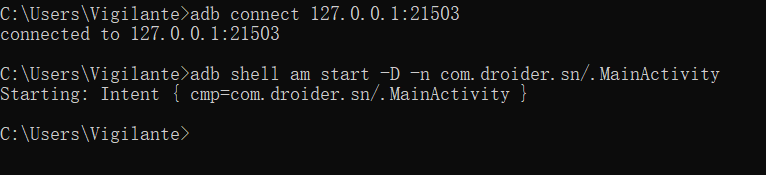
# 1 连接模拟器

首先需要连接模拟器，再输入命令对apk进行动态调试

以逍遥模拟器为例：



连接各模拟器的端口号如下：

夜神模拟器：adb connect 127.0.0.1:62001

逍遥安卓模拟器：adb connect 127.0.0.1:21503

天天模拟器：adb connect 127.0.0.1:6555

海马玩模拟器：adb connect 127.0.0.1:53001

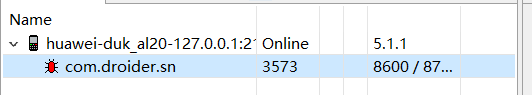
网易MUMU模拟器：adb connect 127.0.0.1:7555 MacOS:adb connect 127.0.0.1:5555

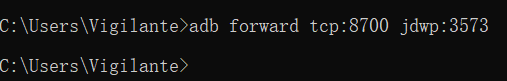
雷电模拟器：adb connect 127.0.0.1:5555

genymotion模拟器：adb connect 127.0.0.1:5555

谷歌原生模拟器：adb connect <设备的IP地址>：5555

进行端口转发：

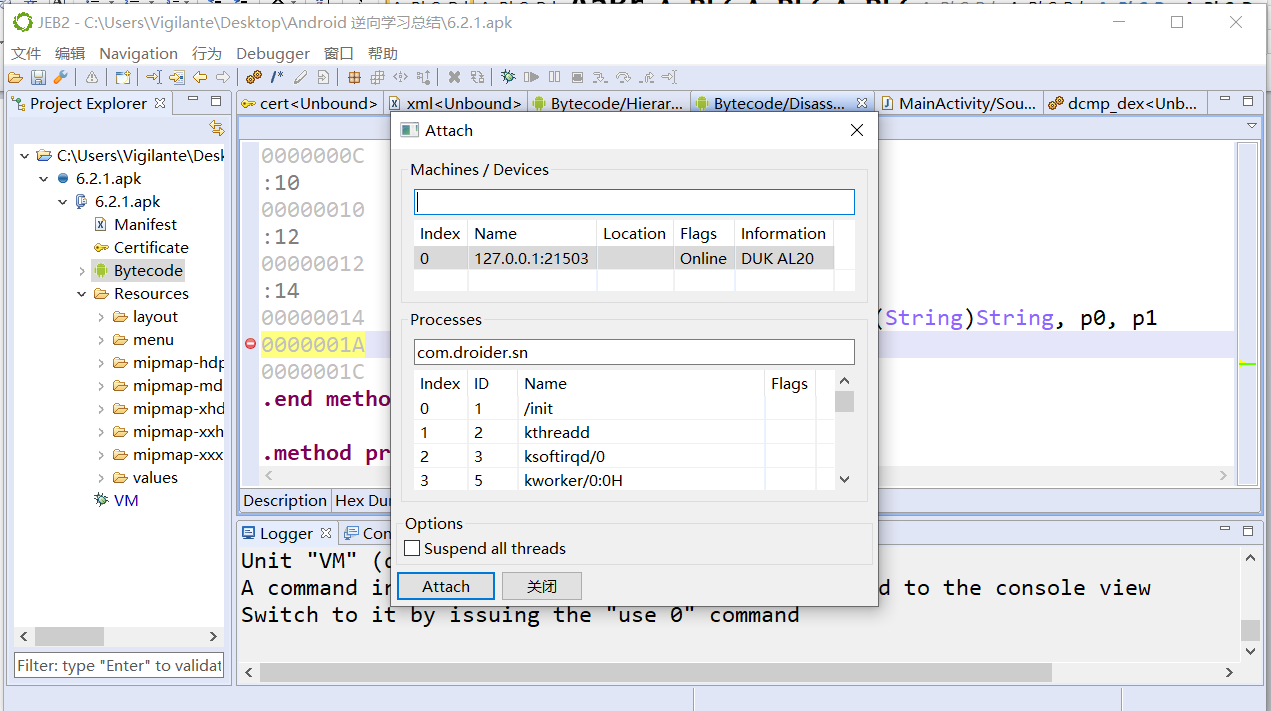


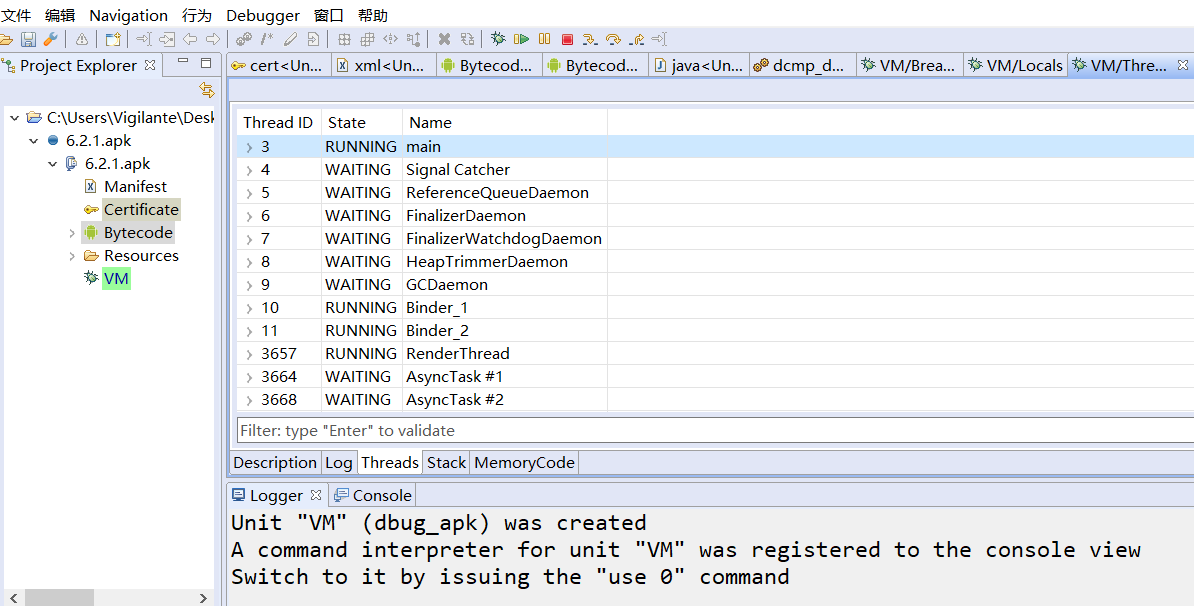


<https://www.52pojie.cn/thread-658865-1-1.html>

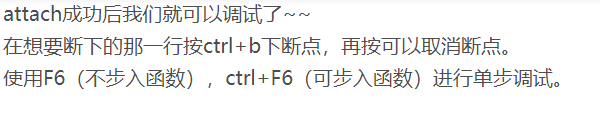
# 2 JEB动态调试

点击Debugger->start，进入如下界面，显示：





JEB环境下：



<https://blog.csdn.net/qq_33364733/article/details/98089751>

<https://blog.csdn.net/magic1an/article/details/78300039>

**JEB基本操作：**

(1)重命名(n)

(2)跟踪(Enter, 双击)

(3)返回(Esc)

(4)前进(Ctrl + Enter)

(5)帮助(H)

(6)条目信息(I)

(7)交叉引用(X)，源码交叉引用(Ctrl + X)

(8)注释(；or C)

(9)改变进制数(B)

(10)反编译(Tab)

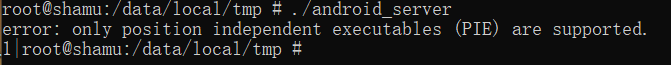
# 3 IDA动态调试

## 第一种

以IDA7.0 为例，首先需要将android\_server文件拷贝到模拟器或真机中，以模拟器为例，拷贝android\_x86\_server文件



接着更改模拟器中该文件的权限，并启动它，如果复制错了文件，会出现以下错误：



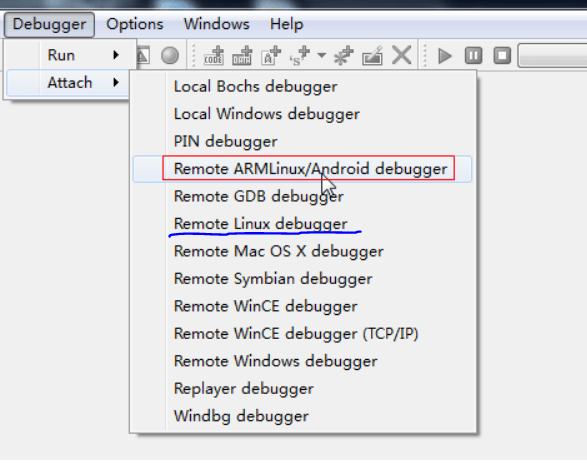


此时，需要进行端口转发：adb forward tcp:23946 tcp:23946

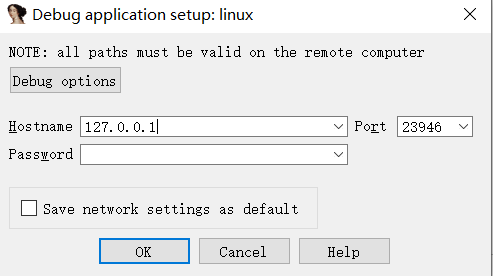


接着在模拟器上运行应用

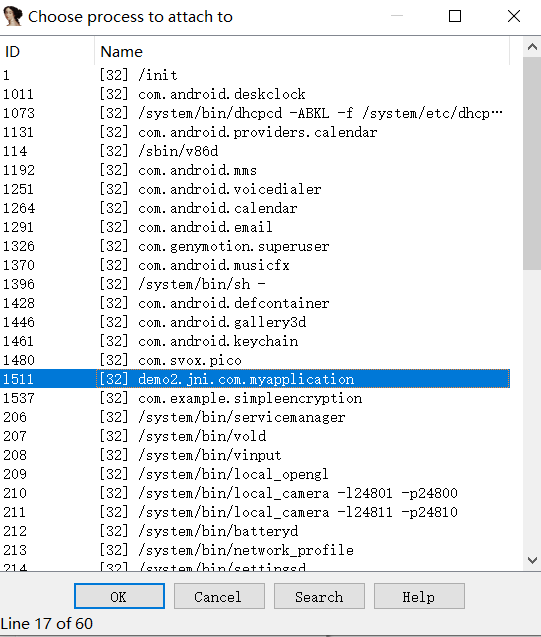
在IDA中执行以下操作：



注意：如果是x86的server文件，这里选择Linux选项



找到需要附加的进程

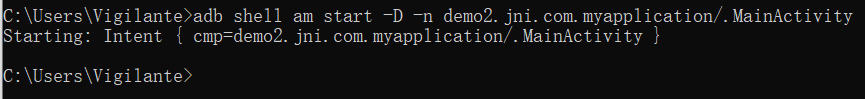


## 第二种（需要在程序刚启动的时候进行调试 ）

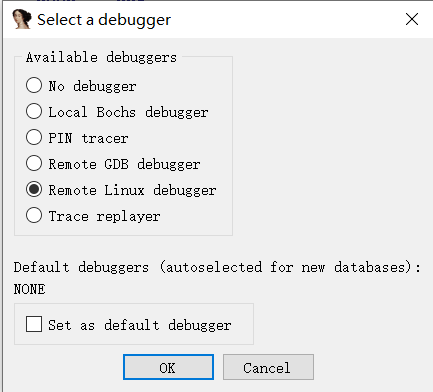
同样需要启动server文件，并进行端口转发，adb forward tcp:23946 tcp:23946



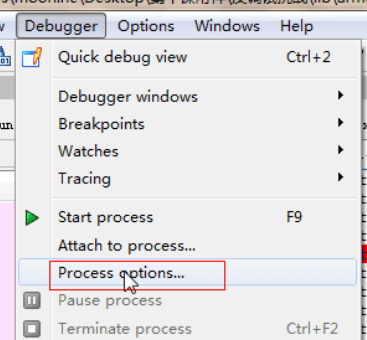
启动程序 adb shell am start -D -n demo2.jni.com.myapplication/.MainActivity

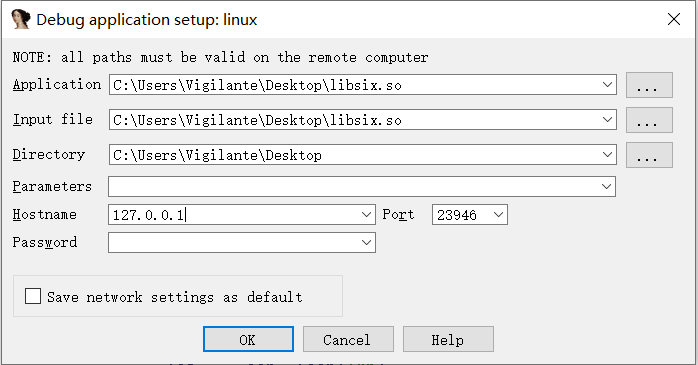


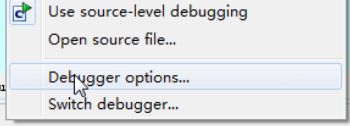
选择debugger

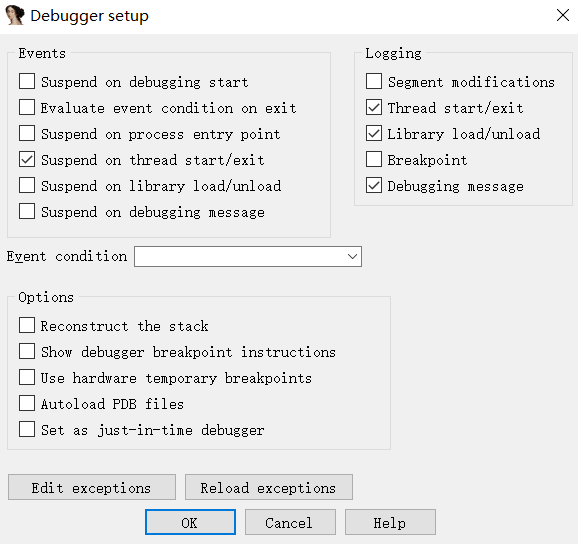


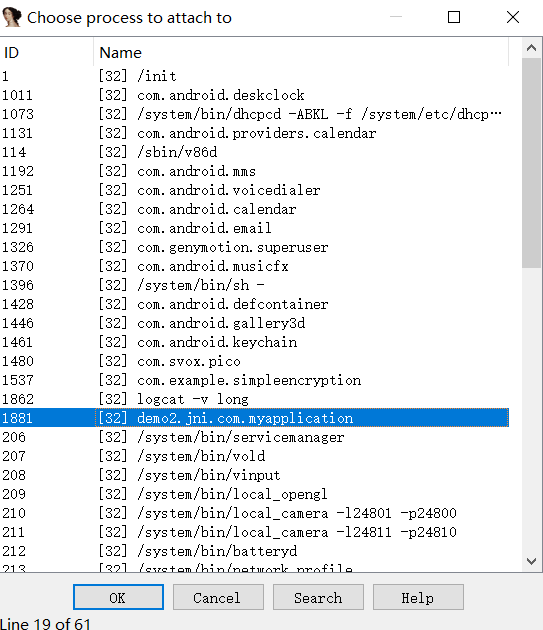
进行设置







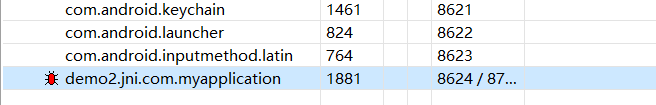
  
选择要附加的进程



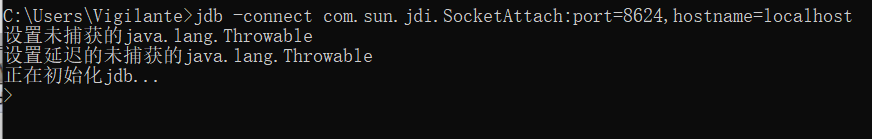
完成后F9运行程序 在IDA等待的时候运行命令：

jdb -connect com.sun.jdi.SocketAttach:port=8700,hostname=localhost

这时需要打开看进程的端口号，如这里是8624

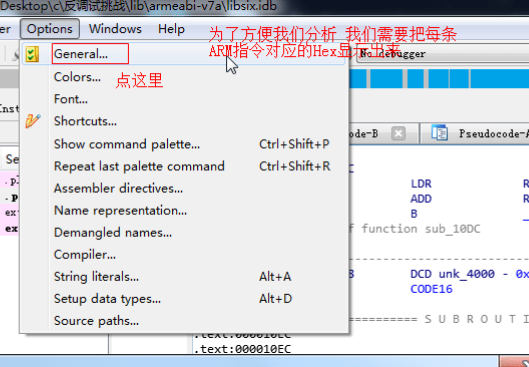


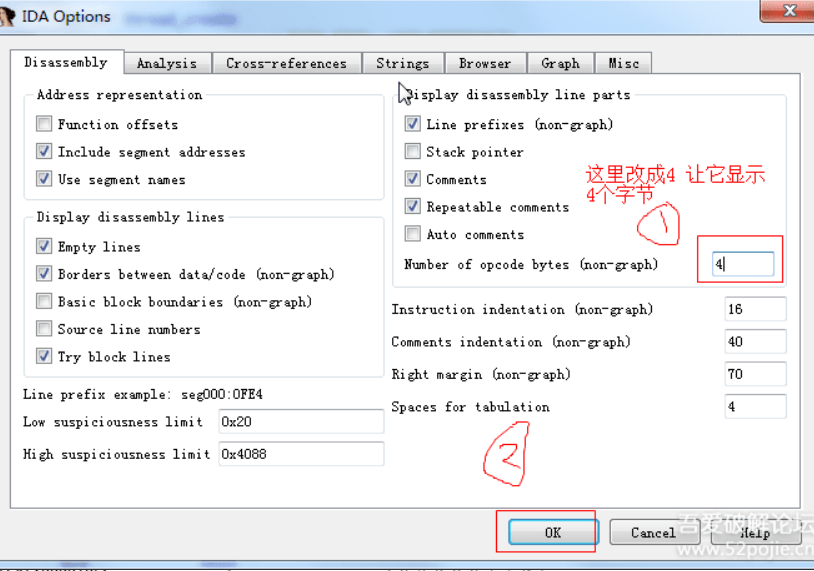
jdb -connect com.sun.jdi.SocketAttach:port=8700,hostname=localhost



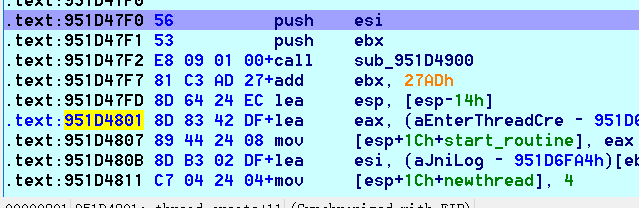
接着便可继续调试程序

## IDA使用技巧

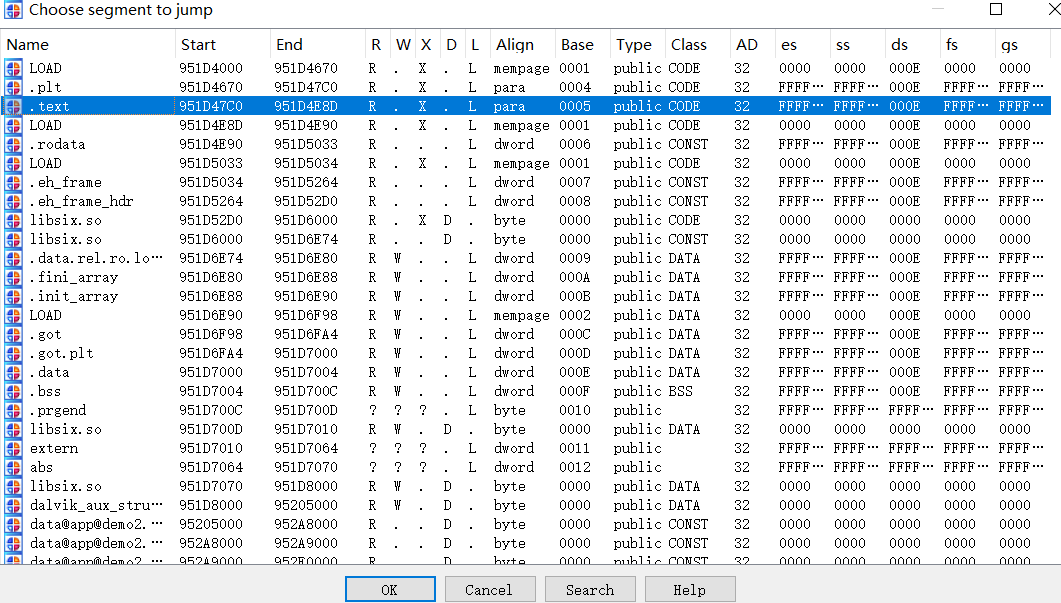


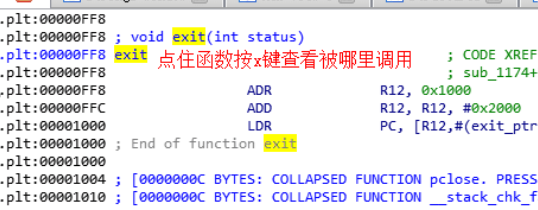


效果如下：



Ctrl+s





手动解析

点住dword\_1140右键Data转化成数据 然后鼠标放在\_\_unwind按住P键就转换成函数了 这个函数就是checkport对应的函数

