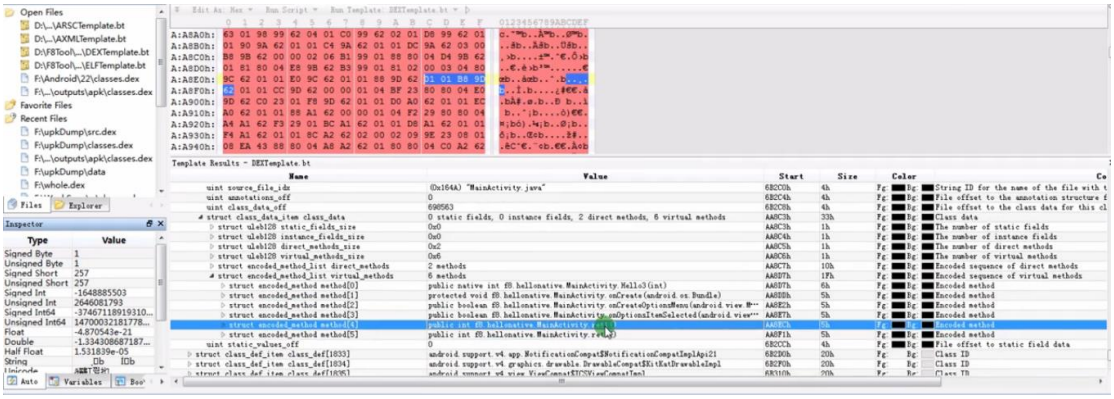
2. **内存中修改 insns**

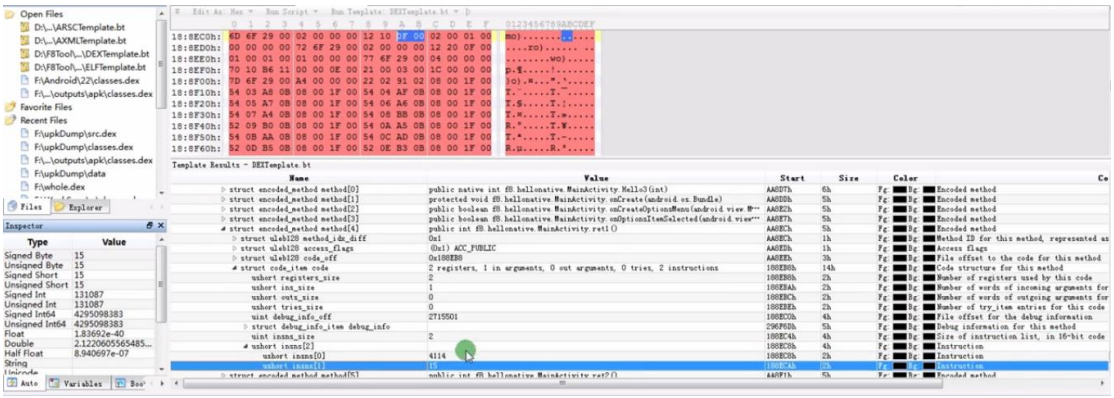
1) 定位到 dex 文件
2) 计算函数的 DexCode 位置
3) 重写 DexCode 的 insns 数据



原始程序返回结果 1

找到 classes.dex 文件中 ret1()的位置





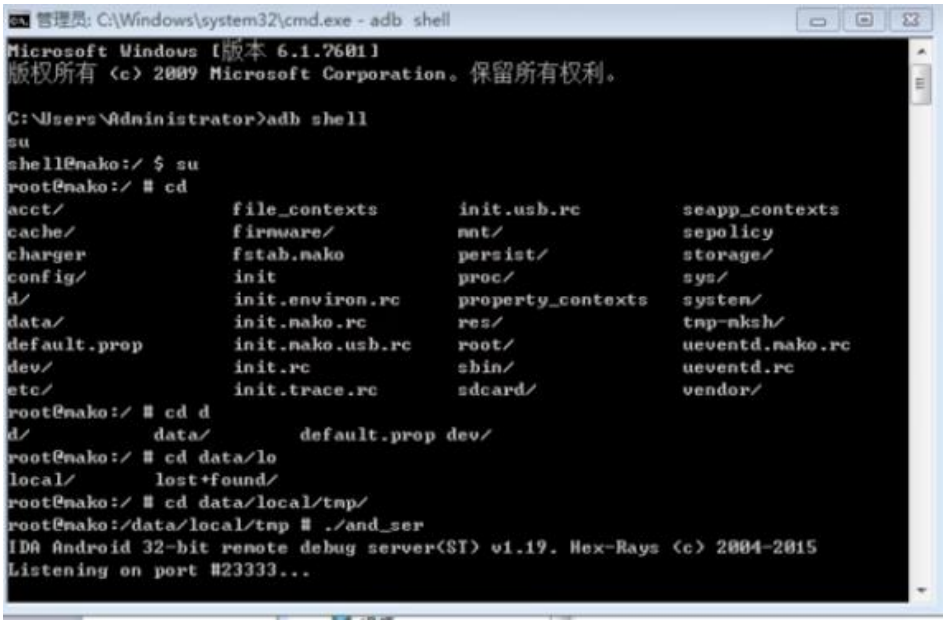
就是将 1210 改为 1220

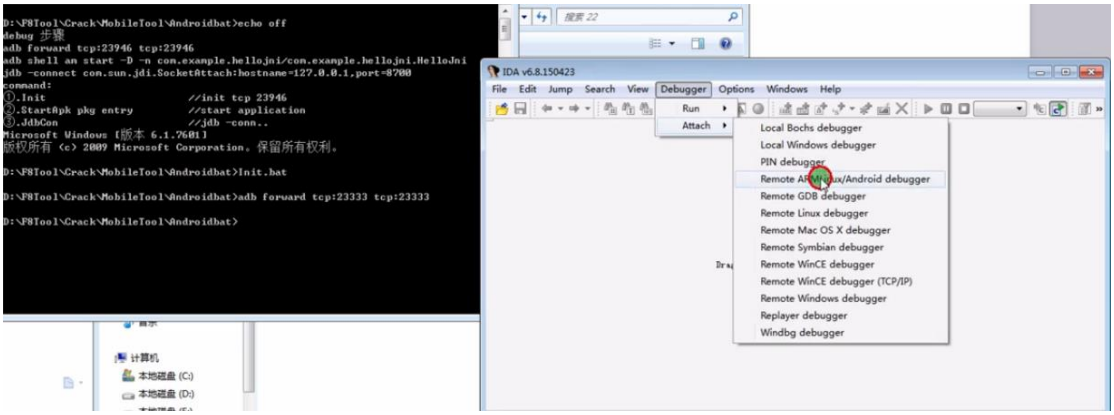
3. ida 中动态修改

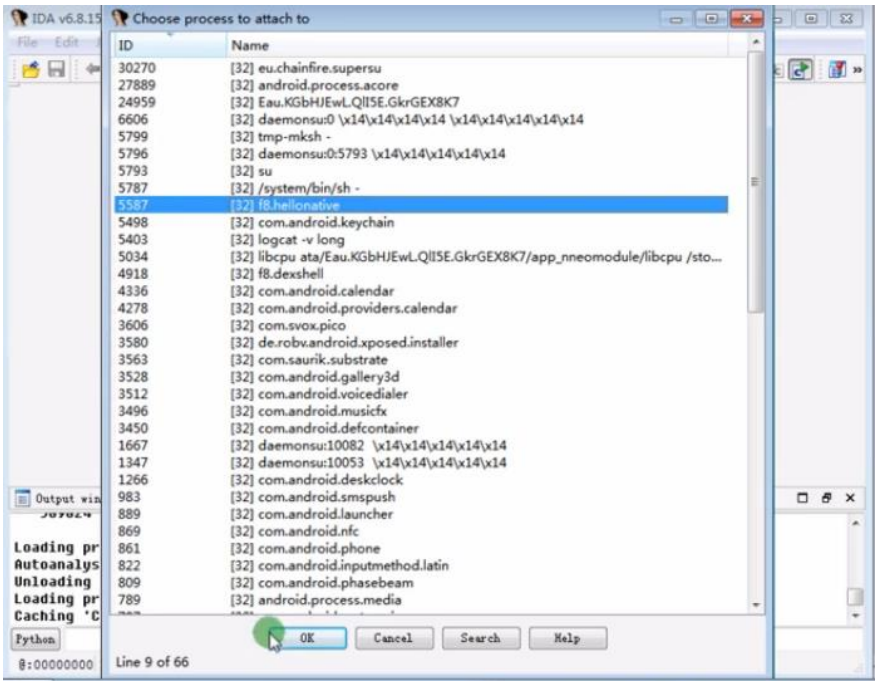
Ctrl + S 打开 map 数据

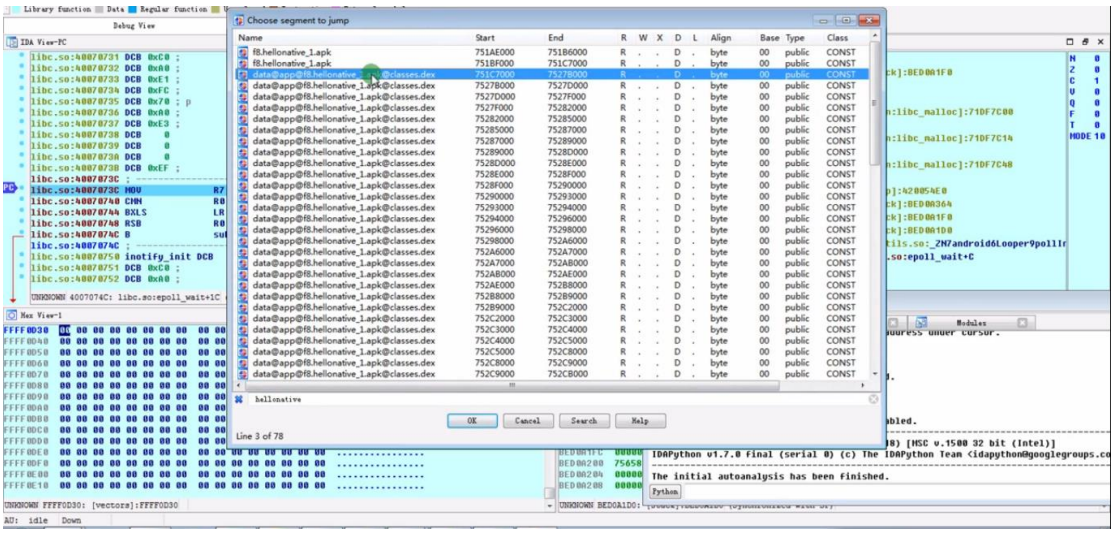
查找内存加载的 classes.dex 的位置

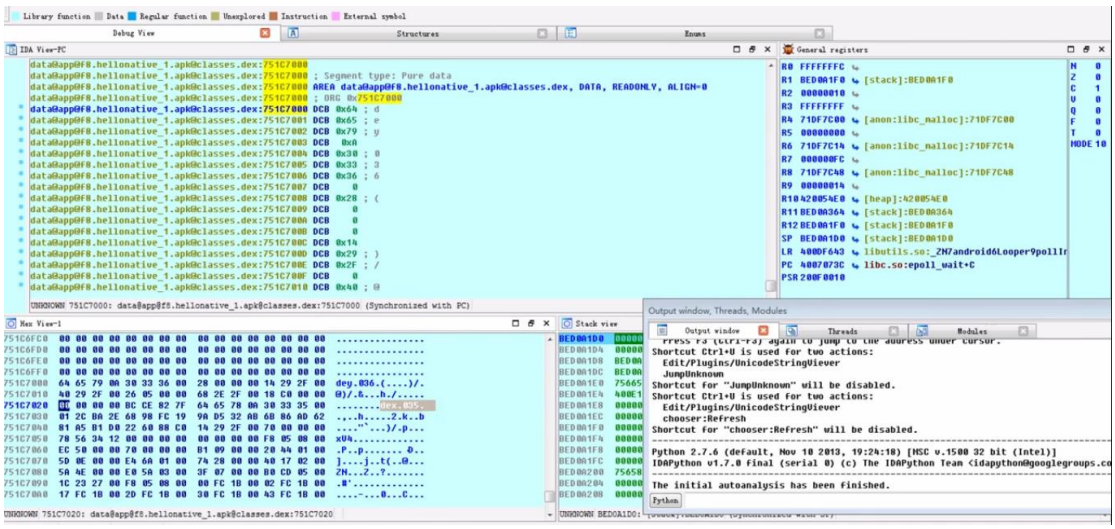
直接计算偏移，修改相应的位置

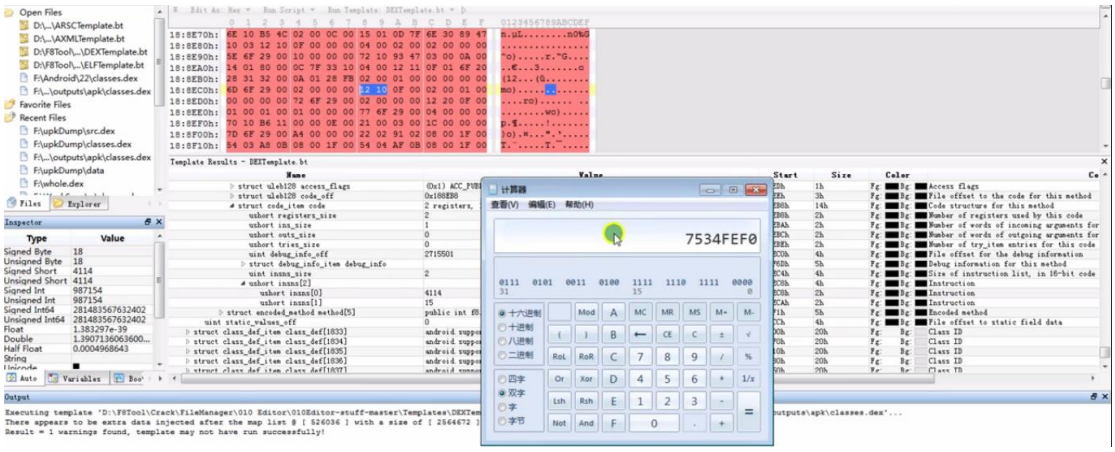


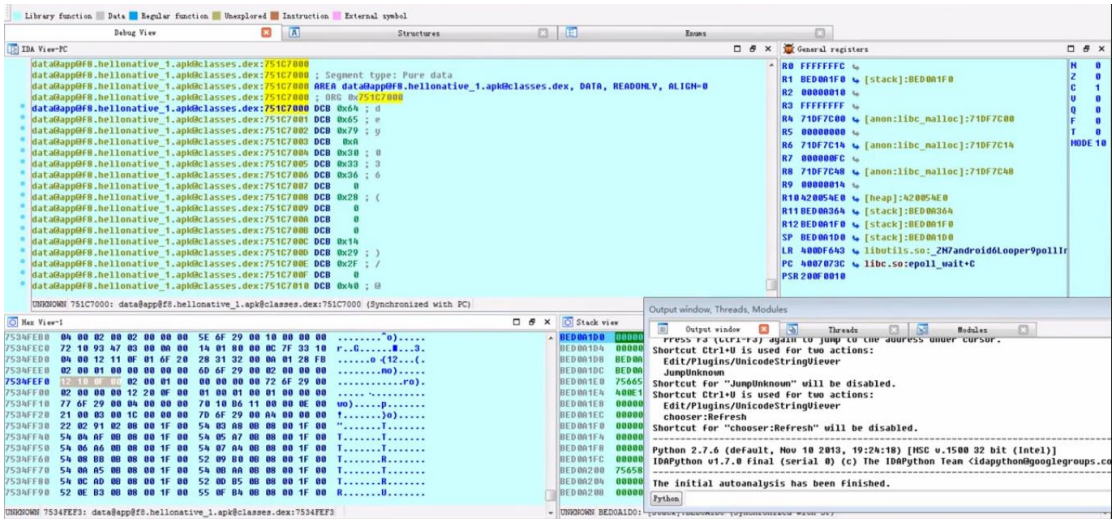

D:\F8Tool\Crack\MobileTool\Androidbat>echo off
debug 步骤
adb forward tcp:23946 tcp:23946
adb shell am start -D -n com.example.hellojni/com.example.hellojni.HelloJni
jdb -connect com.sun.jdi.SocketAttach:hostname=127.0.0.1,port=8700
command:
①.Init //init tcp 23946
②.StartApk pkg entry //start application
③.JdbCon //jdb -conn..
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
D:\F8Tool\Crack\MobileTool\Androidbat>Init.bat
D:\F8Tool\Crack\MobileTool\Androidbat>adb forward tcp:23333 tcp:23333
D:\F8Tool\Crack\MobileTool\Androidbat>
IDA v6.8.150423
File Edit Jump Search View Debugger Options Windows Help
Run
Attach
Local Bochs debugger
Local Windows debugger
PIN debugger
Remote ARM Linux/Android debugger
Remote GDB debugger
Remote Linux debugger
Remote Mac OS X debugger
Remote Symbian debugger
Remote WinCE debugger
Remote WinCE debugger (TCP/IP)
Remote Windows debugger
Replayer debugger
Windbg debugger

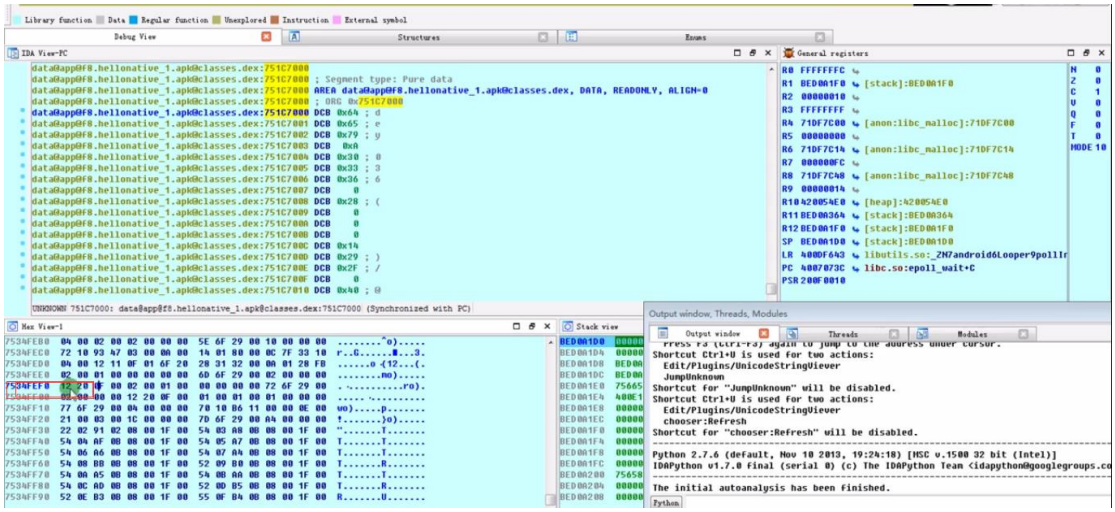

Choose process to attach to
ID Name
30270 [32] eu.chainfire.supersu
27889 [32] android.process.acore
24959 [32] Eau.KGbHJEwL.QII5E.GkrGEX8K7
6606 [32] daemonsu:0 \x14\x14\x14\x14 \x14\x14\x14\x14\x14\x14
5799 [32] tmp-mksh -
5796 [32] daemonsu:0:5793 \x14\x14\x14\x14\x14\x14
5793 [32] su
5787 [32] /system/bin/sh -
5587 [32] f8.hellonative
5498 [32] com.android.keychain
5403 [32] logcat -v long
5034 [32] libcpu ata/Eau.KGbHJEwL.QII5E.GkrGEX8K7/app_nneomodule/libcpu /sto...
4918 [32] f8.dexshell
4336 [32] com.android.calendar
4278 [32] com.android.providers.calendar
3606 [32] com.svox.pico
3580 [32] de.robv.android.xposed.installer
3563 [32] com.saurik.substrate
3528 [32] com.android.gallery3d
3512 [32] com.android.voicedialer
3496 [32] com.android.musicfx
3450 [32] com.android.defcontainer
1667 [32] daemonsu:10082 \x14\x14\x14\x14\x14\x14
1347 [32] daemonsu:10053 \x14\x14\x14\x14\x14\x14
1266 [32] com.android.deskclock
983 [32] com.android.smspush
889 [32] com.android.launcher
869 [32] com.android.nfc
861 [32] com.android.phone
822 [32] com.android.inputmethod.latin
809 [32] com.android.phasebeam
789 [32] android.process.media
OK Cancel Search Help
Line 9 of 66
Python

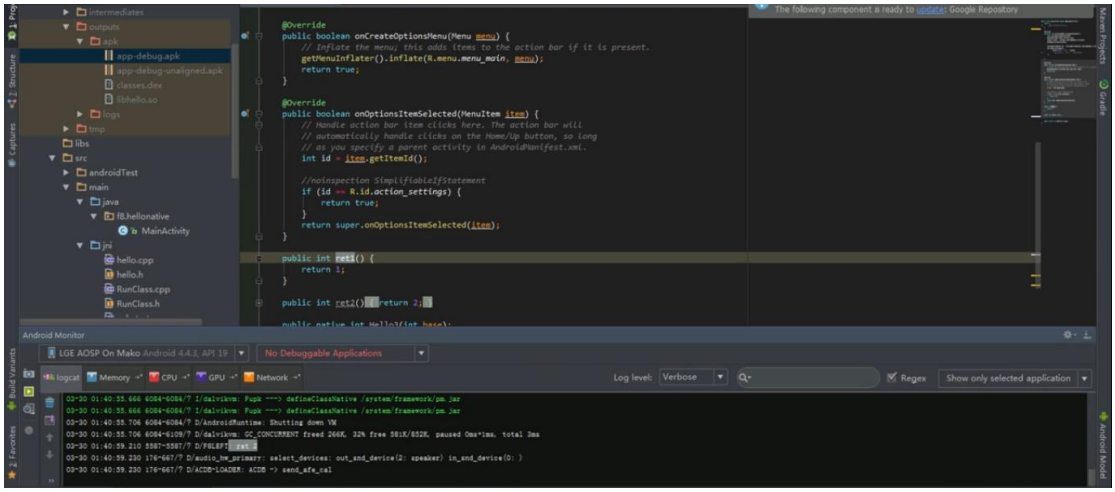

Choose segment to jump
Name Start End R W X D L Align Base Type Class
f8.hellonative_1.apk 751AE000 751B6000 byte 00 public CONST
f8.hellonative_1.apk 751BF000 751C7000 byte 00 public CONST
data@app@f8.hellonative_1.apk@classes.dex 751C7000 7527B000 byte 00 public CONST
OK Cancel Search Help
Line 3 of 78
IDAPython v1.7.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.co
The initial autoanalysis has been finished.
Python











修改生效