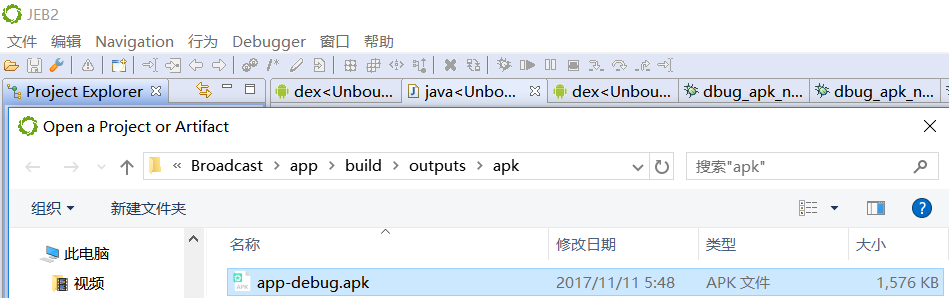
1. 本次实验用到的Android模拟器为“逍遥安卓”，安装程序：XYAZ-Setup-3.6.2.exe，安装完毕之后打开“逍遥安卓多开管理器”因为JEB远程调试要求设备版本最低为Android5.1，因此你可以点击右下角的“+新建模拟器”自己安装5.1版本，我在这边直接给大家提供了我用的emulator的镜像文件Android5.1.ova，直接“导入模拟器”即可



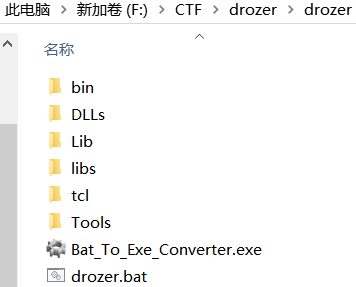
1. “逍遥安卓模拟器”安装好之后，在安装目录的MEmu文件夹下自带了adb.exe工具，大家可以把该目录添加至系统环境变量Path下，比如我这边添加的是D:\xiaoyao\MEmu
2. JEB是逆向Android APK的强有力的武器，给大家提供了破解版压缩包jeb-2.2.7.201608151620\_crack\_qtfreet00.zip，解压完毕之后针对自己的应用端，直接运行jeb\_linux.sh/jeb\_macos.sh/jeb\_wincon.bat 即可打开
3. 针对JEB一运行就闪退的问题，应该是大家的系统环境变量没有设置好，具体是JAVA\_HOME，CLASSPATH，PATH这3个环境变量（大小写不敏感），具体可以参考这篇文章，传送门-><http://blog.csdn.net/csp277/article/details/46672733> 建议JDK版本为8

直接打开APK，然后在左边Project目录下双击Bytecode，到你感兴趣的Class里按Q或者右键反汇编Decompile即可



1. Drozer是Android平台下的安全功能集成软件，分为服务端和代理端，解压drozer-installer-2.3.4.zip文件，其中agent.apk安装在emulator上，然后本地Windows运行setup.exe完成本地安装（也有Linux的版本，自行Google），然后cmd命令行进入到该目录下

F/drozer/drozer> drozer 运行服务端



在emulator里面，打开drozer Agent，开启右下角，就可以看到绑定端口31415，所以要在本地做好端口转发

1. flagstore.apk是我们这次的作业，大家在用“JEB远程调试”和“Drozer sniff”拿flag的时候可能会遇到乱码的问题，截图的时候只要看到"CongratsGoodWorkYouFound”即可
2. 本次两次实验可能会用到的操作：

adb设备发现，进入shell

adb本地与emulator进行端口转发

adb am工具发送自主广播

JEB 通过Debugger-start-Attach进行远程调试

Drozer的sniff模块的使用（广播监听）

请大家自行Google

1. 大家可能会踩到很多‘坑’，如果没有踩到那就算我倒霉，欢迎大家在群里讨论，星期六会发给大家一个参考文档，附带Q&A