1、将手机里面的libdvm.so拷贝到PC上

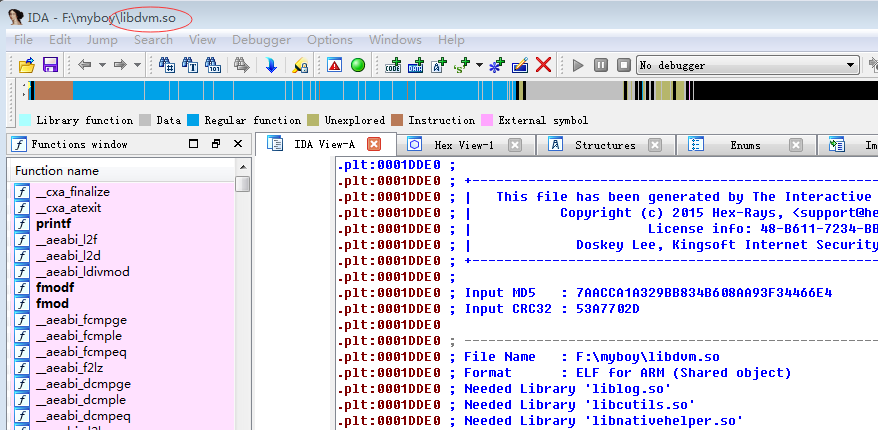
命令：adb push /system/lib/libdvm.so C:\

网上有提到libdvm.so与libart.so的区别。

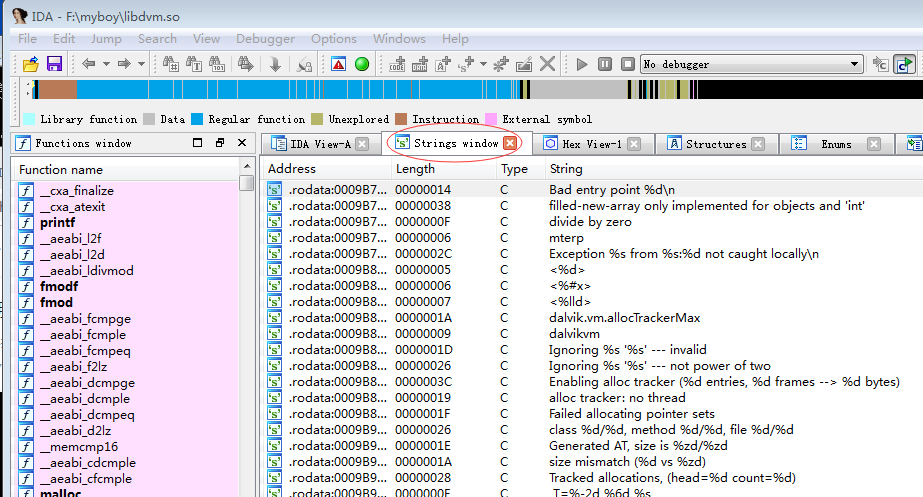
（<https://blog.csdn.net/koffuxu/article/details/44780351>）

我这边使用的是HUWAWEI G750-T00手机，Android版本是4.2.2，可以找到libdvm.so。

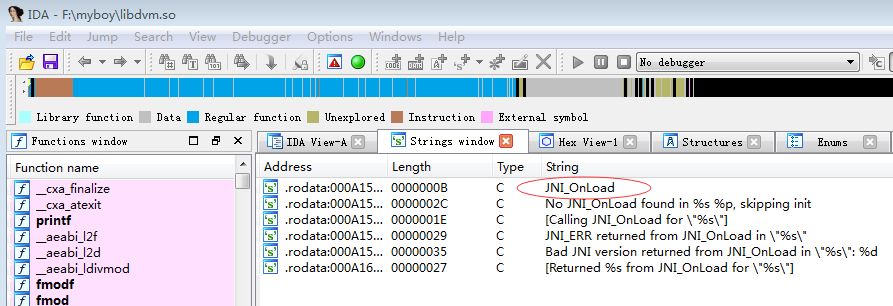
2、直接将libdvm.so拖到IDA里面。



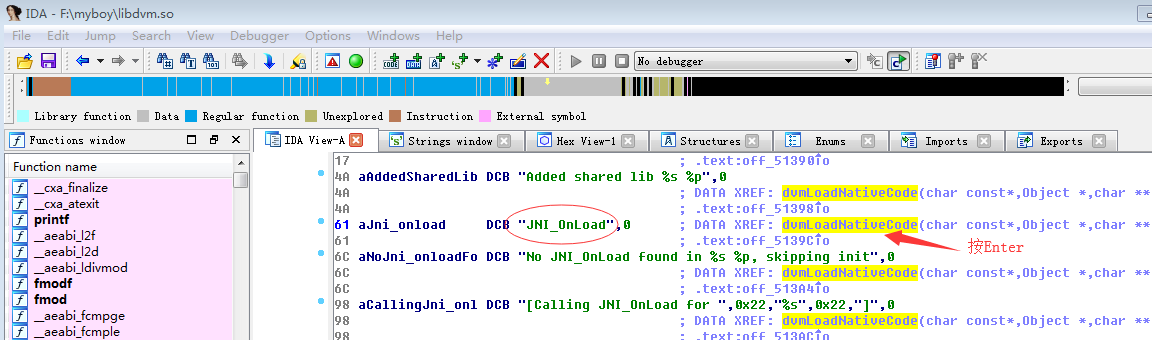
3、IDA中打开View/Open subviews/Strings窗口



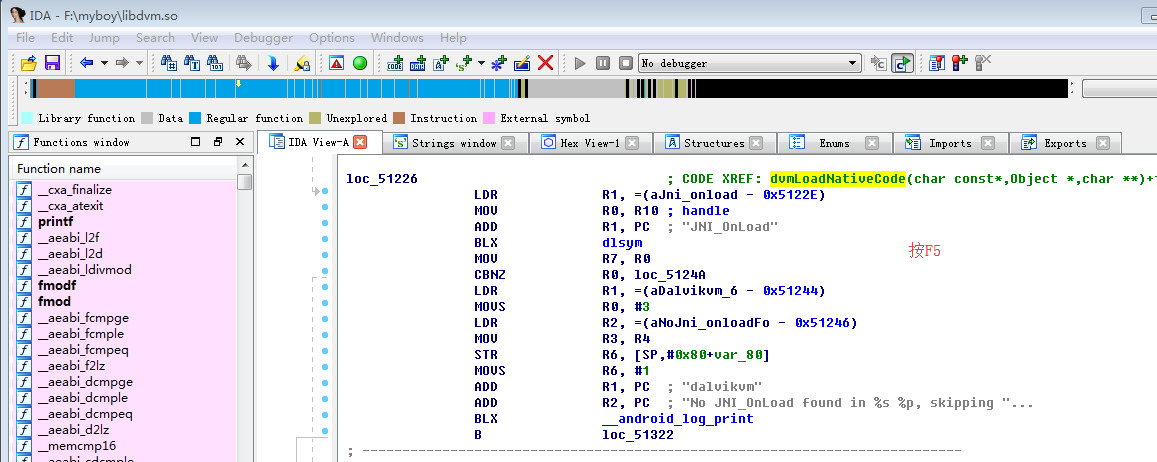
4、Ctrl+F查找JNI\_Onload



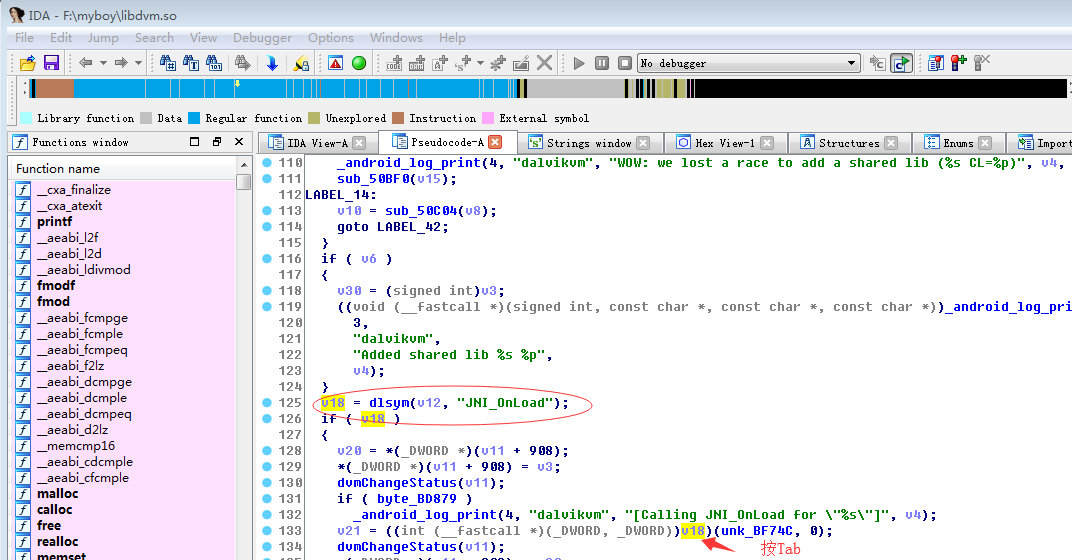
5、双击进入



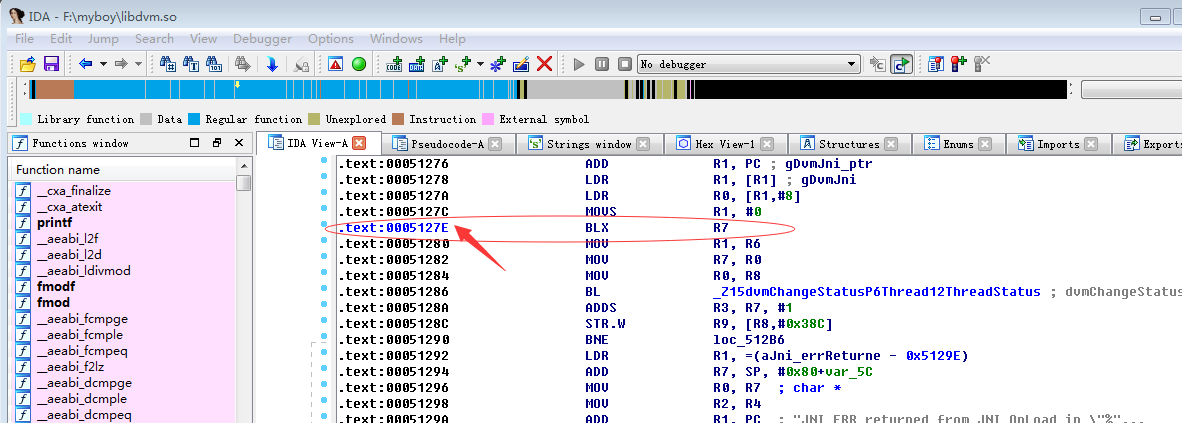
6、按Enter键后进入



7、按F5查看伪C代码



8、在箭头出按Tab键



9、JNI\_Onload函数的偏移是 0005127E

使用到的IDA快捷键：

Enter 进入函数

F5查看伪代码

Tab 伪代码和汇编代码视图切换

参考视频中的讲解（<https://www.bilibili.com/video/av36932216/?redirectFrom=h5> 39:00）