

1. classes.dex

Android 程序编译以后生成一个 apk 文件，里面的 classes.dex 便存放着程序的运行字节码。

2. backsmali

ShakaApktool 使用 bs 命令即可对 classes.dex 实现反编译回 smali，而使用 s 命令可以把 smali 字节码编译为 classes.dex 文件

java -jar ShakaApktool bs xxx.dex -o smali 文件夹路径

java -jar ShakaApktool s smali -o xxx.dex

```
D:\F8Tool\Crack\MobileTool\apktool>java -jar ShakaFix.jar bs F:\Android\21\classes.dex -o F:\Android\21\classes

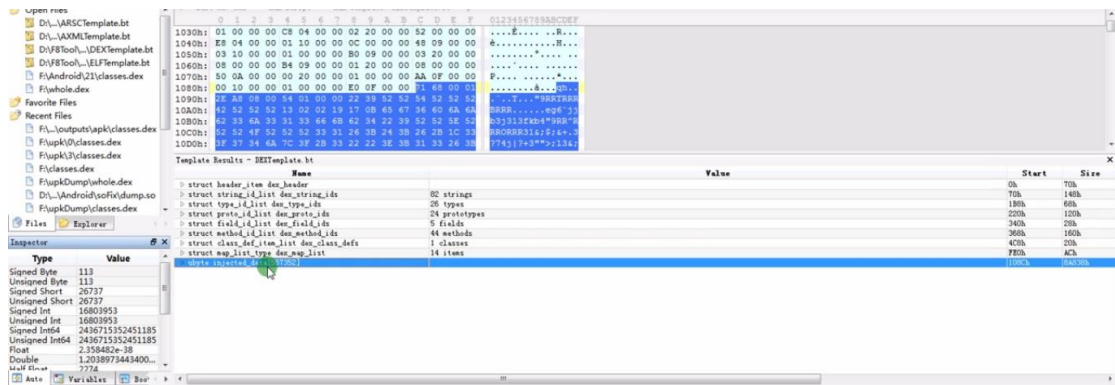
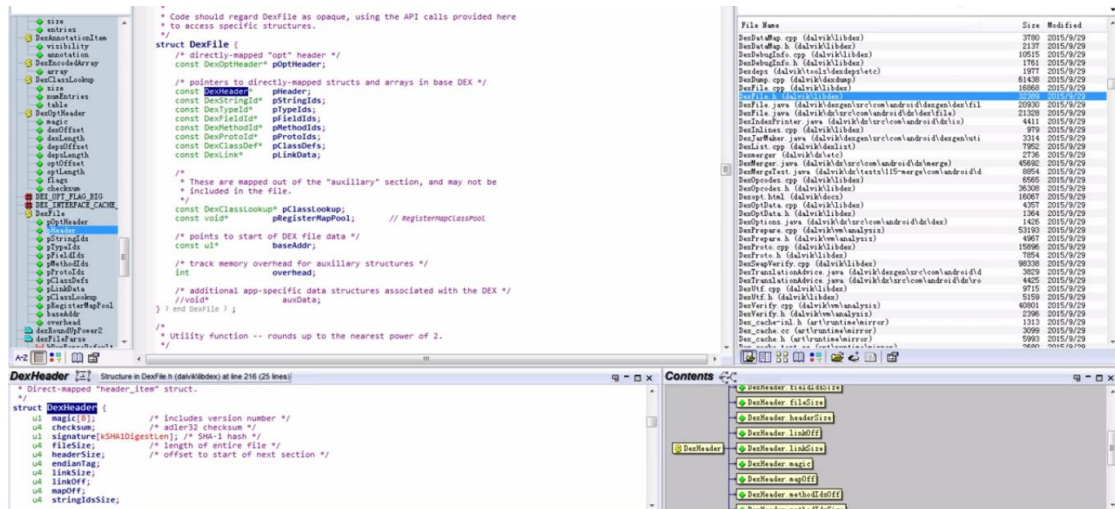
D:\F8Tool\Crack\MobileTool\apktool>java -jar ShakaFix.jar s F:\Android\21\classes -o F:\Android\21\classes
```

3. 010Editor

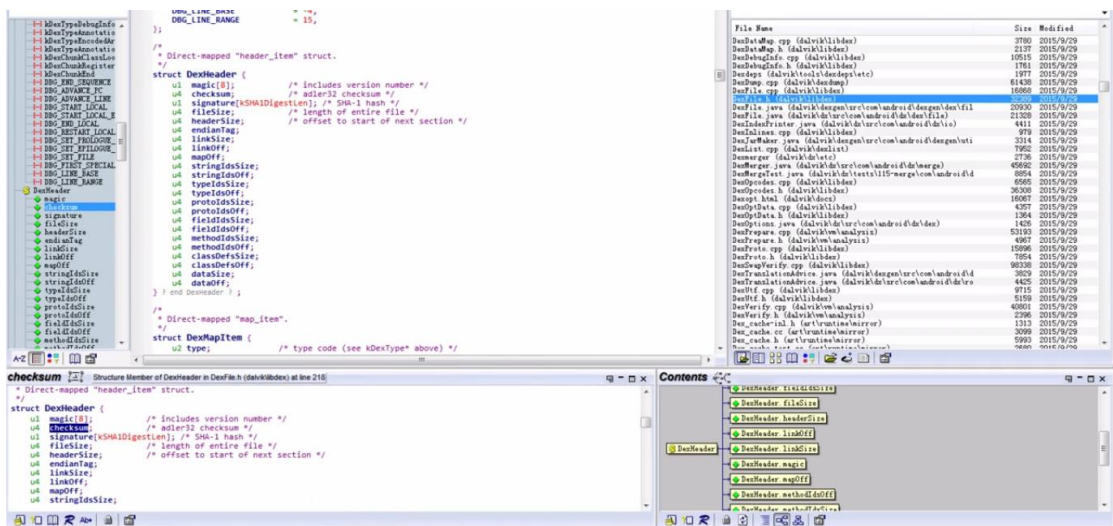
一种很常见的 16 进制查看工具，它的模板功能比较强大，可以通过脚本读取文件。

4. dex 文件

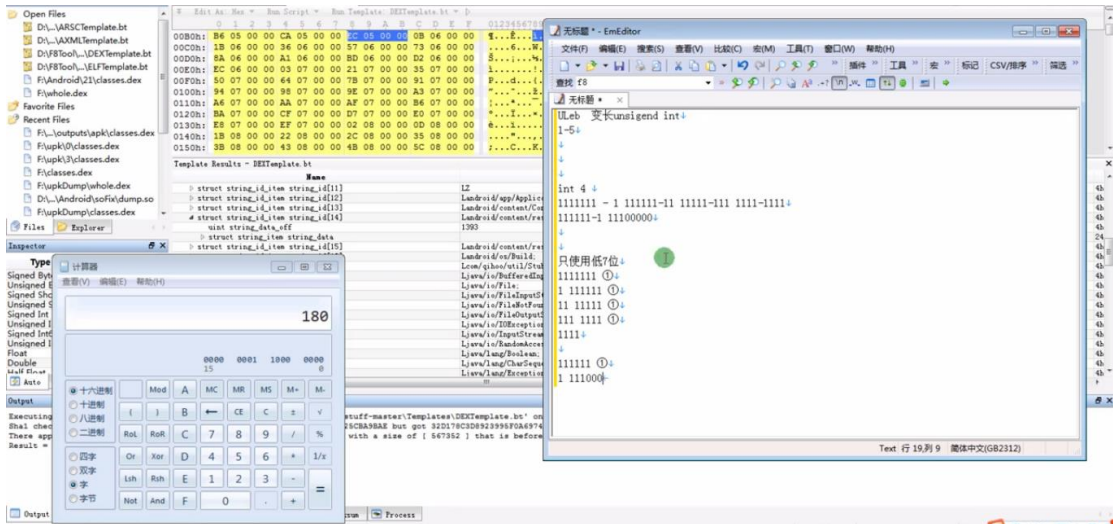
Android 系统源码的 dalvik/libdex 目录下存放的是 dex 文件相关的定义



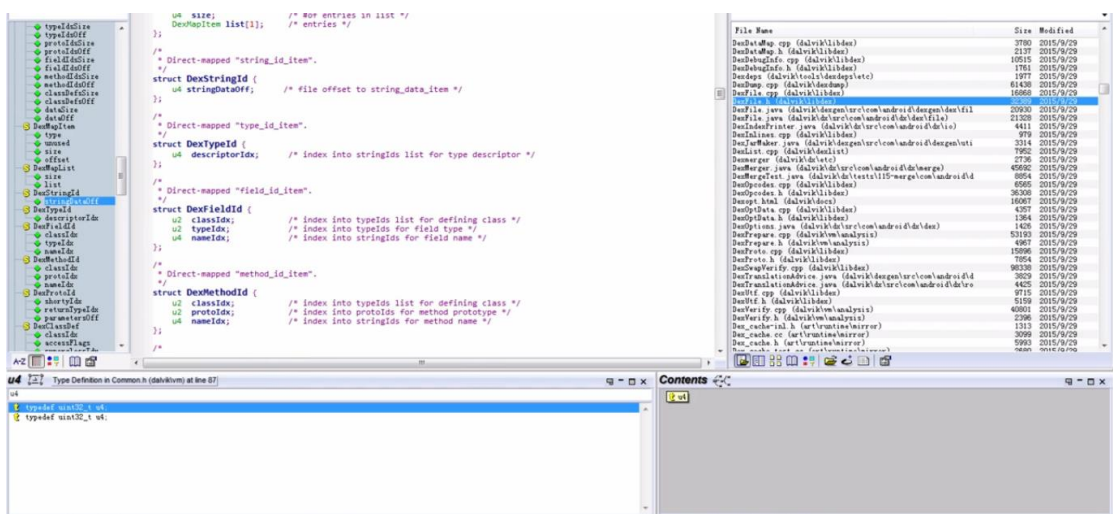
DexHeader 存放 dex 文件的相关信息



ULeb 的作用

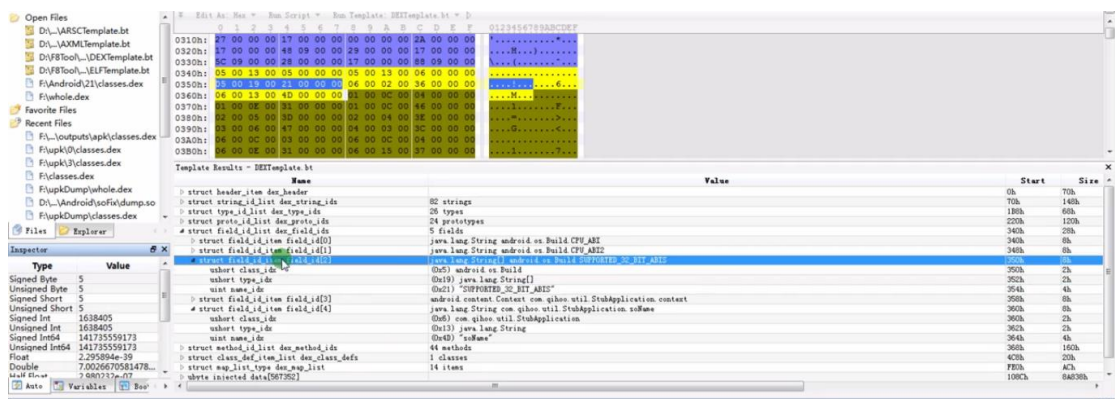
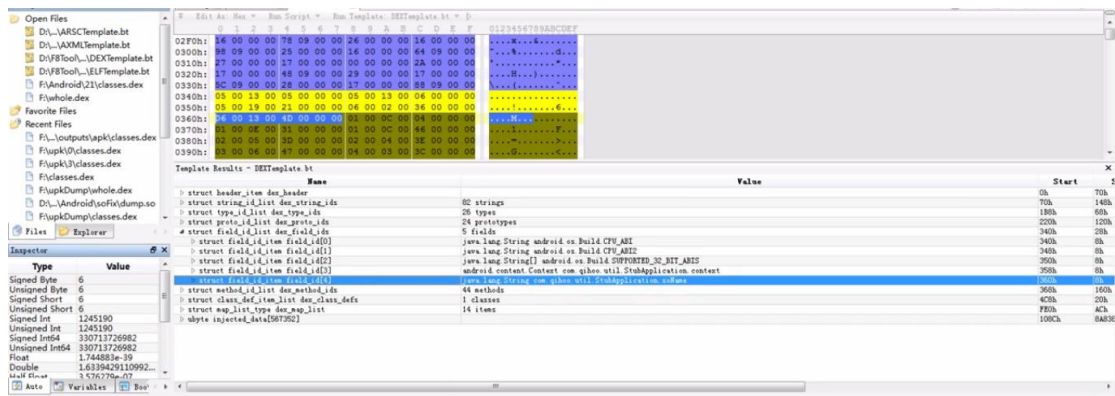


string_id 存放字符串信息

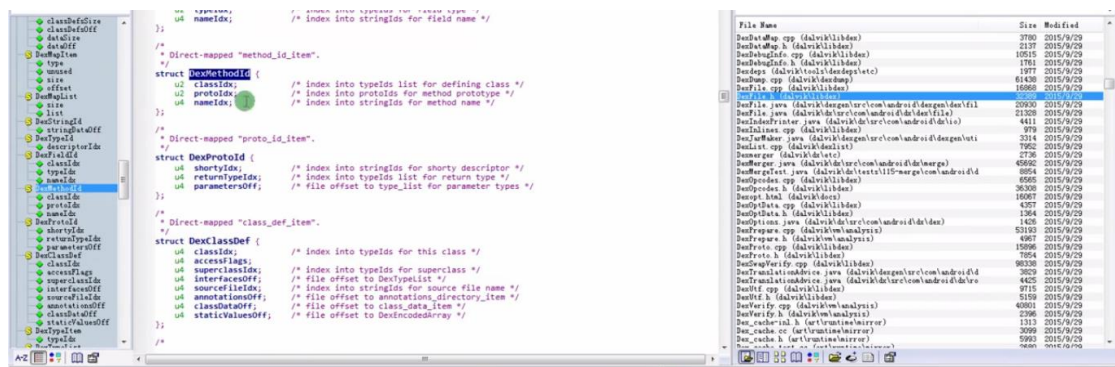
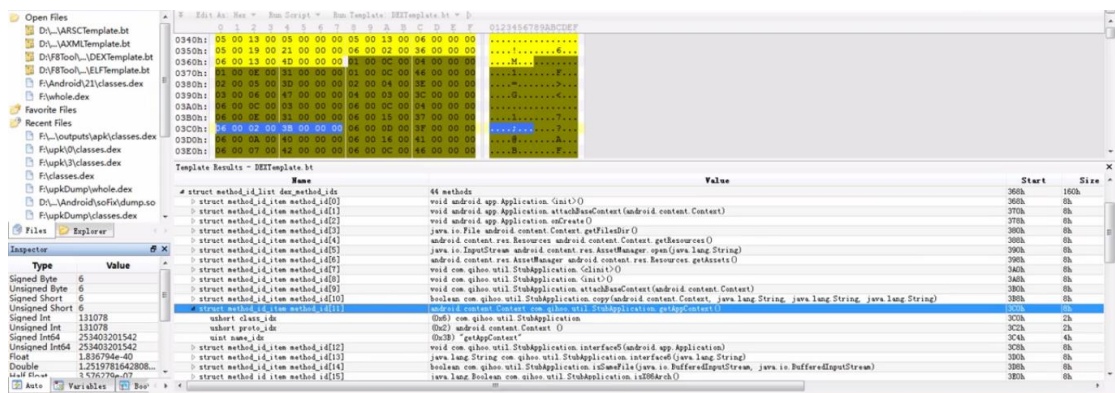


type_id 存放类型定义信息

field_id 存放类型函数名称的描述符



method_id 存放方法的描述信息



class_def 存放类的结构信息

[illegible]