# 实验过程

工具：AndroidKiller、安卓模拟器（我用的是夜神）

理论基础：[Smali基本语法](http://www.cnblogs.com/lee0oo0/p/3728271.html)

|  |  |
| --- | --- |
| .field private isFlag:z | 定义变量 |
| .method | 方法 |
| .parameter | 方法参数 |
| .prologue | 方法开始 |
| .line 12 | 此方法位于第12行 |
| Invoke-super | 调用父函数 |
| const/high16 v0, 0x7fo3 | 把0x7fo3赋值给v0 |
| invoke-direct | 调用函数 |
| return-void | 函数返回void |
| .end method | 函数结束 |
| new-instance | 创建实例 |
| iput-object | 对象赋值 |
| iget-object | 调用对象 |
| invoke-static | 调用静态函数 |

|  |  |
| --- | --- |
| if-eq vA, vB, :cond\_\*\* | 如果vA等于vB则跳转到:cond\_\*\* |
| if-ne | 不等于 |
| if-lt | 小于 |
| if-ge | 大于等于 |
| if-gt | 大于 |
| if-le | 小于等于 |
| if-eqz vA, :cond\_\*\*" | 如果vA等于0则跳转到:cond\_\*\* |
| if-nez | 不等于0 |
| if-ltz | 小于0 |
| if-gez | 大于等于0 |
| if-gtz | 大于0 |
| if-lez | 小于等于0 |

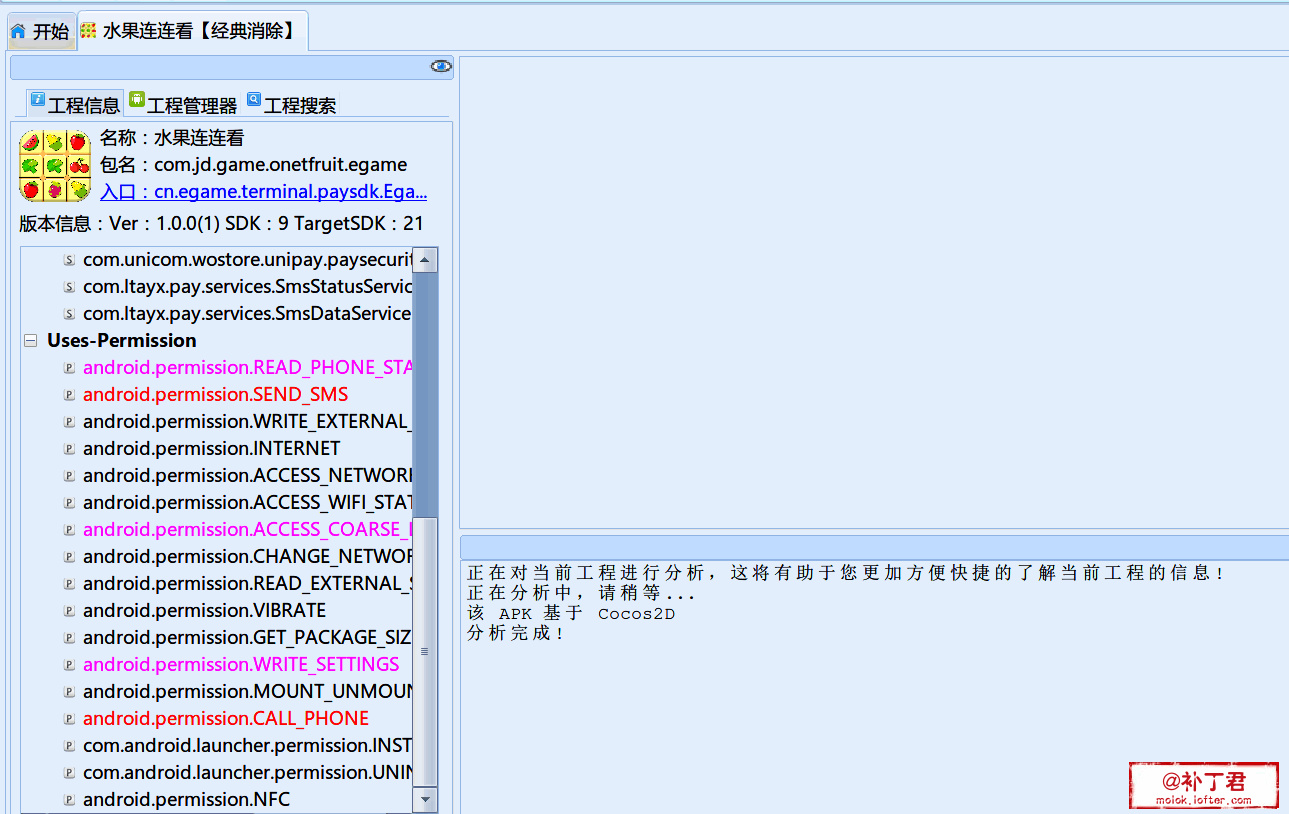
## 第一步：查壳



本次实验对象是无壳无加密的。

## 第二步：反编译

使用Android Killer打开实验对象



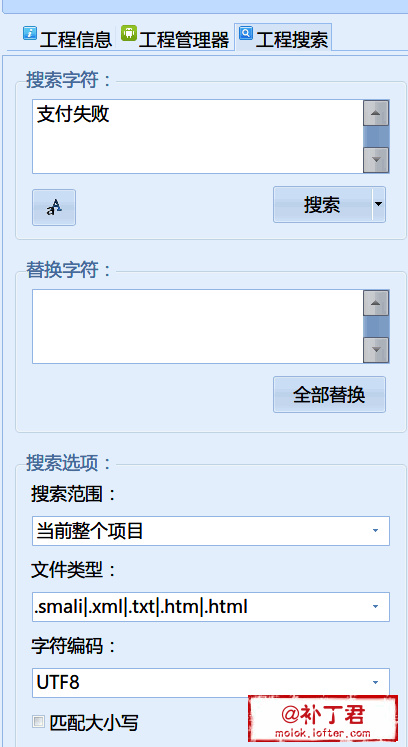
## 第三步：逻辑梳理

将安装包导入模拟器安装，然后点击“礼包”



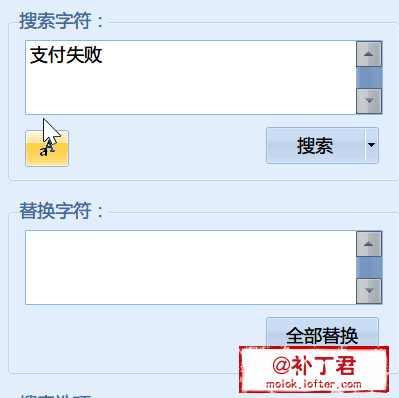
未破解的安装包会提示“支付失败”

那么在“工程搜索”中的关键字就是“支付失败”

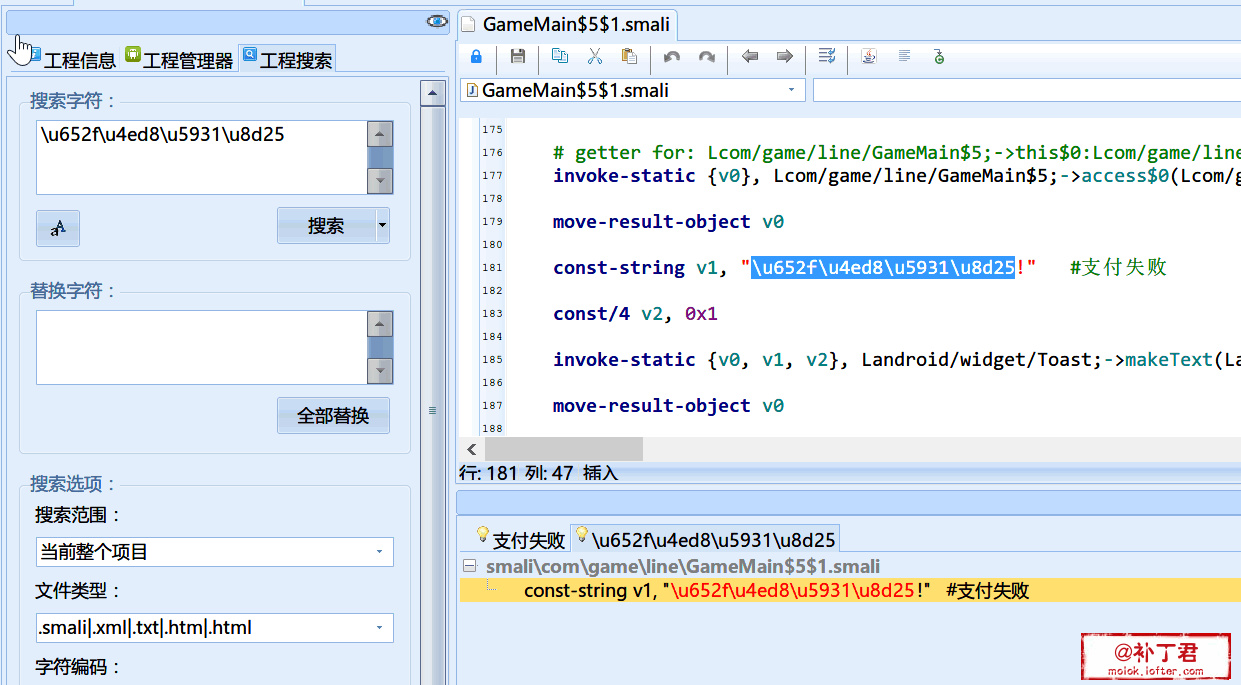


此时点击搜索会提示无结果，原因是源文件里的汉字是unicode编码的

所以，需要将搜索关键字进行转换

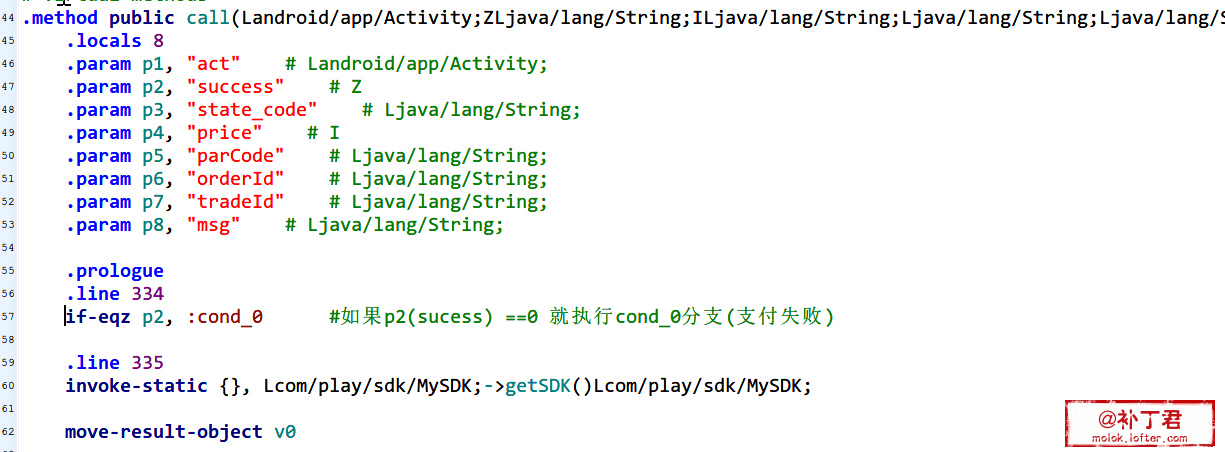


这样就有搜索结果显示出来了



上下大致浏览一遍这个文件的内容

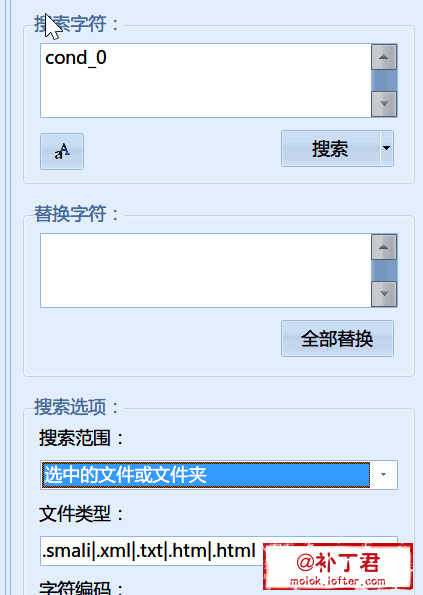
可以发现几条关键语句



.param p2, "success" # 赋值参数p2

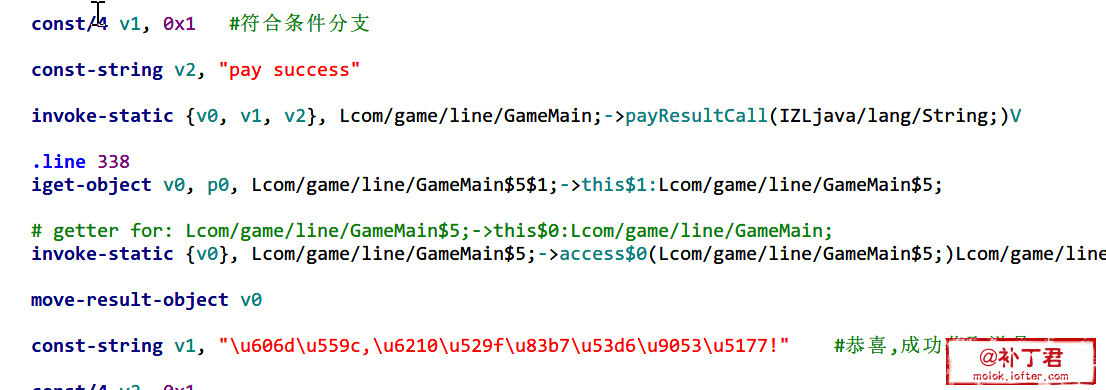
if-eqz p2, :cond\_0 #如果参数p2的值为0，就执行cond\_0分支(支付失败)

那么，cond\_0这个分支在什么地方？还是运用搜索（注意搜索范围）





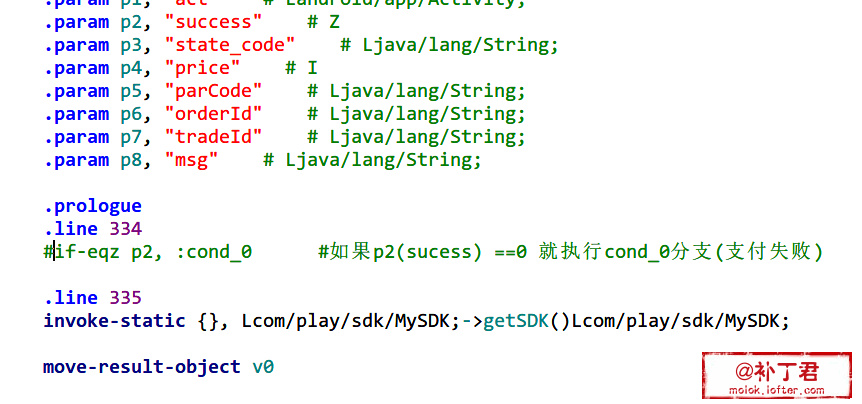
当if判断句不成立的时候，就继续往下执行 [pay success]（成功获取礼包）



## 第四步：破解

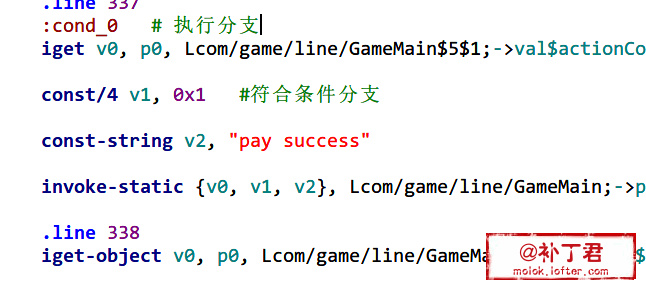
第一招：简单粗暴

直接把判断语句注释，或者删除



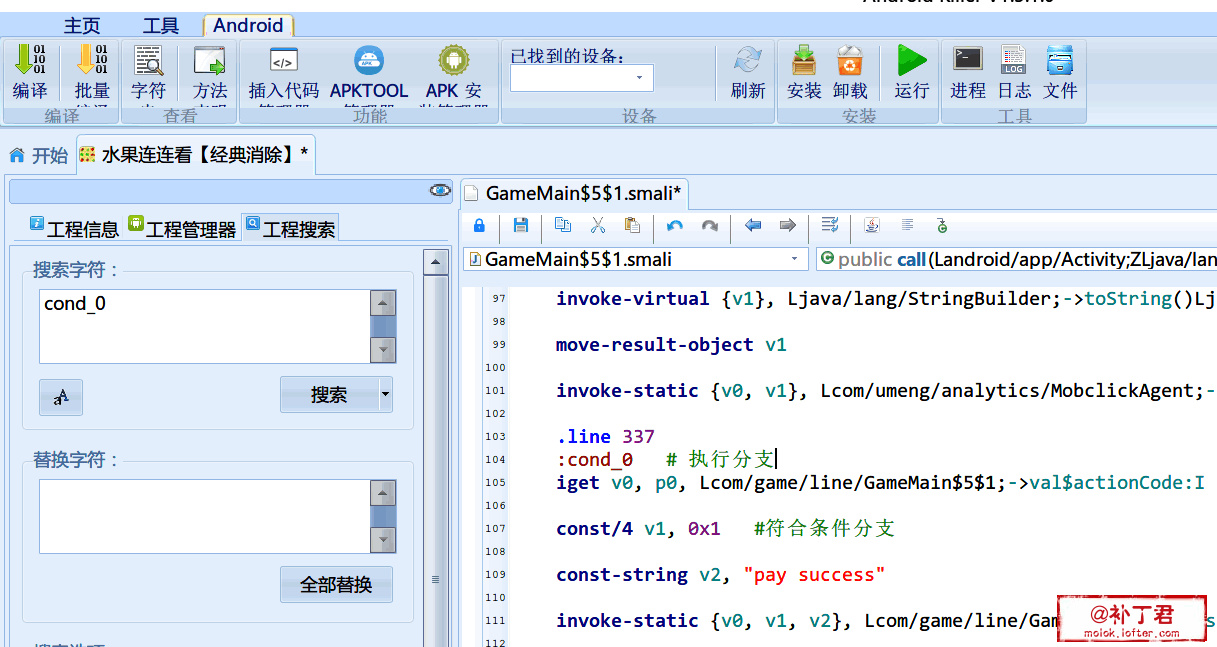
这样没有了判断语句，程序会直接顺序执行下去（成功获取礼包），达到 目的

第二招：修改分支位置



将 :cond\_0 分支点修改在 pay success 之前，就算有判断语句，依旧会执行pay succes，同样可以达到破解目的。

## 第五步：编译APK



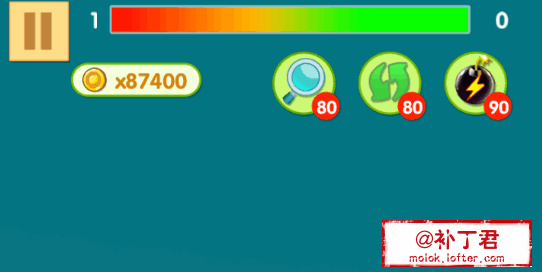
点击左上方 “编译”按钮即可

## 第六步：安装APK

原来安装在模拟器上的原版“水果连连看”需要卸载掉才能安装修改后的APK，因为签名不同。



可以看到破解是成功的，费了点功夫也可以享受破解后的成果了



# 实验样本



# 实验成果



只要肯动手，你也一定可以做到的~

By KK@补丁君