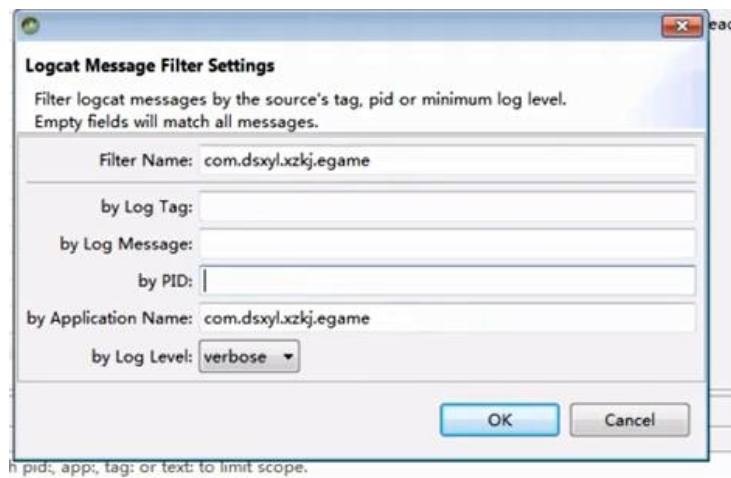


## 内付破解

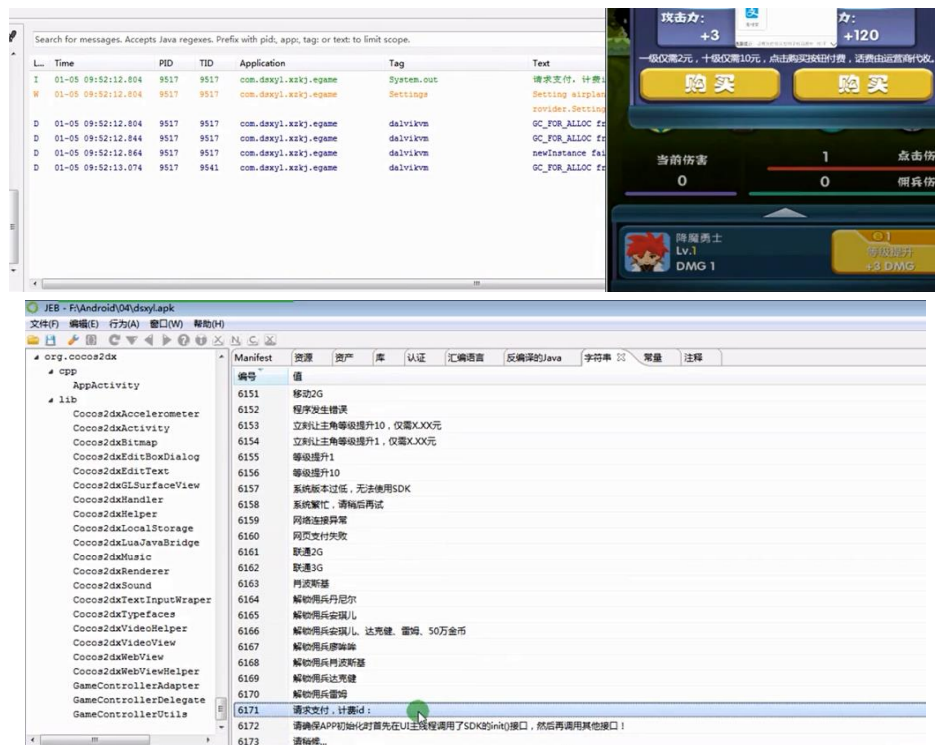
1. 工具: jeb、Android Monitor、Android Killer

2. 步骤:

(1) 通过 Monitor 查看 app 的相关 Log, 根据 app 的 packageName 过滤 Log



(2) 搜索支付操作产生的 Log 中的相关字符串, 根据字符串定位到支付操作代码



```

public void order_internal() {
    Object v9 = this.valueMap.get(Integer.valueOf(this.mOrgID));
    this.mMMID = Long.parseLong(((Map)v9).get("id"));
    System.out.println("请求支付, 计费id: " + this.mMMID);
    this.mOrderID = "orderID-" + SystemClock.elapsedRealtime();
    LSGAVirtualCurrency.onChargeRequest(this.mOrderID, ((Map)v9).get("tradeName"), ((double) (((float) Integer.parseInt(((Map)v9).get("money")) / 1f)), "CNY", ((double) (((float) Integer.parseInt(((Map)v9).get("money")) / 1f)), "爱游戏");
    HashMap v8 = new HashMap();
    v8.put("toolsAlias", ((Map)v9).get("alias"));
    EgamePay.pay(((Activity)this), ((Map)v8), new EgamePayListener() {
        public void payCancel(Map arg3) {
            AppCompatActivity.onActivityResult(AppCompatActivity.this.mOrgID, -1);
        }

        public void payFailed(Map arg3, int arg1) {
            AppCompatActivity.onActivityResult(AppCompatActivity.this.mOrgID, -1);
        }

        public void paySuccess(Map arg3) {
            AppCompatActivity.onActivityResult(AppCompatActivity.this.mOrgID, 0);
        }
    });
}

```

(3)可以看出当 onActivityResult 第二个参数为 0 时，支付成功。定位到 onActivityResult 函数的位置

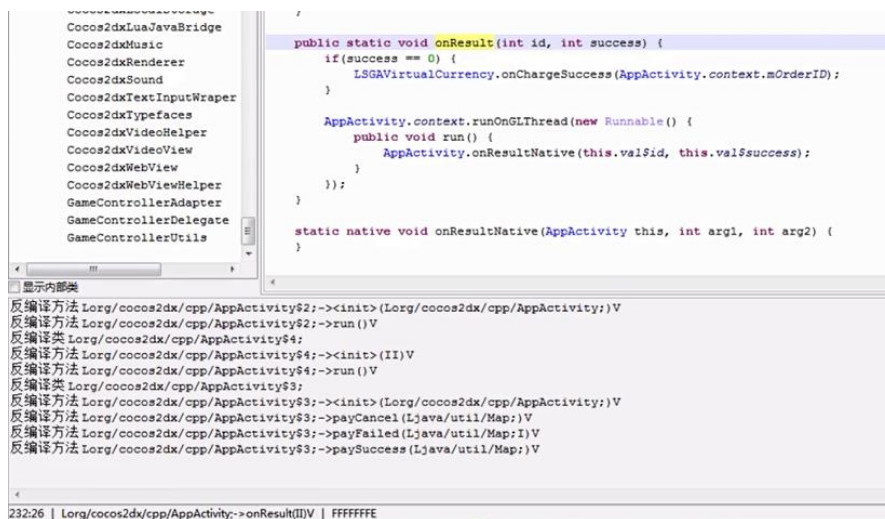
```

public static void onActivityResult(int id, int success) {
    if(success == 0) {
        LSGAVirtualCurrency.onChargeSuccess(AppCompatActivity.context.mOrderID);
    }

    AppCompatActivity.context.runOnUiThread(new Runnable() {
        public void run() {
            AppCompatActivity.onActivityResultNative(this.val$id, this.val$success);
        }
    });
}

```

修改 success==0 的跳转或者使得 success 恒等于 0

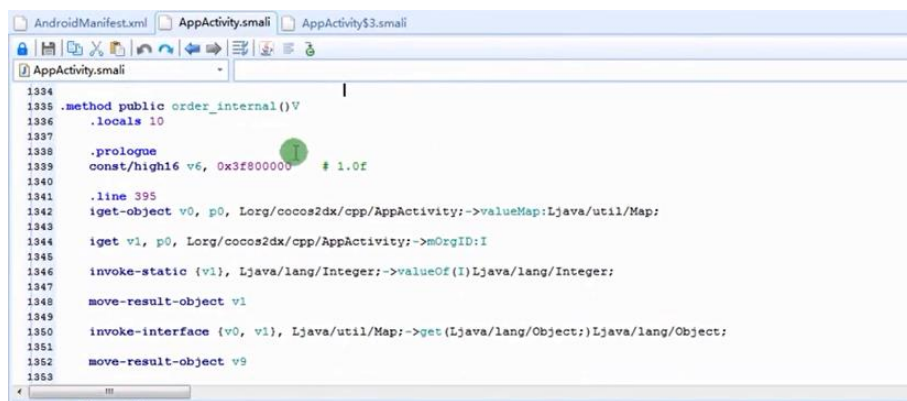


可以在最下面看到 onActivityResult 函数所在的文件位置

(4)在 smali 文件中对 success 参数的值进行修改，使该参数恒等于 0







```
1334
1335 .method public order_internal()V
1336 .locals 10
1337
1338 .prologue
1339 const/high16 v6, 0x3f800000 # 1.0f
1340
1341 .line 395
1342 iget-object v0, p0, Lorg/cocos2dx/cpp/AppActivity;->valueMap:Ljava/util/Map;
1343
1344 iget v1, p0, Lorg/cocos2dx/cpp/AppActivity;->mOrgID:I
1345
1346 invoke-static {v1}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;
1347
1348 move-result-object v1
1349
1350 invoke-interface {v0, v1}, Ljava/util/Map;->get(Ljava/lang/Object;)Ljava/lang/Object;
1351
1352 move-result-object v9
1353
```

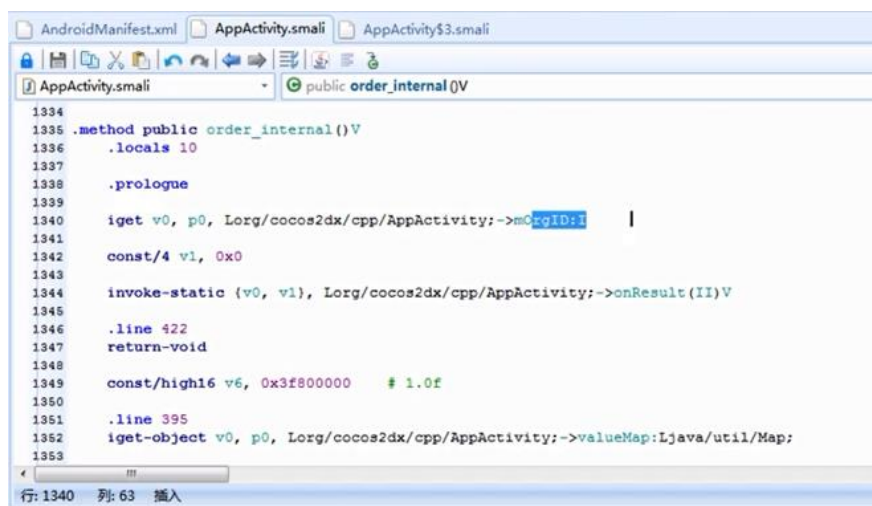


```
1334
1335 .method public order_internal()V
1336 .locals 10
1337
1338 .prologue
1339 iget-object v0, p0, Lorg/cocos2dx/cpp/AppActivity$3;->this$0:Lorg/cocos2dx/cpp/AppActivity;
1340
1341 iget v0, v0, Lorg/cocos2dx/cpp/AppActivity;->mOrgID:I
1342
1343 const/4 v1, 0x0
1344
1345 invoke-static {v0, v1}, Lorg/cocos2dx/cpp/AppActivity;->onResult(II)V
1346
1347 .line 422
1348 return-void
1349
1350 const/high16 v6, 0x3f800000 # 1.0f
1351
1352 .line 395
1353 iget-object v0, p0, Lorg/cocos2dx/cpp/AppActivity;->valueMap:Ljava/util/Map;

```

行: 1348 列: 16 插入

将这段代码插入到选择的位置上，不过在 app 运行时会产生错误，原因是在 1339 行中 p0 是类 AppCompatActivity\$3 的指针而不是 AppCompatActivity 的，所以将该句删掉



```
1334
1335 .method public order_internal()V
1336 .locals 10
1337
1338 .prologue
1339
1340 iget v0, p0, Lorg/cocos2dx/cpp/AppActivity;->mOrgID:I
1341
1342 const/4 v1, 0x0
1343
1344 invoke-static {v0, v1}, Lorg/cocos2dx/cpp/AppActivity;->onResult(II)V
1345
1346 .line 422
1347 return-void
1348
1349 const/high16 v6, 0x3f800000 # 1.0f
1350
1351 .line 395
1352 iget-object v0, p0, Lorg/cocos2dx/cpp/AppActivity;->valueMap:Ljava/util/Map;
1353
```

行: 1340 列: 63 插入

重新编译并安装后，可以完成内付破解