FART 脱壳王课程定制版 jadx，可自动修复并重构被抽取的函数，感兴趣的可以看下简介。

**直接赠送**

船型升级的Fart10内部版镜像！

已经刷好Fart10的Nexus5X手机一部！

即将开源的脚本持久化框架FridaManager内部版！

**课程优势**

**最底层的方案**：从Art源码直击Java类和方法解释执行的根本原理

**最前沿的工具**：Fart重磅更新+船新脚本持久化框架FridaManager

**最顶尖的技术**：掌握一二代壳/DexVmp/Dex2C加壳脱壳核心原理

**最贴心的服务**：超长两年服务时间/与大佬负距离亲密接触/纵享丝滑

- 五月：整体型壳的核心原理
  - **手写整体型壳**：安卓动态加载机制,Classloader详解
  - **Xposed脱壳插件**：Xposed安装使用插件开发,FDex详解
  - **Frida脱壳脚本**：Frida插件开发,DEXDump内存暴力脱壳
- 六月：打造整体脱壳沙箱
  - **安卓源码编译**：源码版本/同步/编译,导入IDE阅读分析
  - **App的加载流程**：App生命周期,dex0oat流程分析脱壳
  - **寻找海量脱壳点**：整体脱壳的本质,直接简介寻找脱壳点
- 八月：抽取型壳的核心原理
  - **壳的种类识别**：壳与加固手段的甄别,手写反调试与绕过
  - **手写抽取型壳**：Native GOT/PLT/inline hook详解与应用
  - **类加载和执行**：Art中类加载和方法执行流程关键函数详解
- 九月：FART10，到来！
  - **构造主动调用**：Art源码Review,Jni流程定制,方法体Dump
  - **方法体的回填**：五元组格式解析,占坑型/偏移型的不同处理
  - **Frida+Fart！**：动态加载的Dex处理,单方法Dump,重构Fart！
- 十一月：DEX-VMP壳的核心原理
  - **DEXVMP特征识别**：解释器的常见特征/分类和运行流程分析
  - **手写DEXVMP壳**：手写映射表,动态解密翻译执行Smali指令流
  - **DEXVMP分析沙箱**：Frida+沙箱动态追踪Vmp执行的Java方法
- 十二月：DEX-VMP分析与还原
  - **分析沙箱强化**：强制解释模式,从Jni进行ArtMethod tracing
  - **搞定"拦路虎"**：重编译内核&定制Art虚拟机绕过所有反调试
  - **重构映射表**：HyperPwn直接调试Vmp分析重构原始映射表
- 二月：Dex2C的原理和分析
  - **Jni&&反射**：从Jni源码分析Java&C(++)互相调用完整流程
  - **Dex2C加固应用**：Dex2C加固流程,特征,执行和Frida动态分析
  - **Dex2C逆向分析**：定制解释执行分析沙箱,打造Jni四向tracer
- 三月：内部版FridaManager！
  - **原理与使用**：使用环境和方法,原理和源码分析,插件编写详解
  - **FridaGadgat**：App启动过程和注入时机点选择,加载和Hook生效
  - **FridaManager**：完全脱离PC,Fart移植,r0capture移植,制作沙箱

**Fart脱壳王!从此没有脱不下来的壳！手把手教你打造陆地最强脱壳机！**

最新的工具和技巧，最实用和有效的方法，前人指路，一点即通；
高手带路，少走弯路，躺捡工具，节约时间，商务便捷，干净卫生；
同时希望营造一起研究、解决问题的环境，互惠互助、无缝交流；

**课程时长：**

- 24 个月（一年授课+一年更新）

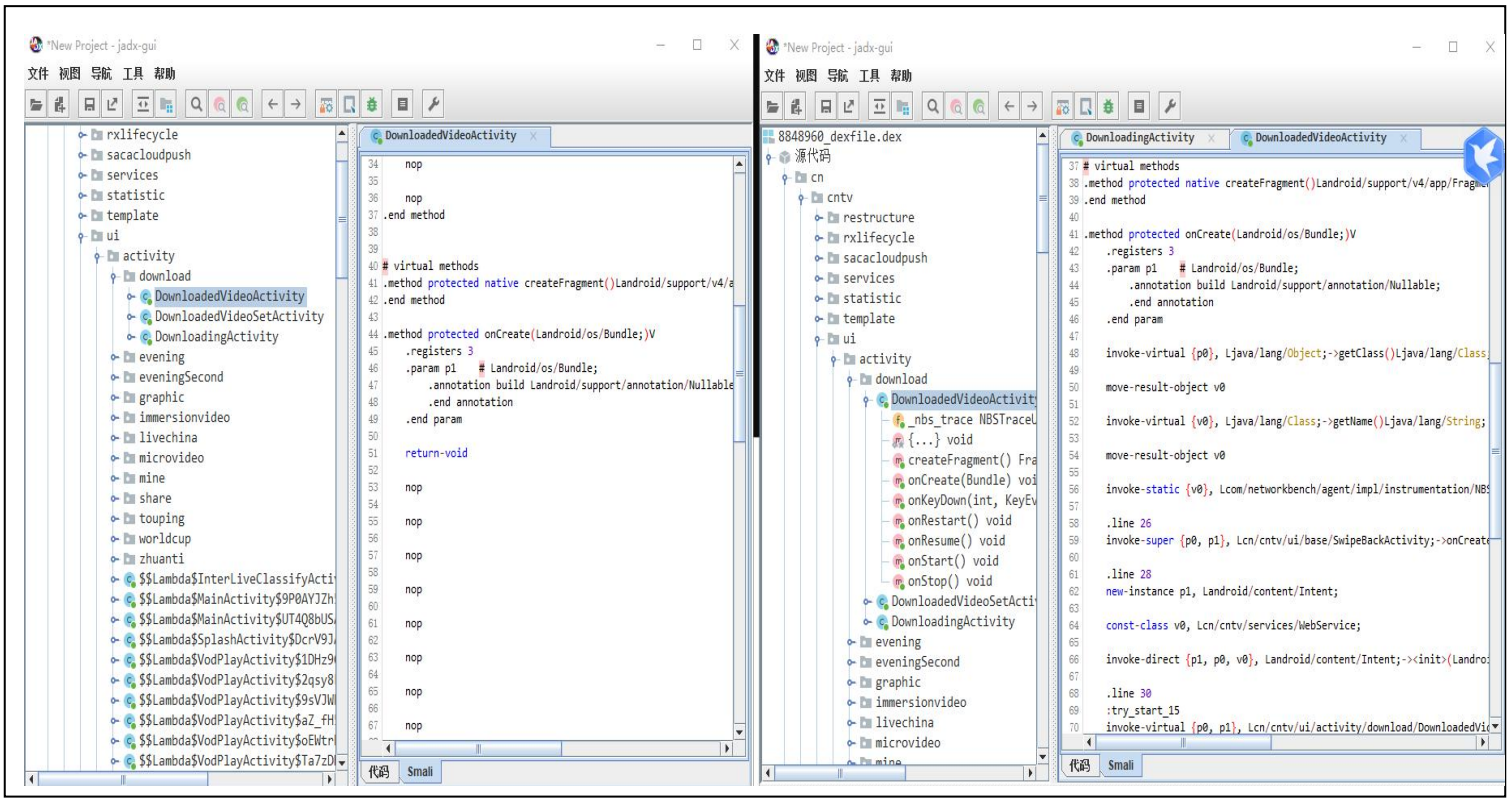
**课程形式：**

- 授课 12 个月合计 48 节课，均包含回放+课件；
- 更新计划见上图，一半内容为录播，一半内容为直播；
- 每节课2h，全程高能干货，手把手操作、在线互动；
- 所有课程均为船新制作，使用最新的工具和最强技术；
- 第一年上课，第二年维护和更新，服务期合计24个月；

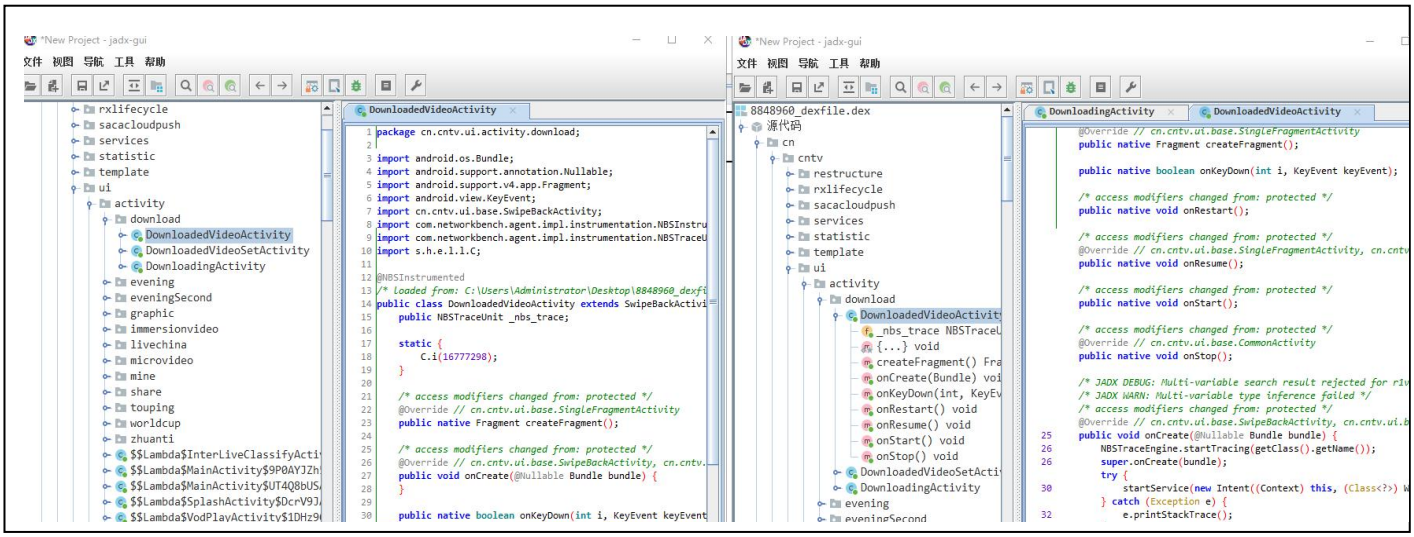

具体使用流程如下：

1. 使用 FART 脱壳机对加壳的 app 脱壳后可得到 dex 文件和对应的函数体文件即 bin 文件。将要修复的 dex 以及对应的 bin 文件拷贝到一个文件夹下，如下图：

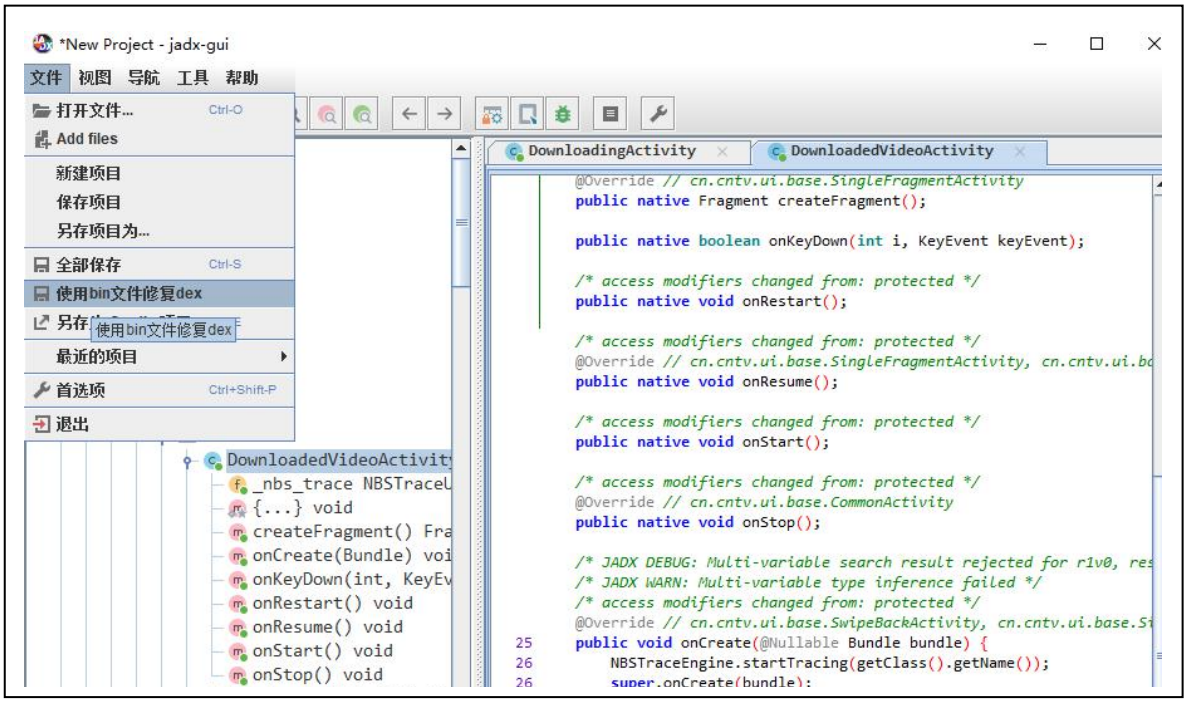

2. 使用 FART 定制版 jadx 直接打开待修复的 dex 即可自动完成 dex 和 bin 文件的合并，恢复被抽空的函数，下图左侧为官方版本 jadx 打开 dump 的 dex 的效果，右侧为 FART 定制版 jadx 根据 dex 和 bin 文件自动修复的效果，可以看到左侧为被抽空的 onCreate 函数，右侧已经进行了修复。



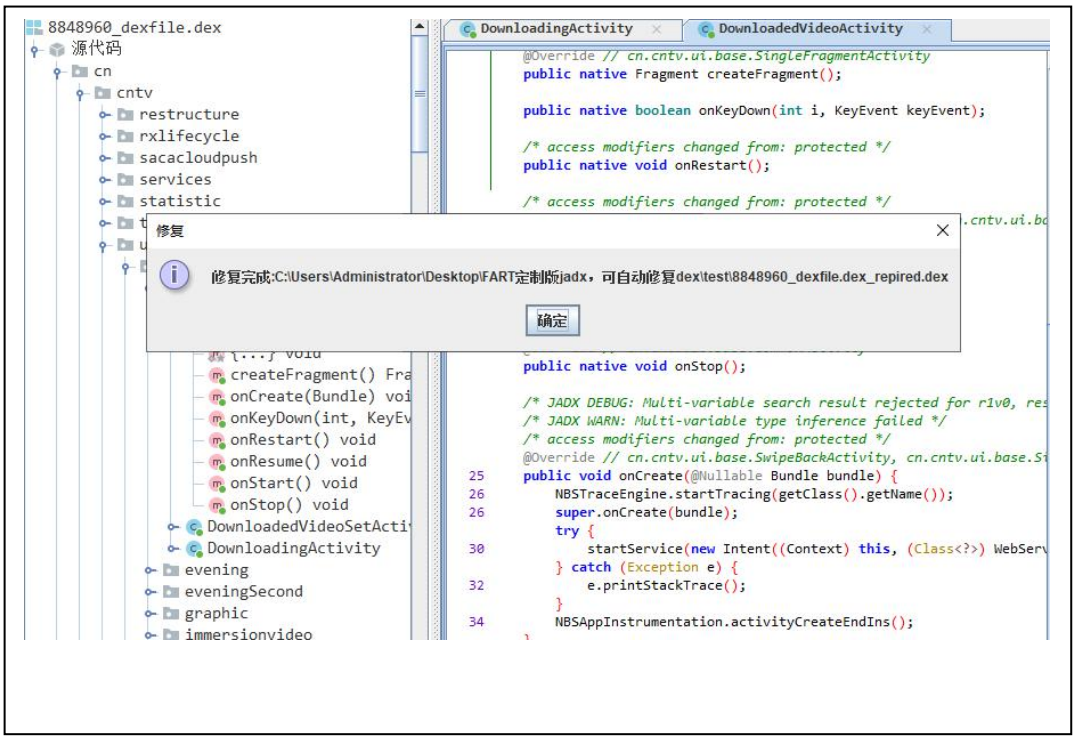
下面为对该函数进行反编译的效果对比图，定制版 jadx 反编译成功。



3. 如果需要针对 dex 和 bin 文件进行合并生成新的修复的 dex，可以直接在文件中点击“使用 bin 文件修复 dex”即可，之后会弹出“修复中”对话框，等待修复完成生成新的 dex 即可。




4. 修复结束后，会弹出修复生成的 dex 对应的路径，如下图：



接下来就可以使用 gda/官方 jadx/jeb 打开修复生成的 dex 进行逆向分析了，下面为使用 gda 打开修复的 dex 的效果图，可以看到原来被抽空的函数已经成功完成了修复。