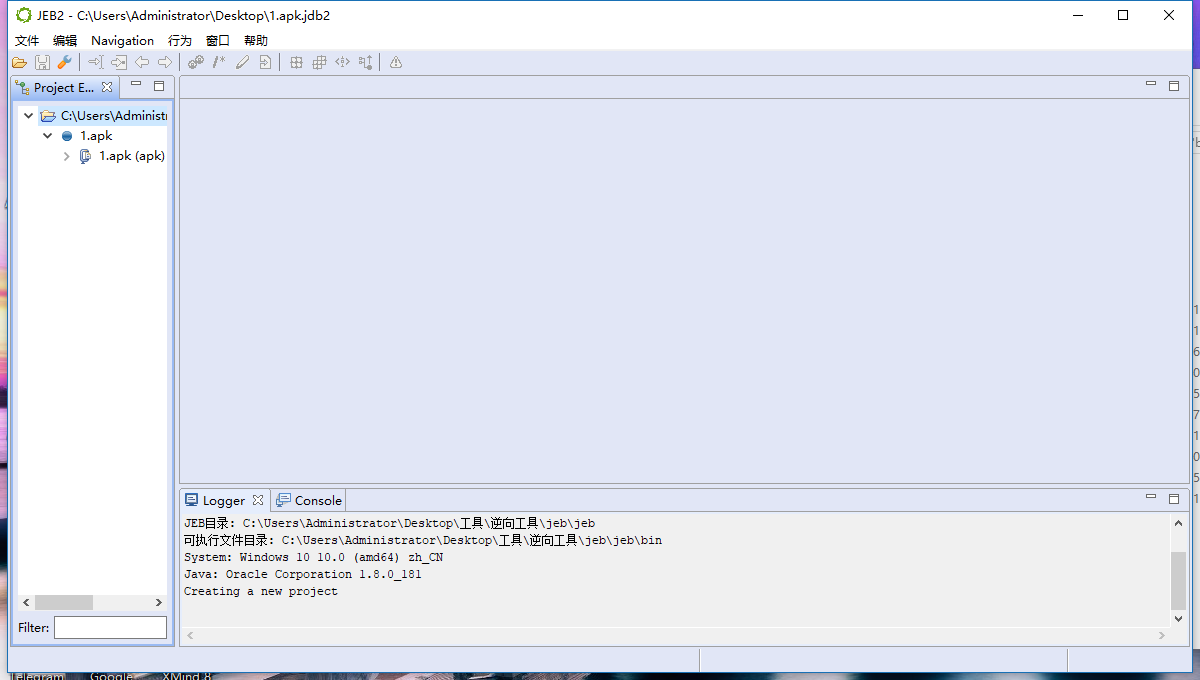
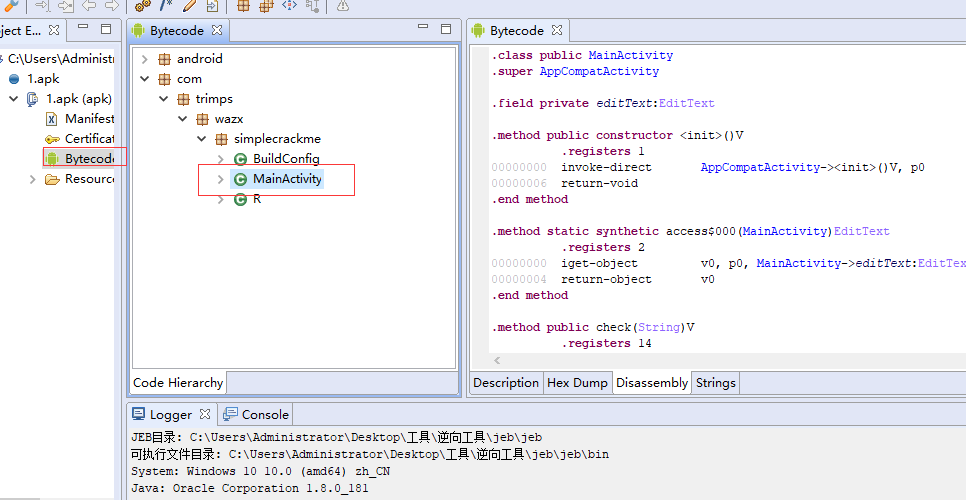
那么做这道题目之前是需要一个反编译的软件。我是使用的jeb.

JEB这个软件是挺好的

那么可以看到的是这就是JEB打开文件的界面

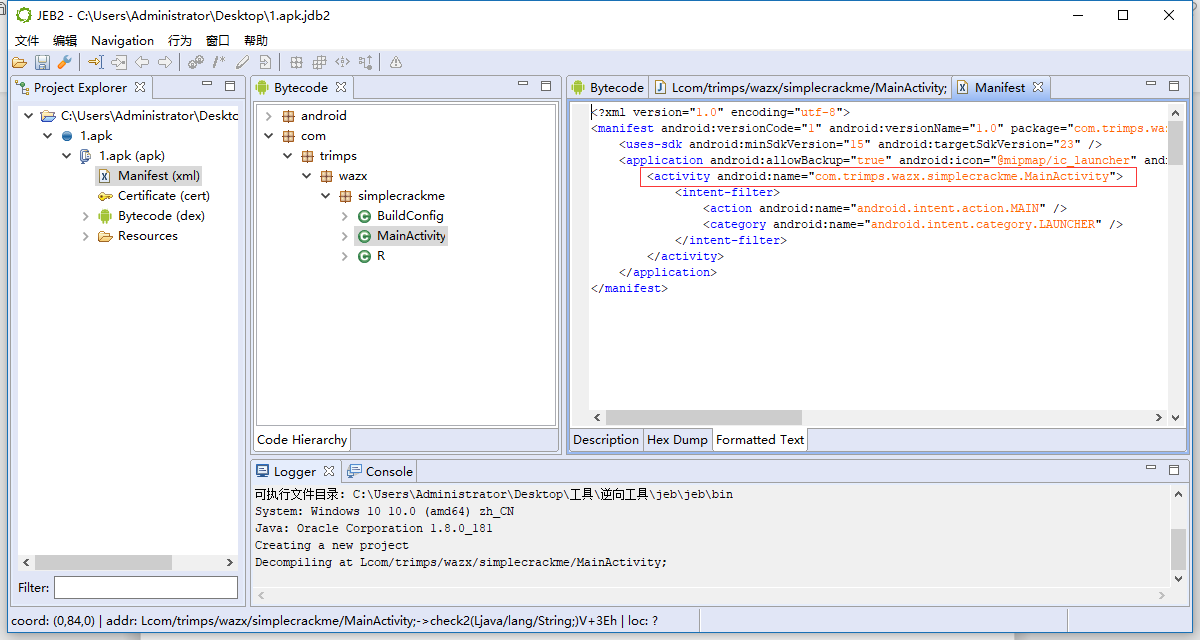


要看文件的函数和使用方法的话，就需要查看dex文件，dex文件是安卓的核心文件，是运行在安卓Dalvik虚拟机上面的。apk的编译过程就是：java源代码----.class文件---转化成dex文件。

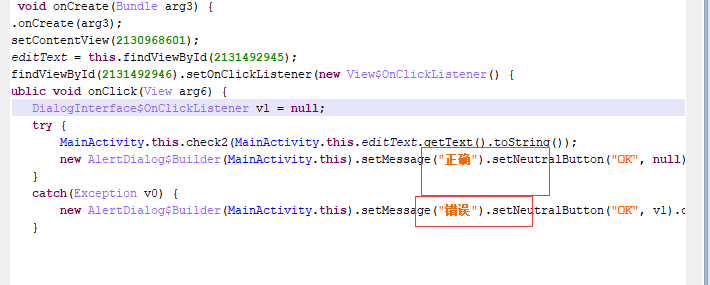


第二个框就是dex文件中的一些类，一些函数的用法。然后在第三块的代码区域不是JAVA代码，可以使用右键选择D就可以转化成了JAVA代码。

可以道xml文件中去找到最先调用的函数



那么可以去看的很清楚是在mainActivity函数中



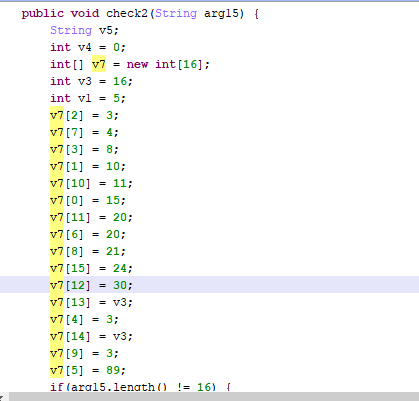
这里有中文，那么就好办了。在那种情况下会输出正确的呢。

如果check2函数执行成功了，那么就会打印出正确。如果没有执行成功就会打印出失败

调用的check2函数来执行我们输入的字符

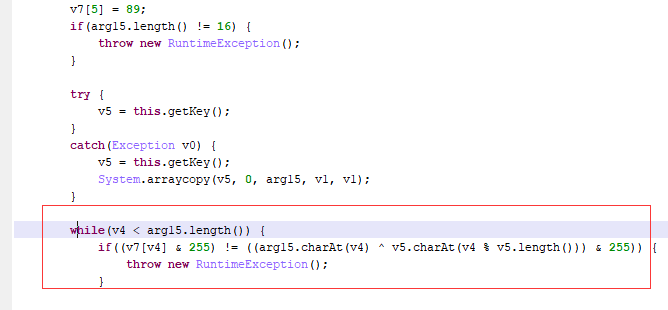
那么去看看check2是怎么做的。

先是定义了一些数组。

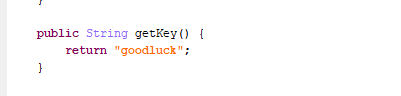


有一个while循环判断。那么其中与255 其实就是自己的数据。没有变化，后面的那个与也可以忽略。主要就是其中的那个异或操作

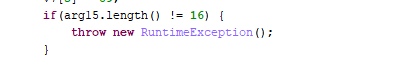
其实其中的arg15也是我们自己传进来的值。和v5进行异或操作



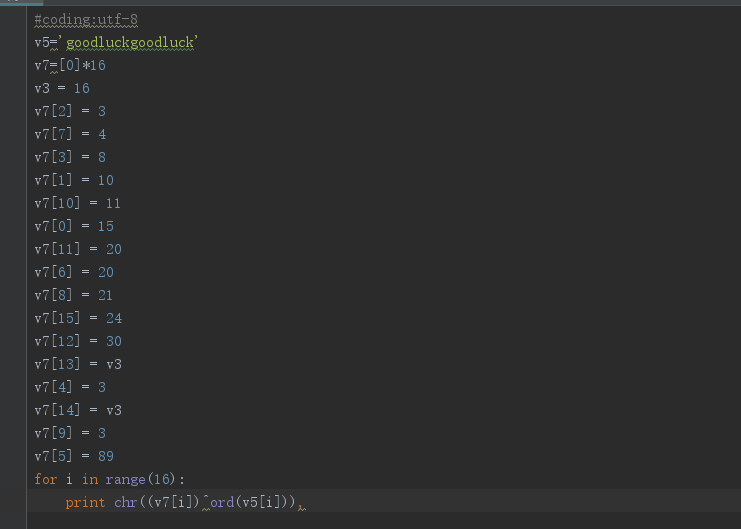
那么可以看到getkey是返回goodluck。是八个字符串 ，那么就是说是v5就是这个八个字符串。那么也就是我们输出的字符在和goodluck进行异或操作



那么就可以写一个脚本把flag跑出来就可以 但是我们输出的字符串是要等于或者是大于16位的。而goodluck刚好是八位，那么可以执行两次就可以了。



那么在程序中是异或的，那么反异或回去就可以了。异或操作就是a ^ b =c a^c =b 都是同样的。



那么就可以出来flag了，在使用夜神模拟器来提交做以下。 flag：hello,worldpress

