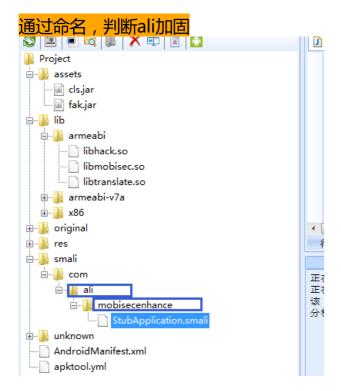
### 简单dex壳实例

? 3.apk





先于activity启动的类

```
选项 帮助
育 开始 🖷
0
    StubApplication.smali 📄 AndroidManifest.xml*
4
    1 <?xml version="1.0" encoding="utf-8" standalone="no"?>
0
       2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.al;</pre>
φ
             <uses-permission android:name="android.permission.INTERNET"/>
             <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
O
             <application android:allowBackup="true" android:debuggable="true"</pre>
           android:icon="@drawable/ic_launcher" android:label="@string/app_name" android:name="com.ali.mobisecenhance.StubApplication"
×
            android:theme="@style/AppTheme">
       9
                 <activity android:label="@string/app name" android:name=".MainActivity">
<intent-filter>
      11
Α
      12
                          <action android:name="android.intent.action.MAIN"/>
      13
                          <category android:name="android.intent.category.LAUNCHER"/>
Ф
                     </intent-filter>
      14
À
      15
                 </activity>
                 <activity android:name=".WebViewActivity"/>
             </application>
      17
      18 </manifest>
      19
```

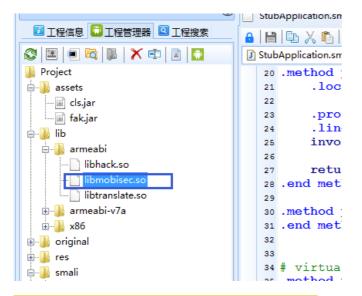
# 找到该类,发现加载了,库文件mobisec

```
StubApplication.smali AndroidManifest.xml*
    .prologue
      10
B
            .line 14
      11
            const-string v0,
                            "mobisec"
                                                   Ι
A
      12
      13
      14
            invoke-static {v0}, Ljava/lang/System;->loadLibrary(Ljava/lang/String;)V
nt 📥
      15
      16
            .line 15
set
      17
            return-void
      18 .end method
fa
      19
      20 .method public constructor <init>() V
            .locals 0
      21
      22
      23
            .prologue
      24
            .line 7
            invoke-direct {p0}, Landroid/app/Application;-><init>() V
      25
      26
```

#### 两个函数,一般用于加固

```
# virtual methods
.method protected native attachBaseContext(Landroid/content/Context;) V
.end method
.method public native onCreate() V
.end method
```

## 找到该so文件 , IDA动态调试

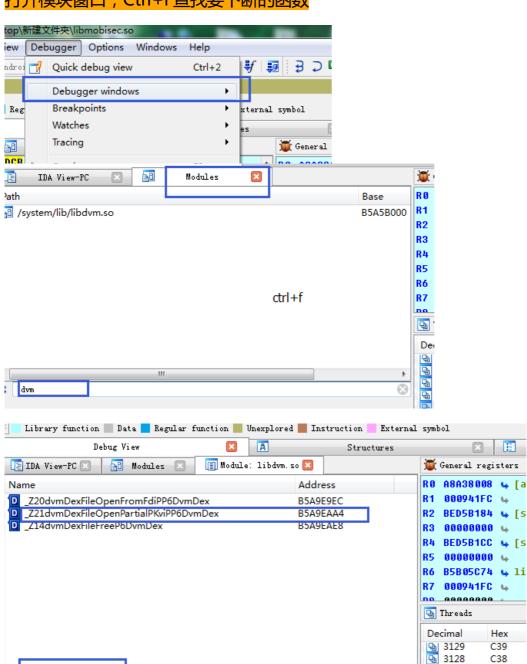


### 打开模块窗口,Ctrl+F查找要下断的函数

dvmdexfile

1039408F FF FF 52 7D 02 00 49 7F 02 00 78 FC FF FF 40 FC

O Hex View-1



면 면 3127

3126 3122 C37

C36

C32

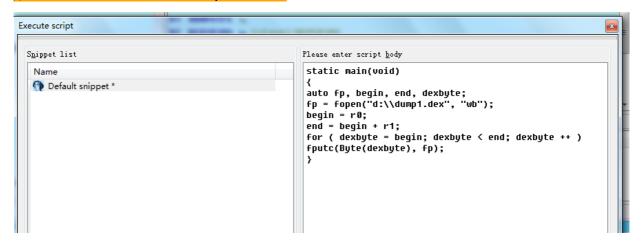
## <mark>//安装要脱壳的软件</mark> //命令行调试启动

```
D:\>adb shell
root@generic:/ # cd ./data/local/tmp
root@generic:/data/local/tmp # ./android_server
IDA Android 32-bit remote debug server($T) v1.19. Hex-Rays (c) 2004-2015
Listening on port #23946...
[1] Accepting connection from 127.0.0.1...
```

## //断下来后查看下寄存器值,r0,r1,在内存中 //确定是dex后dump

```
Library function 💹 Data 🚾 Regular function 💹 Unexplored 🚾 Instruction 🥌 External symbol
                                    A
            Debug View
                                                                               × H
IDA View-PC 🛛 🚹 Modules 🗵 📋 Module: libdvm. so 🗵
                                                                        👿 General registers
 libdvm.so:B5A9EAA1 DCB 0xC2;
                                                                           A8A38008 🛶 [anon:libc_malloc]:A8A38008
 libdvm.so:B5A9EAA2 DCB
                                                                           000941FC L
 libdvm.so:B5A9EAA3 DCB
                                                                           BED5B184 😽 [stack]:BED5B184
 libdum.so:<mark>85A9EAA4</mark> CODE 16
libdum.so:<mark>85A9EAA4</mark> _221dumDexFileOpenPartialPKviPP6DvmDex DCI
                                                                       R3 000000000 w
 libdvm.so:B5A9EAA5 DCB 0xB5
libdvm.so:B5A9EAA6 DCB 0x14
                                                                       R4 BED5B1CC Lack1:BED5B1CC
                                                                       R5 000000000
 libdvm.so:B5A9EAA7 DCB 0x46 ; F
                                                                           B5805C74 🕒 libdvm.so:gDvmInlineOpsTable+868
 libdvm.so:B5A9EAA8 DCB
                                                                           000941FC 😽
 libdvm.so:B5A9EAA9 DCB 0x22 ; "
 libdvm.so:B5A9EAAA DCB
                          0x41
                                                                        🛂 Threads
 libdvm.so:B5A9EAAB DCB 0xF0
 libdvm.so:B5A9EAAC DCB
                          0xR9
                                                                                            State
                                                                        Decimal
                                                                                    Hex
 libdvm.so:B5A9EAAD DCB
                                                                        3129
3128
                                                                                            Ready
 libdvm.so:B5A9EAAE DCB
                                                                                            Ready
 libdvm.so:B5A9EAAF DCB 0x46
                                                                                    C37
                                                                           3127
                                                                                            Ready
                                 omDexFileOpen (Synchronized with PC)
 UNKNOWN B5A9EAA4: libdym.so:
                                                                           3126
                                                                                            Ready
                                                                        맙
 4
                                                                                            Ready
                                                                                                            □ ♂ × | ○ Stack wiew
fex View-1
37FF8
                                                              dex.035.1P4.
      64 65 78 0A 30 33 35 00
                                   6C 50 34 D8 82 04 15 79
                                                                                                                     BED5B14C
                                                                                                                                 0000003
18018
      EB 32 41 72 B7 D9 CE A3 FC 41 09 00 70 00 00 00
                                  6D 51 E6 41 96 56 BC 9D
                                                              .2Ar...mQ.A.V..
.A..p...xV4....
                                                                                                                      REDSR150
                                                                                                                                 0000000
                                  78 56 34 12 00 00 00 00
38028
                                                                                                                      BED5B154
                                                                                                                                B6F53FE
                00 20 41
                          09 00
                                  F0 18 00 00 70 00 00 00
                                                                                                                      BED5B158
                                                                                                                                 B5A5A06
18 048
       02 04 00 00 30 64 00 00
                                  2A 05 00 00 38 74 00 00
                                                                                                                      BED5B15C AC3C22B
                                      19 88 88 F8 F6
static main(void)
{
auto fp, begin, end, dexbyte;
fp = fopen("d:\\dump1.dex", "wb");
begin = r0:
end = begin + r1;
for ( dexbyte = begin; dexbyte < end; dexbyte ++ )
fputc(Byte(dexbyte), fp);
```

#### //运行脚本:菜单file->SCripcomman

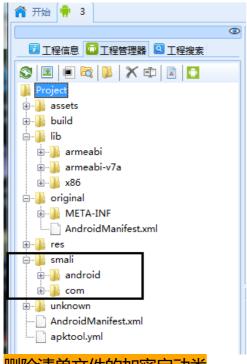


//在d盘目录下找到我们的文件,修复,反编译
Android逆向助手 v2.2
选择:
源文件: C:\Users\laiwenjie\Desktop\新建文件夹\dump1 dex
目标文件: C:\Users\laiwenjie\Desktop\新建文件夹\dump1

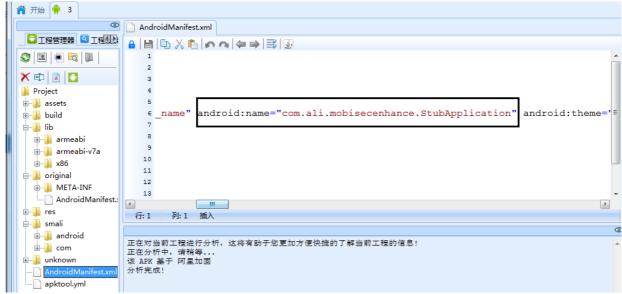
反编译 字符串 选项
操作:
反编译apk ● 重打包apk ● 签名apk ● 提取dex ● 替换dex ● 修复dex
● 反编译dex ● 重打包dex ● dex转dx ● dex转txt ● dex转jar ● jar转dex
● 反汇编elf ● xml转txt ● jd打开jar ● apk对齐

日志:

#### 在原有的smali目录下,右键,路径。将修复反编译的dex文件拷贝在打开的路径下



删除清单文件的加密启动类



最后保存编译就可以了