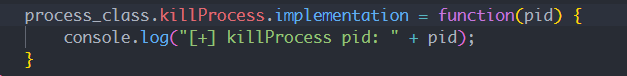
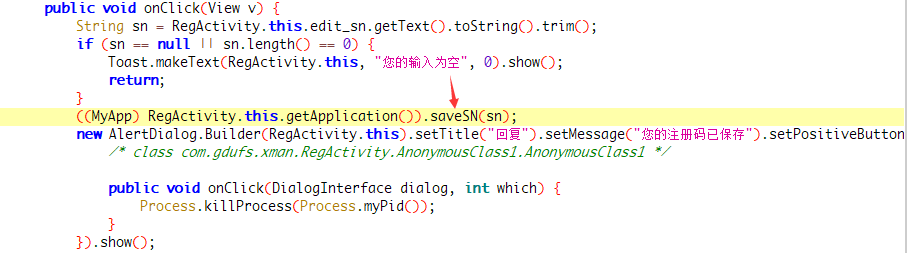
目的： 拿flag

1. 有killprocess，先把这个函数干掉



1. 看下主要的注册函数，在native层





1. 进入n2

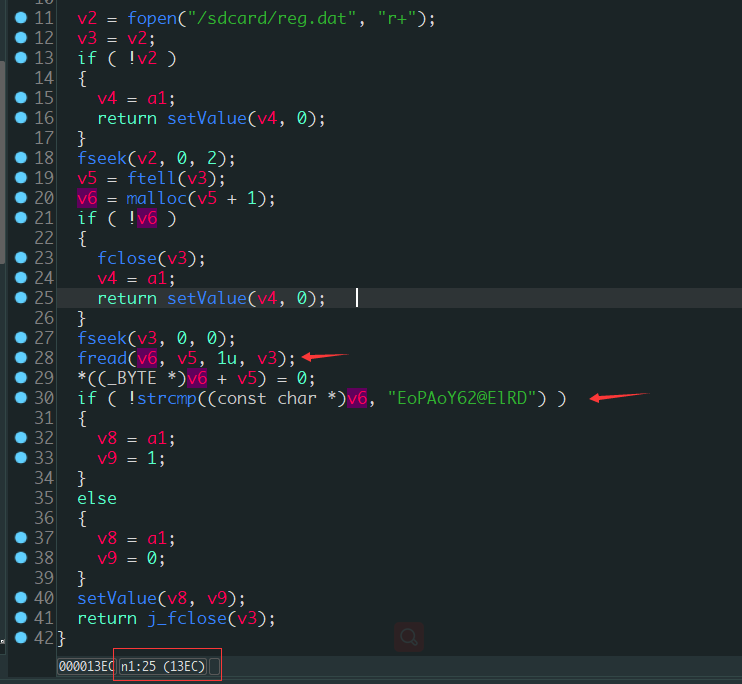


1. saveSN是把输入串处理之后保存在/sdcard/reg.dat文件中，那么说明，肯定还要一个函数去判断这个reg.dat文件内容是否正确。根据这个线索整理一下这个app的流程



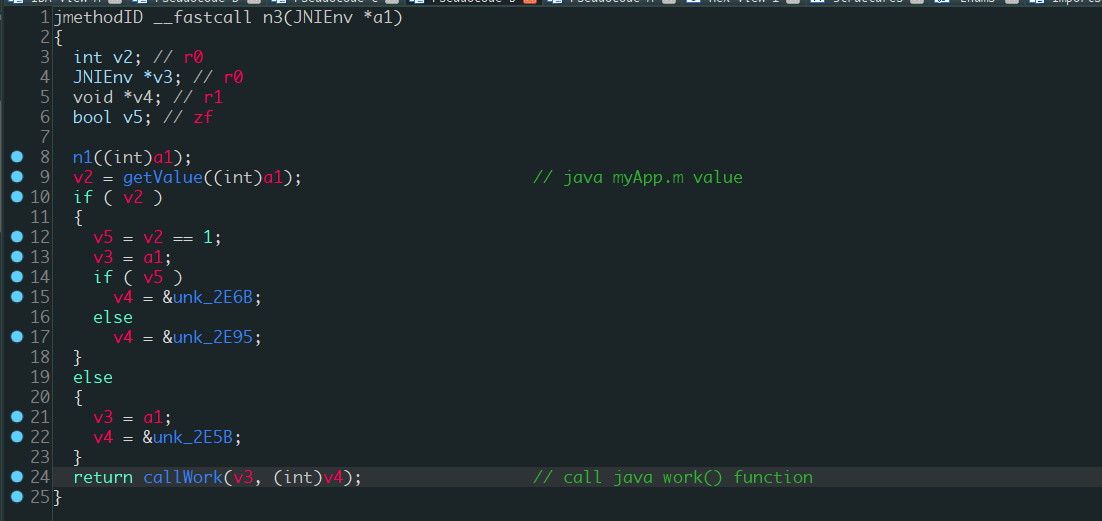
启动initSN() -> doRegister()调用saveSN ->work()对workString赋值，通过Toast显示出flag

initSN(n1)读取文件，与字符串进行对比

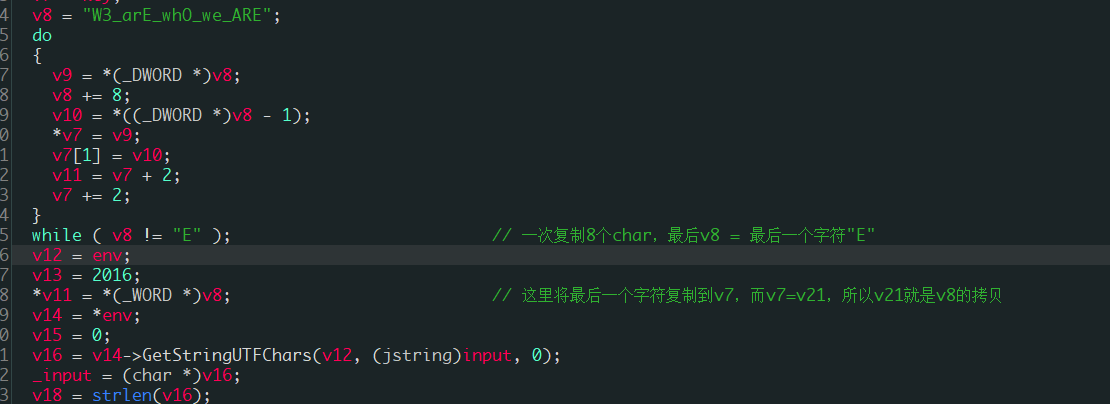


saveSN（n2）写文件，并进行处理

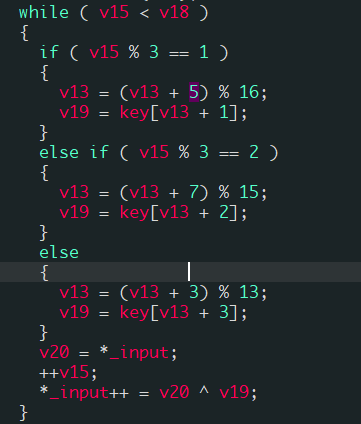
work（n3）



1. 我们的输入就是要和"W3\_arE\_whO\_we\_ARE"进行在n2中的一系列计算之后，得到” EoPAoY62@ElRD”

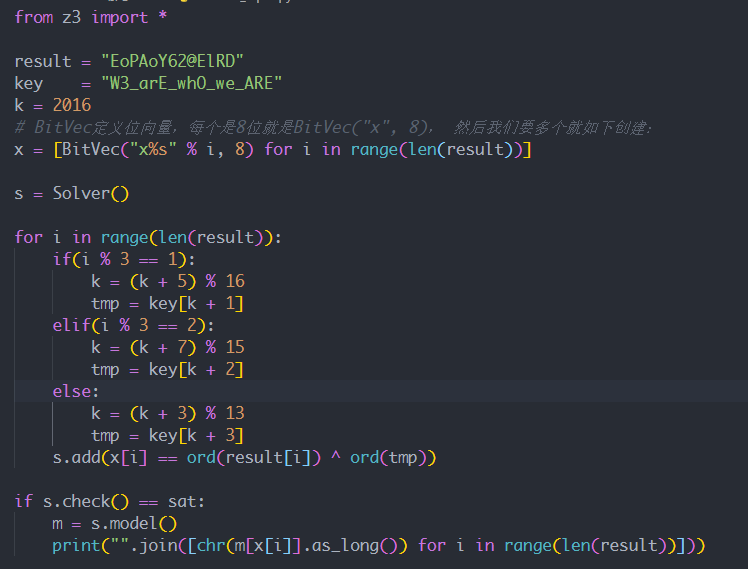


需要还原的算法：



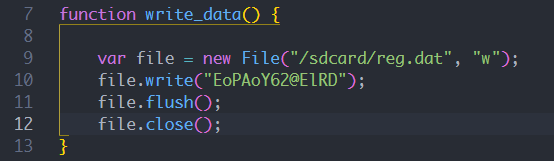
我们用z3-solver来解，这个东西说的通俗易懂就是不用逆向求解，把我们需要求解的设为x，之后解当成就好。

<https://blog.shi1011.cn/learn/1789>



最后结果：201608Am!2333

1. 这个apk其实很多问题，首先用pixel4动态调试和frida hook时会遇到问题，后来没办法用了nexus5，然后是读写文件，只是在清单中申请权限，这个方法只在android早期能有权限读取文件，后来为了调试，直接在ida中patch的内存改了跳转
2. 练习frida的api，使用frida API写文件，使用时需要获取存储空间权限



1. Frida使用c的api写文件



1. 判断dlopen加载对应的so后，进行inline hook

