

怎么用Unidbg把数美SDK里的函数跑起来？本篇做了这方面的尝试和分析，感谢我的朋友nu11进行审稿和技术指导。

样本链接：<https://pan.baidu.com/s/1lIIFUQ9X2MiFScbWbJoXpLw>

提取码：te2q



```
1 package com.ishumei.dfp;
2
3 import android.content.Context;
4 import androidx.annotation.Keep;
5
6 @Keep
7 public class SMSDK {
8     static {
9         try {
10             System.loadLibrary("smsdk");
11         } catch (Throwable unused) {
12         }
13     }
14
15     public static String v1(Context context, String str, String str2, String str3, String str4, String str5) {
16         return new SMSDK().w1(context, str, str2, str3, str4, str5);
17     }
18
19     public static String v3(Context context, String str, String str2, String str3, String str4) {
20         try {
21             return new SMSDK().w3(context, str, str2, str3, str4);
22         } catch (Throwable unused) {
23             return "";
24         }
25     }
26
27     private native String w3(Context context, String str, String str2, String str3, String str4);
28
29     private native String x6(String str, String str2);
30
31     public static String xx6(String str, String str2) {
32         try {
33             return new SMSDK().x6(str, str2);
34         } catch (Throwable unused) {
35             return "";
36         }
37     }
38
39     public native String w1(Context context, String str, String str2, String str3, String str4, String str5);
40 }
```

w1是我们待分析的函数。首先跑一份JNItrace，使用Unidbg做分析时，第一步永远应该是JNItrace，JNI是引路明灯，如果JNItrace崩了或者样本有Frida反调试，补Unidbg时不确定性就会大很多，甚至如盲人摸象。

```
1159     /* TID 14857 */
1160     4106 ms [+]
1161     4106 ms | - JNIEnv* : 0xba872620
1162     4106 ms | - jobject : 0x51 { javax/crypto/Cipher }
1163     4106 ms | - jmethodID : 0x704c0a6c { doFinal([B][B] }
1164     4106 ms | - va_list : 0xb90333f0
1165     4106 ms |: jbyteArray : 0xe1
1166     4106 ms |= jobject : 0x109
1167
1168     4106 ms -----Backtrace-----
1169     4106 ms |-> 0xb1ea7aef: libmsdk.so!0x49aef (libmsdk.so:0xb1e5e000)
1170
1171
1172     /* TID 14857 */
1173     4122 ms [+]
1174     4122 ms | - JNIEnv* : 0xba872620
1175     4122 ms |= jboolean : 0 { false }
1176
1177     4122 ms -----Backtrace-----
1178     4122 ms |-> 0xb1e8ba3f: libmsdk.so!0x2da3f (libmsdk.so:0xb1e5e000)
1179
1180
1181     /* TID 14857 */
1182     4138 ms [+]
1183     4138 ms | - JNIEnv* : 0xba872620
1184     4138 ms | - jobject : 0xf5
1185
1186     4138 ms -----Backtrace-----
1187     4138 ms |-> 0xb1e7990f: libmsdk.so!0x1b90f (libmsdk.so:0xb1e5e000)
1188
1189
1190     /* TID 14857 */
```

接下来进入Unidbg

```
package com.jiuwu;

import com.github.unidbg.AndroidEmulator;
import com.github.unidbg.Emulator;
import com.github.unidbg.Module;
import com.github.unidbg.file.FileResult;
import com.github.unidbg.file.IOResolver;
import com.github.unidbg.linux.android.AndroidEmulatorBuilder;
import com.github.unidbg.linux.android.AndroidResolver;
import com.github.unidbg.linux.android.dvm.AbstractJni;
import com.github.unidbg.linux.android.dvm.DalvikModule;
import com.github.unidbg.linux.android.dvm.VM;
import com.github.unidbg.memory.Memory;
import com.github.unidbg.virtualmodule.android.AndroidModule;

import java.io.File;

public class shumei extends AbstractJni implements IOResolver {
    private final AndroidEmulator emulator;
    private final VM vm;
    private final Module module;

    shumei() {
        // 创建模拟器实例，进程名建议依照实际进程名填写，可以规避针对进程名的校验
        emulator = AndroidEmulatorBuilder
                .for32Bit()
                .setRootDir(new File("target/rootfs"))
                .build();

        // 获取模拟器的内存操作接口
        final Memory memory = emulator.getMemory();
```

```

// 设置系统类库解析
memory.setLibraryResolver(new AndroidResolver(23));
// 绑定重定向
emulator.getSyscallHandler().addIOResolver(this);

vm = emulator.createDalvikVM(new File("unidbg-
android/src/test/resources/shumei/com.jiuwu_1.25.0_1002500.apk"));
new AndroidModule(emulator, vm).register(memory);
DalvikModule dm = vm.loadLibrary(new File("unidbg-
android/src/test/resources/shumei/libssdk.so"), true); // 加载so到虚拟内存
//获取本so模块的句柄,后续需要用它
module = dm.getModule();
vm.setJni(this);
vm.setVerbose(true); // 打印日志

dm.callJNI_OnLoad(emulator); // 调用JNI OnLoad
};

@Override
public FileResult resolve(Emulator emulator, String pathname, int oflags) {
    System.out.println("lilac Path:" + pathname);
    return null;
}

public static void main(String[] args) {
    shumei demo = new shumei();
}

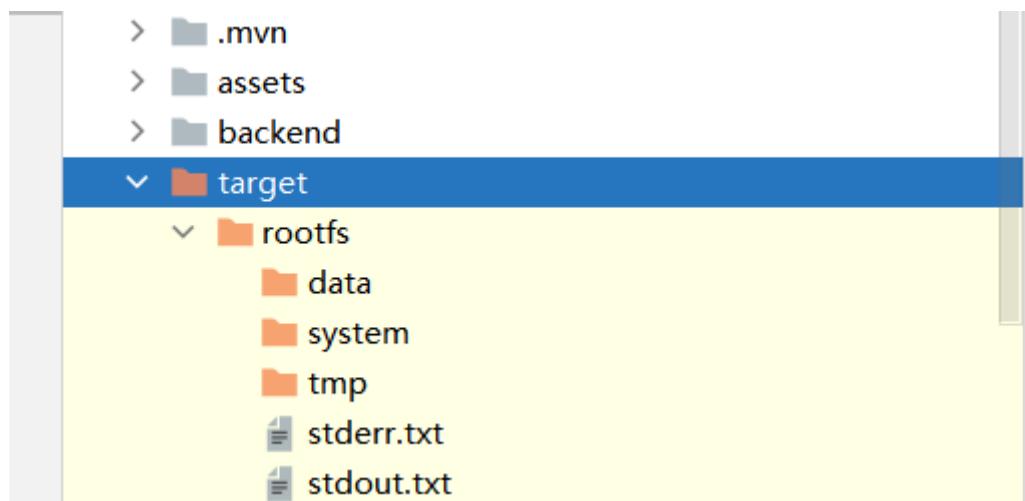
}

```

先前我们提过，样本中如果有文件的访问和操作，Unidbg有两个方式操作和控制文件。

- 使用虚拟文件系统，将样本中对Android文件系统的访问重定位到本机电脑的某个目录或者叫文件夹，按照Android系统中的层级关系将文件放到这个文件夹里就可以了。

初始化模拟器中的 `setRootDir(new File("target/rootfs"))` 是指定当前项目的文件系统位置，运行测试你会在Unidbg目录中看到它。假设要访问tmp/a.txt，你可以将电脑里的a.txt通过adb pull出来，然后放在target/rootfs/tmp下，Unidbg即可完成该样本中对该文件的访问。



这种方式是好的，但有时候我们需要更灵活的文件重定位。

- 使用代码，虚拟文件系统本身也说对代码的封装。

三步骤，缺一不可。

```
10 import com.github.Unidbg.linux.android.dvm.AbstractJni;
11 import com.github.unidbg.linux.android.dvm.DalvikModule;
12 import com.github.unidbg.linux.android.dvm.VM;
13 import com.github.unidbg.memory.Memory;
14 import com.github.unidbg.virtualmodule.android.AndroidModule;
15
16 import java.io.File;
17
18 public class shumei extends AbstractJni implements IOResolver {①
19     private final AndroidEmulator emulator;
20     private final VM vm;
21     private final Module module;
22
23     shumei() {
24         // 创建模拟器实例, 进程名建议依照实际进程名填写, 可以规避针对进程名的校验
25         emulator = AndroidEmulatorBuilder
26             .for32Bit()
27             .setRootDir(new File( pathname: "target/rootfs"))
28             .build();
29
30         // 获取模拟器的内存操作接口
31         final Memory memory = emulator.getMemory();
32         // 设置系统类库解析
33         memory.setLibraryResolver(new AndroidResolver(sdk: 23));
34         // 绑定重定向
35         emulator.getSyscallHandler().addIOResolver(this);②
36
37         vm = emulator.createDalvikVM(new File( pathname: "unidbg-android/src/test/resources/shumei/com.jiuwu_1.25.0_1002500.apk"));
38         new AndroidModule(emulator, vm).register(memory);

```

```
30
31     vm = emulator.createDalvikVM(new File( pathname: "unidbg-android/src/test/resources/shumei/com.jiuwu_1.25.0_1602500.apk"),
32         new AndroidModule(emulator, vm).register(memory);
33     DalvikModule dm = vm.loadLibrary(new File( pathname: "unidbg-android/src/test/resources/shumei/libssmsdk.so"), forceCallInit: true);
34     // 获取本SO模块的句柄, 后续需要用它
35     module = dm.getModule();
36     vm.setJni(this);
37     vm.setVerbose(true); // 打印日志
38
39     dm.callJNI_OnLoad(emulator); // 调用JNI OnLoad
40 }
41
42 @Override
43 public FileResult resolve(Emulator emulator, String pathname, int oflags) {
44     System.out.println("lilac Path:" + pathname);
45     // 具体的处理
46     return null;
47 }
48
49 public static void main(String[] args) {
50     shumei demo = new shumei();
51 }
52
53 }
```

绑定文件重定向这一步，大家很容易忘记，如果没这么一步，我们的文件重定向是无法实现的。我们这里两种文件重定向都使用了，会冲突吗？

——并不。

你可以通过虚拟文件系统补tmp/a.txt，然后通过代码补tmp/b.txt，这是完全没问题的，怎么方便怎么来。

那么如果样本中访问了tmp/c.txt，我既在虚拟文件系统的tmp里放一个c.txt，又通过代码方式补一个c.txt，会发生什么呢？

这里就有一个优先级的问题，如果两种操作都存在，代码方式的优先级更高。

为什么我们要在开头就讲文件重定向呢？因为作为一个搞设备唯一ID的SDK，它对信息的收集应该是很惊人的，应该会有很多文件访问，所以先做好准备嘛。

运行代码

```
lun: shumei > "C:\Program Files\Java\jdk-16.0.1\bin\java.exe" ...
lilac Path:/dev/_properties...
lilac Path:/proc/stat
JNIEnv->FindClass(com/ishumei/dfp/SMSDK) was called from RX@0x400176af[libsmsdk.so]0x1760f
JNIEnv->RegisterNatives(com/ishumei/dfp/SMSDK, RW@0x400d3610[libsmsdk.so]0xd3010, 3) was called from RX@0x40017723[libsmsdk.so]0x17723
RegisterNative(com/ishumei/dfp/SMSDK, w1(Landroid/content/Context;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;), R@0x40017795[libsmsdk.so]0x17095)
RegisterNative(com/ishumei/dfp/SMSDK, x6(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;, RX@0x40017095[libsmsdk.so]0x17095)
RegisterNative(com/ishumei/dfp/SMSDK, w3(Landroid/content/Context;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;), RX@0x40016f41[libsmsdk.so]0x16f41)
Process finished with exit code 0
```

我们发现，它正常的完成了函数注册。似乎发生了两次文件访问？不用担心，开头这两次访问不是样本的操作，是libc中的固定流程，不用我们管。

我心里不太踏实，因为它做的实在太少了？到NIOOnLoad截至怎么啥都没做？担心有诈，把Unidbg日志全开一下。（src/test/resources/log4j.properties中全部INFO改成DEBUG）

好像还是看不出啥。。。那算了，可能真没有，或者我眼拙辽。

```
public void w1(){
    List<Object> list = new ArrayList<>(10);
    list.add(vm.getJNIEnv());
    list.add(0);
    DvmObject<?> obj =
    vm.resolveClass("android/content/Context").newObject(null);
    list.add(vm.addLocalObject(obj));
```

```
String str2 = "
{\\"a1\\":\\"a11\\",\\"a3\\":\\"none\\",\\"a4\\":\\"4\\",\\"a2\\":\\"SRCM3hsEtSjSE1fQv1Cares092
5Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOCiXTuZJ+Va9w5pRw==\\",\\"a5\\":\\"\\",\\"a
7\\":\\"3.0.4\\",\\"a8\\":\\"\\",\\"a6\\":\\"android\\",\\"a44\\":\\"wifi\\",\\"a47\\":
[\"16, qualcomm\", \"4, qualcomm\", \"19, qualcomm\", \"19, qualcomm\", \"9, qualcomm\",
\"18, qualcomm\", \"18, qualcomm\", \"17, qualcomm\", \"22, qualcomm\", \"2, akm\", \"10, qu
alcomm\", \"20, qualcomm\", \"3, xiaomi\", \"30, qualcomm\", \"30, qualcomm\", \"33171027
,xiaomi\", \"33171027,xiaoMi\", \"33171036,xiaoMi\", \"33171036,xiaoMi\", \"11,xiaom
i\", \"5,Rohm\", \"5,Rohm\", \"6,Bosch\", \"29, qualcomm\", \"29, qualcomm\", \"1, qualco
mm\", \"35, qualcomm\", \"15, qualcomm\", \"27,xiaomi\", \"27,xiaomi\", \"33171029,xiao
Mi\", \"33171029,XiaoMi\", \"14, akm\", \"33171070,xiaomi\", \"33171070,xiaomi\", \"8,
Elliptic Labs\", \"33171031,xiaomi\"],\"a46\\":{\"cpu_abi\"::\\armeabi-
v7a\\\",\"serial\":\\\"unknown\\\",\"fingerprint\":\\\"Xiaomi\\\\polaris\\\\polaris:10\\\\Q
KQ1.190828.002\\\\V12.0.2.0.QDGCNXM:user\\\\release-keys\\\",\"model\":\\\"MIX
2S\\\",\"cpu_abi2\":\\\"armeabi\\\",\"brand\":\\\"Xiaomi\\\",\"board\":\\\"sdm845\\\",\"serial
_P\\\":\\\"unknown\\\",\"manufacturer\":\\\"Xiaomi\\\"},\"a38\\\":\\\"1.25.0\\\",\"a33\\\":\\\"ARMv8
Processor rev 13
(v81)\\\",\"a103\\\":\\\"faf6c8c7ad942343\\\",\"a23\\\":\\\"\\\",\"a54\\\":\\\"0000010\\\",\"a48\\\":5
905514496,\"a10\\\":\\\"10\\\",\"a11\\\":\\\"95fen\\\",\"a15\\\":\\\"false\\\",\"a17\\\":
[\\\"wlan1,,f460e217db64,\\\",\\\"wlan0,172.16.16.12,f460e296db64,fe80::f660:e2ff:fe96
:db64%wlan0\\\",\\\"p2p0,,f660e218db64,\\\"],\"a18\\\":
{\\\"ro.boot.hardware\\\":\\\"qcom\\\",\\\"gsm.sim.state\\\":\\\"LOADED_LOADED\\\",\\\"sys.usb.sta
te\\\":\\\"adb\\\",\\\"ro.debuggable\\\":\\\"0\\\"},\"a19\\\":\\\"02:00:00:00:00:00\\\",\"a9\\\":16281
28282220,\"a39\\\":\\\"com.jiuwu\\\",\"a40\\\":1627972313927,\"a45\\\":\\\"46001\\\",\"a21\\\":
\\\",\"a24\\\":\\\"6d9de21492b99db9\\\",\"a25\\\":\\\"\\\",\"a22\\\":\\\"\\\",\"a34\\\":2803200,\"a37
\\\":1295,\"a27\\\":
[\\\"1628127546162,com.jiuwu,,1,1002500,1.25.0,1628127546162\\\",\\\"1230768000000,com
.android.cts.priv.ctsshim,,0,28,9-
5374186,1230768000000\\\",\\\"1230768000000,com.miui.contentextension,,0,10164,2.4.2
,1611338104848\\\",\\\"1230768000000,com.qualcomm.qti.qcolor,,0,29,10,1230768000000\\
\",\\\"1230768000000,com.android.internal.display.cutout.emulation.corner,,0,1,1.0,
1230768000000\\\",\\\"1230768000000,com.google.android.ext.services,,0,291900801,q_p
r1-
release_am1_291900801,1230768000000\\\",\\\"1230768000000,com.qualcomm.qti.improveto
uch.service,,0,29,10,1230768000000\\\",\\\"1230768000000,com.android.internal.displa
y.cutout.emulation.double,,0,1,1.0,1230768000000\\\",\\\"1230768000000,com.android.p
roviders.telephony,,0,29,10,1230768000000\\\",\\\"1230768000000,com.android.dynsyste
m,,0,29,10,1230768000000\\\"],\"a29\\\":\\\"4.0.c2.6-00335-0914_2350_3c8fca6,4.0.c2.6-
00335-0914_2350_3c8fca6\\\",\"a32\\\":8,\"a30\\\":\\\"<unknown
ssid>\\\",\"a31\\\":\\\"172.16.16.12\\\",\"a90\\\":28,\"a105\\\":
{},\"a108\\\":\\\"\\\",\"a109\\\":\\\"\\\",\"a110\\\":\\\"\\\",\"a111\\\":\\\"\\\",\"a107\\\":
{\\\"java\\\\lang\\\\reflect\\\\Modifier\\\":2,\\\"com\\\\android\\\\internal\\\\telephony\\\\
/PhoneProxy\\\":2,\\\"java\\\\lang\\\\ProcessBuilder\\\":2,\\\"com\\\\android\\\\internal\\\\
telephony\\\\PhoneSubInfo\\\":2,\\\"android\\\\location\\\\LocationManager\\\":2,\\\"com\\\\
tencent\\\\mapapi\\\\service\\\\LocationManager\\\":2,\\\"com\\\\android\\\\internal\\\\te
lephony\\\\gsm\\\\GSMPhone\\\":2},\"a20\\\":\\\"\\\",\"a49\\\":\\\"\\\",\"a52\\\":
{\\\"magisk\\\":1},\"a53\\\":{},\"a50\\\":
{},\"a60\\\":\\\"u0_a349\\\",\"a62\\\":\\\"\\\\data\\\\user\\\\0\\\\com.jiuwu\\\\files\\\",\"a55\\
\":\\\"a58929cd0e3202053f6137261ecd3c40\\\",\"a57\\\":1160259262,\"a36\\\":\\\"1080,2030,44
0\\\",\"a56\\\":\\\"CN=jiuwu, OU=jiuwu, O=jiuwu, L=上海, ST=上海,
C=CN\\\",\"a76\\\":\\\"\\\",\"a88\\\":\\\"locateServiceName:android.os.BinderProxy|phoneServ
iceName:android.os.BinderProxy\\\",\"a84\\\":\\\"3vDSuAiODgqAwBUsIqCEpuAFJ+xKBFFJ383k
+\\\\M2+M=____\\\",\"a68\\\":
[],\"a92\\\":\\\"1080,2030\\\",\"a93\\\":0,\"a95\\\":-1,\"a96\\\":\\\"du56APPx0pvUi
zMTZXVP\\\",\\\"a97\\\":\\\"SRCM3hsEtSjSE1fQv1Cares0925Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOC
iXTuZJ+Va9w5pRw==\\\",\"a98\\\":\\\"\\\",\"a99\\\":\\\"\\\",\"a100\\\":\\\"\\\",\"a101\\\":\\\"\\\",\"a102
\\\":[],\"a63\\\":\\\"InputMethodInfo{com.sohu.inputmethod.sogou.xiaomi\\\\.SogouIME,
settings:
```

```
com.sohu.inputmethod.sogou.SogouIMESettingsLauncher}\\"", \"InputMethodInfo{com.iflytek.inputmethod.miui\\/.FlyIME, settings:  
com.iflytek.inputmethod.LauncherSettingsActivity\"]}, \"a67\": {}, \"a64\":  
{} , \"suc\": \"1\" , \"enable\": \"0\" , \"service\": [] } , \"a65\": 39 , \"a66\":  
{} , \"a74\": 0 , \"a73\": 0 , \"a78\": [] , \"a75\": 0 , \"a77\":  
{} , \"a86\": \"1100100\" , \"a79\": \"\" , \"a80\": \"1628128282029-  
12295\" , \"a83\": \"1001100\" , \"a85\":  
[] , \"a69\": 15533490176 , \"a71\": 118982303744 , \"a72\":  
{} , \"temp\": 370 , \"vol\": 4095 , \"level\": 85 , \"scale\": 100 , \"status\": 2 } , \"a70\": 1568  
4485120 } ;
```

```
    String str3 = "
{\\"all_atamper\\":true,\\"core_atamper\\":true,\\"hook_java_switch\\":true,\\"hook_switc
tch\\":false,\\"risk_apps\\": [{"\"xposed\\":
{\\"pn\\":\"de.robv.android.xposed.installer\",\"uri\\\":\"\"}, {\\"controllers\\":
{\\"pn\\":\"com.soft.controllers\",\"uri\\\":\"\"}, {\\"apk008v\\":
{\\"pn\\":\"com.soft.apk008v\",\"uri\\\":\"\"}, {\\"apk008Tool\\":
{\\"pn\\":\"com.soft.apk008Tool\",\"uri\\\":\"\"}, {\\"ig\\":
{\\"pn\\":\"com.doubee.ig\",\"uri\\\":\"\"}, {\\"anjian\\":
{\\"pn\\":\"com.cyjh.mobilejian\\\",\"uri\\\":\"\"}, {\\"rktech\\":
{\\"pn\\":\"com.ruokuai.rktech\",\"uri\\\":\"\"}, {\\"magisk\\":
{\\"pn\\":\"com.topjohnwu.magisk\",\"uri\\\":\"\"}, {\\"kinguser\\":
{\\"pn\\":\"com.kingroot.kinguser\",\"uri\\\":\"\"}, {\\"substrate\\":
{\\"pn\\":\"com.saurik.substrate\",\"uri\\\":\"\"}, {\\"touchsprite\\":
{\\"pn\\":\"com.touchsprite.android\",\"uri\\\":\"\"}, {\\"scriptdroid\\":
{\\"pn\\":\"com.stardust.scriptdroid\",\"uri\\\":\"\"}, {\\"toolhero\\":
{\\"pn\\":\"com.mobileuncle.toolhero\",\"uri\\\":\"\"}, {\\"huluxia\\":
{\\"pn\\":\"com.huluxia.gametools\",\"uri\\\":\"\"}, {\\"apkeditor\\":
{\\"pn\\":\"com.gmail.heagoo.apkeditor.pro\",\"uri\\\":\"\"}, {\\"xposeddev\\":
{\\"pn\\":\"com.sollyu.xposed.hook.model.dev\",\"uri\\\":\"\"}, {\\"anywhere\\":
{\\"pn\\":\"com.txy.anywhere\",\"uri\\\":\"\"}, {\\"burgerzws\\":
{\\"pn\\":\"pro.burgerz.wsm.manager\",\"uri\\\":\"\"}, {\\"vdloc\\":
{\\"pn\\":\"com.virtualdroid.loc\",\"uri\\\":\"\"}, {\\"vdtxl\\":
{\\"pn\\":\"com.virtualdroid.txl\",\"uri\\\":\"\"}, {\\"vdwzs\\":
{\\"pn\\":\"com.virtualdroid.wzs\",\"uri\\\":\"\"}, {\\"vdkit\\":
{\\"pn\\":\"com.virtualdroid.kit\",\"uri\\\":\"\"}, {\\"vdwxg\\":
{\\"pn\\":\"com.virtualdroid.wxg\",\"uri\\\":\"\"}, {\\"vdgps\\":
{\\"pn\\":\"com.virtualdroid.gps\",\"uri\\\":\"\"}, {\\"a1024mlloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\"}, {\\"drhzg\\":
{\\"pn\\":\"com.deruhai.guangzi.noroot2\",\"uri\\\":\"\"}, {\\"yggb\\":
{\\"pn\\":\"com.mcmonjmb.yggb\",\"uri\\\":\"\"}, {\\"xsrv\\":
{\\"pn\\":\"xiake.xserver\",\"uri\\\":\"\"}, {\\"fakeloc\\":
{\\"pn\\":\"com.dracrays.fakeloc\",\"uri\\\":\"\"}, {\\"ultra\\":
{\\"pn\\":\"net.anylocation.ultra\",\"uri\\\":\"\"}, {\\"locationcheater\\":
{\\"pn\\":\"com.wifi99.android.locationcheater\",\"uri\\\":\"\"}, {\\"dwzs\\":
{\\"pn\\":\"com.dingweizhou\",\"uri\\\":\"\"}, {\\"mockloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\"}, {\\"anywhereclone\\":
{\\"pn\\":\"com.txy.anywhere.clone\",\"uri\\\":\"\"}, {\\"fakelocc\\":
{\\"pn\\":\"com.dracrays.fakelocc\",\"uri\\\":\"\"}, {\\"mockwxlocation\\":
{\\"pn\\":\"com.tandy.android.mockwxlocation\",\"uri\\\":\"\"}, {\\"anylocation\\":
{\\"pn\\":\"net.anylocation\",\"uri\\\":\"\"}, {\\"totalcontrol\\":
{\\"pn\\":\"com.sigma_rt.totalcontrol\",\"uri\\\":\"\"}, {\\"ipjl2\\":
{\\"pn\\":\"com.chuangdian.ipjl2\",\"uri\\\":\"\"}], {\\"risk_dirs\\": [{"\"008Mode\\":
{\\"dir\\\":\".system/008Mode\", \"type\\\":\"sdcard\"}, {\\"008OK\\":
{\\"dir\\\":\".system/008OK\", \"type\\\":\"sdcard\"}, {\\"008system\\":
{\\"dir\\\":\".system/008system\", \"type\\\":\"sdcard\"}, {\\"iGrimace\\":
{\\"dir\\\":\"iGrimace\", \"type\\\":\"sdcard\"}, {\\"touchelper\\":
{\\"dir\\\":\"/data/data/net.aisence.Touchelper\", \"type\\\":\"absolute\"}, {\\"elfscript\\":
{\\"dir\\\":\"/mnt/sdcard/touchelf/scripts/\", \"type\\\":\"absolute\"}, {\\"spritelua\\": {\\"dir\\\":\"/mnt/sdcard/TouchSprite/lua\", \"type\\\":\"absolute\"}, {\\"spritelog\\": {\\"dir\\\":\"/mnt/sdcard/TouchSprite/log\", \"type\\\":\"absolute\"}, {\\"assistant\\": {\\"dir\\\":\"/data/data/com.xxAssistant\", \"type\\\":\"absolute\"}, {\\"assistantscript\\":
{\\"dir\\\":\"/mnt/sdcard/com.xxAssistant/script\", \"type\\\":\"absolute\"}, {\\"mobilejian\\":
{\\"dir\\\":\"/data/data/com.cyjh.mobilejian\", \"type\\\":\"absolute\"}], {\\"risk_file_switch\\": true, {\\"risk_files\\": \"zb5E/i2Gv4IxR50xSBiXKChu8gdkDXKei9GwOBNbN6jq3xMULFFAvT94C0wwwhychgUggyBRjbNG1gz0dh171P0b7ZnqdDPKYq5NrmMJr3Fwtzccme/nv4R00yuTb

```

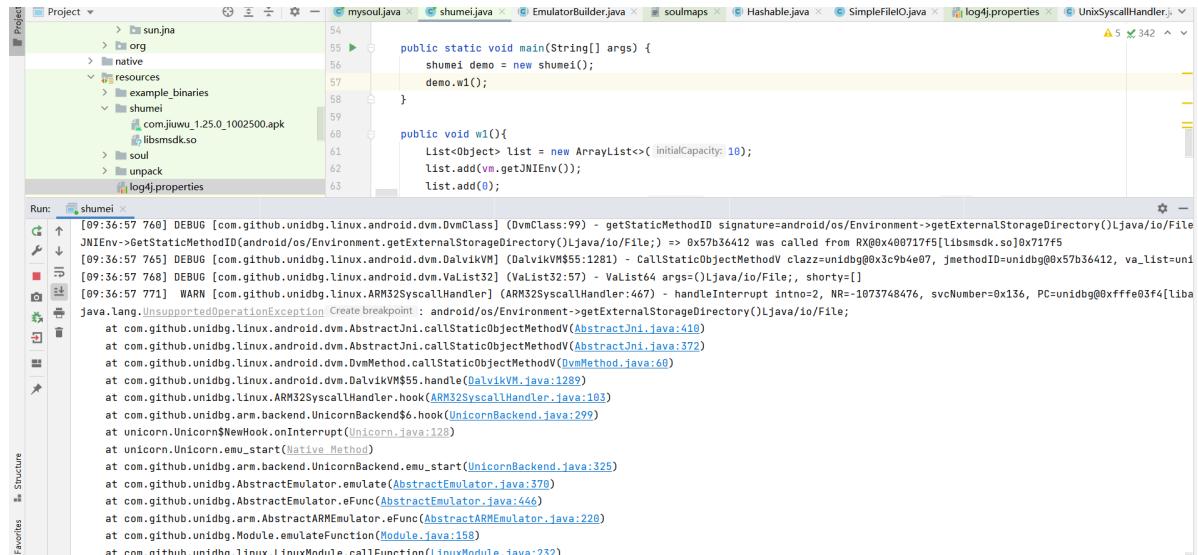
f1jc3DdFuA8eOMaLkvLFfsxnx13Jdu6ZY38LTdbc+h2fnf4KnsRbgcZ5JVfaeiKz5HFQvKzjKJH6x/uQ  
i190PF2kpg4uRmTDh6ev0En0RGh9Jg318Nr0xd87izNvUg5Jg941Q/FX98DYetR2RYe3Sp/9u+cT1EnE  
SikjyMxGjaJ3R1TQ701LfuNwqceVsYw99YeNkCwwTBMQII5a3/2i09HzxRXXiswvk23Txt41xmumhs5  
HDmj6D1/oeQ6oFHqsfd3c/auB0vFrxrqbNH68H9pw/b2wpYnnAJsgYxowaz1MaQj5Y21IGkzz7jSeTN2  
IJFTzPsHesHc2K4QS7OSWju/d1rCrA5BXSn05TIGXNukm2AwPEtduBeg4FpR7Lb/Vi0K0cgry4gVRPV1  
QnNbR5mjI2fs30C1sdZibJG2sZxo56BxeF8HzXDpBr03T+Nqg77E4cynk9a57kkq0eA1RaZn8yHJws4q  
97tFrusokRbcFwmVkyeJ5z1rbwLevZ9fkTcyy3VIQY3E2mwR7kaAJepds1+iDeJBHZwBKUBPJqoPoiE0  
uKTnn8KmvyKjb+Jc8mYXR/mgT1r0c6Cgn6CM9BfynzrJoyTmlXzy2tm6dn66eHM5tsplzG0c3JEgvB2T  
5nSyAc9X0u9/rIbsWQ/8OUNFz2pu7vbfgyswakkPKMbksj3MsRHHE6mljv/P0rEtunth5/KwH1JQBWW  
R/1epqywjoev2fiJ5FqGTvBt6ZTESeAx+9AIUhv9nMx32sVw0VmIIjv6R8UUoa1b5EZHYcm804BEszx2  
/ke/e+1dEvw5ntT0khvme5HIX9Qn0uz6u+gQpJds2aVHMGOXI670xhepwaMskl1tu268x53PYc+rjx  
NXNbKGGD+kJAISPF4d2u0tbVNf57cy1sIF4HK8+7FPxn6gqd4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc  
sWSmmWIQQZE9ri0ubxSFLThQMUW2tI0GFHCJVsppIQtmxz6M9bTuerjd0Ii5oamMswxK3MkAyM1581u  
d05x4ycwfouRXOoxerpjvEmT4jfJJRh86ud/Ecihm6Fp5dm8r4Hg9nPQKebng/Gjl1+/n0S0dpaq/4rQ  
vIk2GWN7Q/M7BboqN7+5ou4qkcyOHaGC8H90YpwrlhzB/IEYhgBvCePKW6bGkiPBReu72+Bmhgb5KaPN  
JYLFWcdsN9+df7DcvpVcmntsM56HnKLym168o8XHJIhawjajkElhsqy1s0FOOu1EcN90coIPi7XQFI  
Q2jk7A1qits1bKhtp0m49jcsomHBwqqT5kNno6WF6xiNXODhIZ3diLHXHe1kfWPjpnPZzq2FugBvj0Tx  
+tftPYoGwi1jvlu4sBeGez4jcfi2qkCofjm7EeMojox6BuBF3HKjUV+bugusy5BF8qFhb1azop/0++qHt  
BtGkQejeqESFZWWxjhsrHja68rPa0YDxxCl1tH4xS+38tFWKqgbKovck+2udz1auCSA0etjqfzz70fj  
C4hwJp8wCDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiV06e70sayn1kppG1RW1UmGhLe5g08WDB  
IO1MGFSJMffn1gt90nJxpWQoymcUM6tuAKSoim0aExqsvK+SIHI/dchN6tiFaHLzesXhqXaHpbixVqDa  
D8gHN/yMR4IEY8e0ohVLwPAFZIWuGPdz3bgqQBmerdLp1zHrzCjWLsoaskyDWW0G0RjkP/YSWK+s1dLe  
wadQpFAtt6x7c5DnkdmvmsxxF7a3fG7G0Tk8miLwSmpgIij80w/oLCbUgYDGEpjGiSG6XEHPktc6ThTs  
+czc2QNgBi15g12NABEHQKxc3tzykwspoaamWrDe8vNCuKd+Tkk+q0zw66LTmE+maWX56TAQY50MQXOr  
H+6c5iULwda9Qn6rDSVNpTAN6KU6duxDb23QYthBd2orBq6T0Z8NLc8h6QVA9QEG7zs9j/fz/st94xi  
tuk8jkvr131f6bD646ixTx27NzzoQEt2E1s/ZM/iaAxwlaohOKKO5adtDATLyL7Ia1vdwdQz0XGwzus  
IKUjxDIrB0JzgCuGwg2Cj5cRL059Kfs0hgYv8rRgTa41vJcvuhEi6VtpFbGwv+T0C7Zx3xNPmnAVDwth  
UDPKu36z2wzzp89p6qrw7k0UwnN7XiGaV5Lv1Hcih7FnwLe107Mdvg41TprLFMLTwccwjhLf5mrIh6et  
Y5Zqp5ikVKv4vrb0s0SqqFLbz0Zj4KshyT2Yzaz7ZK5uQRF2f2u8gPYwn0oF4C8rNbbkdxAzoierX/s7m  
01AMD0Bjss1Lgc180v1jcn5u2drqQm1rkTG5r1k0140fTkoKnjyj90zxrD7/khxs6+Pwv6v3Czcdr8  
ojX+7MqmZxVEsdceHzE7gCfR17kb1H8bTzhaQPqh09vDLAo8RjtD2HHjYt2Qvjing8PtX57+/TBuIVPD  
wog6p8mi1hqzlhouzVpbhdruYqlhh45sbT99ydfs2j6/zovv84c8se1bq//zh3jku74boayGDzKjsr8u  
NbDZ5sP4DMFg/Zxqnku0nSjjv1p/DU1mfDZA+kzn8Iad/5sdedyjmPb2yIag0uEjvjt0qz6FeoT2h7m  
MVLwBCMy12Wk+0tTXL2xEpA63Y7Mfxymj8R2Deax6WRz96Io10Gr8+11Tsav16EHHanMJdy94Es+s+x  
00yvJnRybbNn1qvqu4FcE+16EeDiojoqbaczz0Ys6zkpcyIdrlmIbdxjcdxq1Zcw9FQXXNvREKf0k9PE  
DmHJQ8y2hJTTyqaSVqu7imgbOPR1GBV4Eu2/r1euLftwR1mZc6cfRqre9Y0GazGsnHyYh60k135z1bsx  
uNaGogr/ow32s5xuaq6026hdxdFvbwn7j30yvJ30rHEOGArj95DFnx2IURvMgYRrmUgwdCvmiNTLqzxf  
sbfbm2kUWGkp2mwa5RwrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8Ypgbs6Khh1jwvwTr7ah  
occhi1aa/9y53xuoB9cDrqbm08rj+4VFbyxkFMchY6rhoY23ok1ystqxxvdf5FjzndbHCenvmkz8Thju  
uSP3VOuVrUHAZssuyiqocQhr8gxPsc6k4XDzohrp+Yfzq5YbLT0nv4+FmTIJ8JWzy5axUG2oACiL8Lny  
pQ1qmTCBixpjFM5iQKPSVdkC0TmZ8b0T+UQLa2Yoxn5Thr0ktaTTN3GkeWq2DlmFkt0FCQcbjIawxy75  
RtuitkcooctFQ3xUNH7s/royb/sx1v+8ebi6L59L3x2PCvqoEXn9gsirr241oyxitrxsE1zaavrU9Y  
Zcb+a49A602Nrywn81dRPb5t02mUQRp/Kg1IjPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWdnI  
S+Djqn9pbhb8wroyxOFF8aehwul02hsgw91Rwz9umAfjEC4sSt8sc1ELaqaqwKnooKg7sevLq25b6toF  
ARwgdd8yTXH70jPniFuF+UE143yk912LwxFM/squ/UZP97RqbwuPu+bv2bYe3hiqbkj5xv5Toxgs6H3F  
u1lp2zyGwHGrxwoaqz+4/npkuJ7iLAv7y1g8s0zWfc86hPyRirv2Lna3gr0bnNUOCsfpcRwdkmBlyhn  
1bGqoj0iurBkjUbYPQ4G8jzoqujmq5xNyH60AQb0u7LdEDiC0HSUSI3SKzo1uESNSeE3qfv+UF87kzt  
eLj+RaqhAGN9nxstGn9F3yIUb76j13STbwwdEUzb7x8mhij9gQVLNFBR2tgrY=\", \"sensitive.ain  
fo\": true, \"sensitive.apps\": true, \"sensitive.aps\": true, \"sensitive.bssid\": tru  
e, \"sensitive.camera\": true, \"sensitive.cell\": true, \"sensitive.gps\": false, \"se  
nsitive.iccid\": true, \"sensitive.imsi\": true, \"sensitive.mac\": true, \"sensitive.  
ssid\": true, \"sensitive.tel\": false, \"white\_apps\": []}";

```

String str4 =
"\"MIIDLZCCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAYMQSwCQYDVQQGEWJDTjELMAKGA1UECwwCU00
xJjAUBgNVBAMMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDDE4WhcNNDAxMjAyMDMzMDE4WjAyMQs
WCQYDVQQGEWJDTjELMAKGA1UECwwCU00xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wggEiMA0GCSqGSIb
3DQEBAQUAA4IBDWAwggEKAoIBAQCT947yNGa4EPVheGp6hsDo4KBVmwcacn6tqfwit/j1xaZZBSPcw4
3jjxGuF4exM4NPJJtMft/j0IIwJeEx0YHDCJIqu/1pEPsXYb01bhwd5mq34c0RiRx1ji+g+d4rFRO/Xr
efRJSeB3w1djvoAMkxoygp+813zM6mzPd36zjbUIajfzkc5LoeITUCC6Db98XiN/hNmvcIwti01Sm9FE
U1ip1fFb9NZ04vb2Z6xt/ti/rUVzWyshZC1qqVq4s9W4iGPqfTnBsxttiooRuproe2LtB+J73kKTgJJH
60pn01jqd+FaMsL/sddY61ggM+w4ePTe4HF+/dv2ZzP+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
ZA5/0RAVrhwrYF1nyrex4FjAfBgNVHSMEGDAwgbS83RQZA5/0RAVrhwrYF1nyrex4FjAMBgnVHRMEBTA
DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZ06fn+mH124C8Djm15jCrjYqOISpgk
gsReEX2F00sxYqBuRPidycdsRNYQG44/i4PQrBwc9T/wLSOyHICaKbXXPhfw14PLRNR0LtgmcLoIveDy
jzTn3BEF57tzCYSmpHMUI0eJeV9o3yh1uURV3vbih+0ca2Mql9m7N49dkkgeZ04FAWUp9yG+p1jf5tA
Iwa6t1vvH1T8TKwjGtBH3jVYenKBk+W+DWZnDepg0l+8Xozo0JP5u1u68sqf+cke0Bw1RfsTFU4yA
OEBSIIZ/Stx7Q82K8M4XucAFV8PTT8i30QoGcsduEj4zapec1vnNn7f";
String str5 = "du56APPx0pvUiZMTZXVP";
String str6 = "95fen";
list.add(vm.addLocalObject(new StringObject(vm, str2)));
list.add(vm.addLocalObject(new StringObject(vm, str3)));
list.add(vm.addLocalObject(new StringObject(vm, str4)));
list.add(vm.addLocalObject(new StringObject(vm, str5)));
list.add(vm.addLocalObject(new StringObject(vm, str6)));
Number number = module.callFunction(emulator, 0x16f1d, list.toArray())[0];
String result = vm.getObject(number.intValue()).getValue().toString();
System.out.println(result);
}

```

那就执行目标函数吧。



```
shumei x
[4] llac Path:/proc/self/maps
[4] llac Path:/proc/net/arp
[09:39:02 040] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/proc/net/arp, oflags=0x20000, mode=0
[4] llac Path:/data/system
[09:39:02 069] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/data/system, oflags=0xa4000, mode=0
[4] llac Path:/data/system
[09:39:02 084] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/data/system, oflags=0xa4000, mode=0
[4] llac Path:/data/system
[09:39:02 089] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/data/system, oflags=0xa4000, mode=0
[4] llac Path:/vendor/firmware
[09:39:02 091] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/vendor/firmware, oflags=0xa4000, mode=0
[4] llac Path:/system/bin
[09:39:02 092] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/system/bin, oflags=0xa4000, mode=0
[4] llac Path:/vendor/lib
[09:39:02 094] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/vendor/lib, oflags=0xa4000, mode=0
[4] llac Path:/system/framework
[09:39:02 096] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/system/framework, oflags=0xa4000, mode=0
[4] llac Path:/system/fonts
[09:39:02 097] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/system/fonts, oflags=0xa4000, mode=0
[4] llac Path:/system/fonts
[09:39:02 099] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/system/fonts, oflags=0xa4000, mode=0
[4] llac Path:/system/bin/su
[09:39:02 182] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/bin/su, oflags=0x0, mode=0x0
[4] llac Path:/system/xbin/su
[09:39:02 184] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/xbin/su, oflags=0x0, mode=0x0
[4] llac Path:/sbin/su
[09:39:02 185] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/su, oflags=0x0, mode=0x0
[4] llac Path:/system/bin/ls
```

可以发现，访问的还挺杂，访问maps是惯例，maps能做的事太多了，可以检测frida，也可以查看系统运行了哪些库，或者找到某个SO的地址等等。

/proc/net/arp呢，是网络相关的文件，读取本地Arp表获取当前局域网内其他设备信息。我们可以在日志中看到，还访问了很多文件目录，甚至是fonts字体文件。而/system/bin/su这一类是检测是否设备是否Root。

## 我们来补JAVA环境吧

Google可知，`Environment.getExternalStorageDirectory()` 获取的是SD卡文件

```
@Override
public DvmObject<?> callStaticObjectMethodv(BaseVM vm, DvmClass dvmClass, String
signature, VaList vaList) {
    switch (signature){
        case "android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;":{
            return vm.resolveClass("java/io/File").newObject(signature);
        }
    }
    return super.callStaticObjectMethodv(vm, dvmClass, signature, vaList);
}
```

我们直接补了一个空File对象，这是为什么呢？

因为我们知道，后面肯定是想拿什么东西，比如文件名？绝对路径？或者文件里的内容？但我们现在没有那么多信息，预料不了之后的情况，所以可以只补一个空的，后续在它被使用的时候再补救。补 Unidbg Java 环境时，“**开局一个碗，过程慢慢补**”是一种不太优雅，但很省事的补法。

运行测试一下

```
Run: shumei >
Q Cc L W * 0 results ↑ ↓ + H E T
[09:46:48 115] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/system/bin/ls, oflags=0x20000, mode=0
JNIEnv->FindClass(android/os/Environment) was called from RX@0x0004507b[libmsdk.so]@x4507b
JNIEnv->GetStaticMethodID(android/os/Environment.getExternalStorageDirectory()Ljava/io/File;) => 0x57b36412 was called from RX@0x400717f5[libmsdk.so]@x717f5
JNIEnv->CallStaticObjectMethodV(class android/os/Enviroment, getExternalStorageDirectory() => java.io.File@2f8f5f62) was called from RX@0x40071da5[libmsdk.so]@x71da5
JNIEnv->GetMethodID(Ljava/io/File;.getAbsolutePath()Ljava/lang/String;) => 0x4553f34 was called from RX@0x0071b31[libmsdk.so]@x71b31
[09:46:48 296] WARN [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=1073748476, svcNumber=0x115, PC=unidbg@0xffffe
java.lang.ClassCastException Create breakpoint : class java.lang.String cannot be cast to class java.io.File (java.lang.String and java.io.File are in module java.base of lo
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethodV(AbstractJni.java:267)
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethodW(AbstractJni.java:224)
    at com.github.unidbg.linux.android.dvm.DvmMethod.callObjectMethodW(DvmMethod.java:85)
    at com.github.unidbg.linux.android.dvm.DalvikVM$22.handle(DalvikVM.java:434)
    at com.github.unidbg.linux.ARMS32SyscallHandler.hook(ARMS32SyscallHandler.java:103)
    at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:299)
    at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
    at unicorn.Unicorn.emu_start(Native Method)
    at com.github.unidbg.arm.backend.UnicornBackend.emu_start(UnicornBackend.java:325)
    at com.github.unidbg.arm.backend.UnicornBackend.emu_start(UnicornBackend.java:325)
```

好家伙，这是个什么报错？宝，为什么37度的手指能打出这么冰凉的文字？

点进去看看

```
264     return serviceManager.getService(vm, serviceName.getValue());
265 }
266 case "java/io/File->getAbsolutePath()Ljava/lang/String;":
267     File file = (File) dvmObject.getValue();
268     return new StringObject(vm, file.getAbsolutePath());
269 case "android/app/Application->getPackageManager()Landroid/content/pm/PackageManager;":
270 case "android/content/ContextWrapper->getPackageManager()Landroid/content/pm/PackageManager;":
271 case "android/content/Context->getPackageManager()Landroid/content/pm/PackageManager;":
272     DvmClass clazz = vm.resolveClass(className: "android/content/pm/PackageManager");
273     return clazz.newInstance(signature);
274 case "android/content/pm/PackageManager->getPackageInfo(Ljava/lang/String;I)Landroid/content/pm/PackageInf
275     StringObject packageName = vaList.getObjectArg(index: 0);
276     assert packageName != null;
277     int flags = vaList.getIntArg(index: 1);
278     if (!vm.isDebuggerEnabled())
279 }
```

AbstractJNI是Unidbg内置的、常见JAVA环境的补充，怎么会报错？

其实很简单，报错发生在**java/io/File->getAbsolutePath()Ljava/lang/String;**，上一步获取了文件，这一步获取文件的绝对路径，Unidbg 默认我们上一步传入的文件是“真”的，所以在很老实的把它转成文件，通过JAVA API获取绝对路径，但是呢，因为我们的文件根本不存在，我们只穿了个空的File对象，其实根本就不是File，所以它没法强转成File，就报错了。

咋办呢？在我们的类里重写呗。这个不是Unidbg本身的问题，也不是我们的问题，当报错发生在AbstractJNI时，一定不要讶异是不是Unidbg出错了，没啥大不了的，本类里根据样本的需求重写就完事了。

```
@Override
public DvmObject<?> callObjectMethodV(BaseVM vm, DvmObject<?> dvmObject, String
signature, VaList vaList) {
    switch (signature) {
        case "java/io/File->getAbsolutePath()Ljava/lang/String;": {
            String tag = dvmObject.getValue().toString();
            if (tag.equals("android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;")){
                return new StringObject(vm, "/storage/emulated/0");
            }
        }
    }
    return super.callObjectMethodV(vm, dvmObject, signature, vaList);
}
```

考虑两个问题

1是这个返回的字符串哪来的？或者说绝对路径哪来的，有两个办法

- Google，既然它是Android标准API，上网搜一下
- JNITrace看一下，前面我们阐述过怎么用JNITrace看参数和返回值，你会用了吗？

```
/* TID 14857 */
2684 ms [+] JNIEnv->CallObjectMethodV
2684 ms |- JNIEnv*           : 0xba872620
2684 ms |- jobject          : 0x21
2684 ms |- jmethodID         : 0x704eea84      {
getAbsolutePath()Ljava/lang/String; }
2684 ms |- va_list           : 0xb9032ab4
2684 ms |= jobject          : 0x31
```

```

2684 ms -----Backtrace-----
2684 ms | -> 0xb1ecfdf5: libssmsdk.so!0x71df5 (libssmsdk.so:0xb1e5e000)

    /* TID 14857 */
2700 ms [+] JNIEnv->ExceptionCheck
2700 ms |- JNIEnv*           : 0xba872620
2700 ms |= jboolean          : 0     { false }

2700 ms -----Backtrace-----
2700 ms | -> 0xb1ecf617: libssmsdk.so!0x71617 (libssmsdk.so:0xb1e5e000)

    /* TID 14857 */
2716 ms [+] JNIEnv->DeleteLocalRef
2716 ms |- JNIEnv*           : 0xba872620
2716 ms |- jobject            : 0x15

2716 ms -----Backtrace-----
2716 ms | -> 0xb1ecf567: libssmsdk.so!0x71567 (libssmsdk.so:0xb1e5e000)

    /* TID 14857 */
2733 ms [+] JNIEnv->GetStringUTFChars
2733 ms |- JNIEnv*           : 0xba872620
2733 ms |- jstring             : 0x31
2733 ms |- jboolean*          : 0x0
2733 ms |= char*              : 0xb6f70a10

2733 ms -----Backtrace-----
2733 ms | -> 0xb1e7bdff: libssmsdk.so!0x1ddff (libssmsdk.so:0xb1e5e000)

    /* TID 14857 */
2749 ms [+] JNIEnv->ReleaseStringUTFChars
2749 ms |- JNIEnv*           : 0xba872620
2749 ms |- jstring             : 0xb6f70a10
2749 ms |- char*               : 0xb6f70a10
2749 ms |:      /storage/emulated/0

2749 ms -----Backtrace-----
2749 ms | -> 0xb1ecfedd: libssmsdk.so!0x71edd (libssmsdk.so:0xb1e5e000)

```

第二个问题是，为什么我们还做了签名验证，因为防止后面还有别的File，别的getAbsolutePath，免得造成混淆。

```

[10:09:35 640] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1846) - faccessat dirfd=-100, pathname=/sbin/.magisk/modules/riru_exposed/module.prop, utime=0
lilac Path:/proc/self/mounts
[10:09:35 643] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/proc/self/mounts, oflags=0x0, mode=0x0
[10:09:35 667] INFO [com.github.unidbg.linux.AndroidSyscallHandler] (AndroidSyscallHandler:149) - pipe2 pipefd=unidbg@0xbffffd08, flags=0x0, readfd=4, writefd=3
[10:09:35 669] WARN [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=190, svcNumber=0x0, PC=RX@0x401be5c[libc.so]0x41b5c, L
[10:09:35 671] WARN [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=358, svcNumber=0x0, PC=RX@0x401bed0[libc.so]0x41db0, L
java.lang.AbstractMethodError Create breakpoint : com.github.unidbg.linux.file.PipedWriteFile0
    at com.github.unidbg.file.AbstractFile0.dup2(AbstractFile0.java:16)
    at com.github.unidbg.linux.ARMS32SyscallHandler.dup3(ARM32SyscallHandler.java:2103)
    at com.github.unidbg.linux.AndroidSyscallHandler.hook(ARM32SyscallHandler.java:437)
    at com.github.unidbg.linux.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:299)
    at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
    at unicorn.Unicorn.emu_start(Native Method)
    at com.github.unidbg.arm.backend.UnicornBackend.emu_start(UnicornBackend.java:325)
    at com.github.unidbg.AbstractEmulator.emulate(AbstractEmulator.java:370)
    at com.github.unidbg.AbstractEmulator.eFunc(AbstractEmulator.java:446)
    at com.github.unidbg.arm.AbstractARMEmulator.eFunc(AbstractARMEmulator.java:220)
    at com.github.unidbg.unidbg.Module.emulateFunction(Module.java:158)
    at com.github.unidbg.linux.LinuxModule.callFunction(LinuxModule.java:232)
    at com.jiuwu.shumei.w1(shumei.java:80)
    at com.jiuwu.shumei.main(shumei.java:61)
Exception in thread "main" java.lang.NullPointerException Create breakpoint : Cannot invoke "com.github.unidbg.linux.android.dvm.DvmObject.getValue()" because the return value of "co
    at com.jiuwu.shumei.w1(shumei.java:81)
    at com.jiuwu.shumei.main(shumei.java:61)

```

先别看这糟心的报错，看看文件访问，好像又多了不少，从后往前看看

```

Run: shumei
  ↗ q Lilac Path
  ↘ C:\Program Files\Java\jdk-16.0.1\bin\java.exe" ...
  ↗ Lilac Path:/dev/_properties--
  ↗ Lilac Path:/proc/stat
  ↗ JNIEnv->FindClass(com/ishumei/dfp/SMSDK) was called from RX@0x4001760f[libsmssdk.so]0x1760f
  ↗ JNIEnv->RegisterNatives(com/ishumei/dfp/SMSDK, RW@0x400d3010[libsmssdk.so]0x3d010, 3) was called from RX@0x40017723[libsmssdk.so]0x17723
  ↗ RegisterNative(com/ishumei/dfp/SMSDK, w1(Landroid/content/Context;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)Ljava/lang/RegisterNative(com/ishumei/dfp/SMSDK, x6(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;), RX@0x40017095[libsmssdk.so]0x17095)
  ↗ RegisterNative(com/ishumei/dfp/SMSDK, w3(Landroid/content/Context;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;), RX@0x40017095[libsmssdk.so]0x17095)
  ↗ JNIEnv->GetStringUTFChars>{"a1","a1L","a3","none","a4","4","a2":"SRchM3hsEtSjSE1fQv1Cares0925Tis1PYZFk58Ez2MNqdh6k0RlGaYm8Nld0140FXZ0C1XTuZJ+Va9w5pRw==","a5":"","a7""}
  ↗ JNIEnv->ReleaseStringUTFChars>{"a1","a1L","a3","none","a4":"4","a2":SRchM3hsEtSjSE1fQv1Cares0925Tis1PYZFk58Ez2MNqdh6k0RlGaYm8Nld0140FXZ0C1XTuZJ+Va9w5pRw==,"a5":"","a7""}
  ↗ JNIEnv->GetStringUTFChars("dU56APPx0pvUiZMTZXPV") was called from RX@0x400556df[libsmssdk.so]0x556df
  ↗ JNIEnv->ReleaseStringUTFChars("dU56APPx0pvUiZMTZXPV") was called from RX@0x4005585f[libsmssdk.so]0x5585f
  ↗ JNIEnv->GetStringUTFChars("MIDLzCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAyMqsWCQYDQGGEwJDTjELMAKGA1UECwwCU00xFjAUBgNVBAMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNNDAxM
  ↗ JNIEnv->ReleaseStringUTFChars("MIDLzCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAyMqsWCQYDQGGEwJDTjELMAKGA1UECwwCU00xFjAUBgNVBAMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNN
  ↗ JNIEnv->GetStringUTFChars("95fen") was called from RX@0x400556df[libsmssdk.so]0x556df
  ↗ JNIEnv->ReleaseStringUTFChars("95fen") was called from RX@0x4005585f[libsmssdk.so]0x5585f
  ↗ JNIEnv->GetStringUTFChars>{"all_atamper":true,"core_atamper":true,"hook_java_switch":true,"hook_switch":false,"risk_apps":[{"xposed":{"pn":"de.rob.v.android.xposed
  ↗ JNIEnv->ReleaseStringUTFChars>{"all_atamper":true,"core_atamper":true,"hook_java_switch":true,"hook_switch":false,"risk_apps":[{"xposed":{"pn":"de.rob.v.android.xposed
  ↗ lilac Path:/proc/self/maps
  ↗ lilac Path:/proc/net/arp
  [10:09:35 211] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/proc/net/arp, oflags=0x20000, mode=0
  ↗ lilac Path:/data/system
  [10:09:35 248] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/data/system, oflags=0xa4000, mode=0

```

来看看

```

  ↗ Lilac Path:/dev/wgzs
  [10:09:35 600] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/dev/wgzs
  ↗ lilac Path:/proc/self/maps
  ↗ lilac Path:/proc/self/maps
  ↗ lilac Path:/data/user_de/0/zposed.installer
  [10:09:35 614] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/data/use
  ↗ lilac Path:/data/data/zposed.installer
  [10:09:35 617] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/data/dat
  ↗ lilac Path:/sbin/.magisk/modules/riru-core/system/lib/libmemtrack.so
  [10:09:35 619] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/.ma
  ↗ lilac Path:/sbin/magiskinit
  [10:09:35 622] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/.mag
  ↗ lilac Path:/sbin/.magisk/modules/riru_exposed
  [10:09:35 624] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/.ma
  ↗ lilac Path:/sbin/.magisk/modules/riru_core
  [10:09:35 626] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/.ma
  ↗ lilac Path:/system/framework/exposed.dex
  [10:09:35 629] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/f
  ↗ lilac Path:/system/framework/exdp.jar
  [10:09:35 631] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/f
  ↗ lilac Path:/system/lib/libriru_edxp.so
  [10:09:35 634] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/l
  ↗ lilac Path:/system/lib64/libriru_edxp.so
  [10:09:35 637] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/l
  ↗ lilac Path:/sbin/.magisk/modules/riru_exposed/module.prop
  [10:09:35 640] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/.ma
  ↗ lilac Path:/proc/self/mounts
  [10:09:35 643] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/procsel

```

proc/self/mounts 是访问与Magisk检测有关 [\[讨论\] Magisk隐藏root的实现-Android安全-看雪论坛-安全社区|安全招聘|bbs.pediy.com](#)

上面的文件访问也基本是EDxposed、xposed、Magisk相关

再往上面看看

```

lilac Path:/proc/self/maps
lilac Path:/sys/class/net/wlan0
[10:09:35 574] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sys/class/net/wlan0, oflags=0
lilac Path:/sys/class/net/eth0
[10:09:35 576] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sys/class/net/eth0, oflags=0x
lilac Path:/proc/iomem
[10:09:35 580] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/proc/iomem, oflags=0x0, mode=
lilac Path:/proc/misc
[10:09:35 581] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/proc/misc, oflags=0x0, mode=
lilac Path:/sdcard/user
[10:09:35 582] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sdcard/user, oflags=0x0, mode=
lilac Path:/data/local/tmp/user
[10:09:35 584] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/data/local/tmp/user, oflags=0
lilac Path:/sdcard/fenshen/device.zip
[10:09:35 585] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sdcard/fenshen/device.zip, oflag
lilac Path:/data/local/tmp/configs
[10:09:35 586] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/data/local/tmp/configs, oflag
lilac Path:/sdcard/fenshen/xiansi.json
[10:09:35 588] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sdcard/fenshen/xiansi.json, o
lilac Path:/sdcard/fenshen/gps.json
[10:09:35 589] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sdcard/fenshen/gps.json, ofla
lilac Path:/data/local/tmp/configs/.a
[10:09:35 591] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/data/local/tmp/configs/.a, of
lilac Path:/data/local/tmp/configs/.d
[10:09:35 592] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/data/local/tmp/configs/.d, of
lilac Path:/data/local/tmp/configs/.en
[10:09:35 594] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/data/local/tmp/configs/.en, o
lilac Path:/data/local/tmp/configs/.gg
[10:09:35 595] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/data/local/tmp/configs/.gg, o

```

像是检测应用分身

接下来处理糟糕的报错

```

lilac Path:/proc/self/mounts
[10:09:35 643] INFO [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/proc/self/mounts, oflags=0x0, mode=0x0
[10:09:35 667] INFO [com.github.unidbg.linux.AndroidSyscallHandler] (AndroidSyscallHandler:149) - pipe2 pipefd=unidbg@0xbffffdc0, flags=0x0, readfd=4, writefd=3
[10:09:35 669] WARN [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:467) handleInterrupt intno=2, NR=190, svcNumber=0x0, PC=RX@0x401be5c[libc.so]0x41b5c, L
[10:09:35 671] WARN [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:467) handleInterrupt intno=2, NR=358, svcNumber=0x0, PC=RX@0x401bedb0[libc.so]0x41db0, L
java.lang.AbstractMethodError Create breakpoint : com.github.unidbg.linux.file.PipedWriteFileIO
    at com.github.unidbg.file.AbstractFileIO.dup2(AbstractFileIO.java:166)
    at com.github.unidbg.linux.ARMSyscallHandler.dup3(ARM32SyscallHandler.java:2103)
    at com.github.unidbg.linux.ARMSyscallHandler.hook(ARM32SyscallHandler.java:437)
    at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:299)
    at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
    at unicorn.Unicorn.emu_start(Native Method)
    at com.github.unidbg.arm.backend.UncornBackend.emu_start(UncornBackend.java:325)
    at com.github.unidbg.AbstractEmulator.emulate(AbstractEmulator.java:378)
    at com.github.unidbg.AbstractEmulator.eFunc(AbstractEmulator.java:446)
    at com.github.unidbg.arm.AbstractARMEmulator.eFunc(AbstractARMEmulator.java:220)
    at com.github.unidbg.Module.emulateFunction(Module.java:158)
    at com.github.unidbg.linux.LinuxModule.callFunction(LinuxModule.java:232)
    at com.jiuwu.shumei.w1(shumei.java:80)
    at com.jiuwu.shumei.main(shumei.java:41)
Exception in thread "main" java.lang.NullPointerException Create breakpoint : Cannot invoke "com.github.unidbg.linux.android.dvm.DvmObject.getValue()" because the return value of "co

```

NR = 190, 190是什么系统调用? Unidbg尚未实现

```

tnud / unidbg / linux / ARM32SyscallHandler
mysoul.java x shumei.java x AbstractFileIO.java x ARM32SyscallHandler.java x AbstractUni.java x EmulatorBuilder.java x soul
Q case 18
278     return;
279 case 180:
280     backend.reg_write(ArmConst.UC_ARM_REG_R0, pread64(emulator));
281     return;
282 case 183:
283     backend.reg_write(ArmConst.UC_ARM_REG_R0, getcwd(backend, emulator));
284     return;
285 case 186:
286     backend.reg_write(ArmConst.UC_ARM_REG_R0, sigaltstack(emulator));
287     return;
288 case 192:
289     backend.reg_write(ArmConst.UC_ARM_REG_R0, mmap2(backend, emulator));
290     return;
291 case 194:
292     backend.reg_write(ArmConst.UC_ARM_REG_R0, ftruncate(backend));
293     return;
294 case 195:
295     backend.reg_write(ArmConst.UC_ARM_REG_R0, stat64(emulator));
296     return;
297 case 196:
298     backend.reg_write(ArmConst.UC_ARM_REG_R0, lstat(emulator));

```

查一下表 [Chromium OS Docs - Linux System Call Table \(googlesource.com\)](https://chromium.googlesource.com/chromiumos/docs/+/master/linux/SystemCallTable.md)

					*filename				
183	getcwd	man/ cs/	0xb7	char *buf	unsigned long size	-	-	-	-
184	capaget	man/ cs/	0xb8	cap_user_header_t header	cap_user_data_t dataptr	-	-	-	-
185	capset	man/ cs/	0xb9	cap_user_header_t header	const cap_user_data_t data	-	-	-	-
186	sigaltstack	man/ cs/	0xba	const struct sigaltstack *uss	struct sigaltstack *uoss	-	-	-	-
187	sendfile	man/ cs/	0xbb	int out_fd	int in_fd	off_t *offset	size_t count	-	-
188	not implemented		0xbc						
189	not implemented		0xbd						
190	vfork	man/ cs/	0xbe	-	-	-	-	-	-
191	ugetrlimit	man/ cs/	0xbf	?	?	?	?	?	?
192	mmap2	man/ cs/	0xc0	?	?	?	?	?	?
193	truncate64	man/ cs/	0xc1	const char *path	loff_t length	-	-	-	-
194	ftruncate64	man/ cs/	0xc2	unsigned int fd	loff_t length	-	-	-	-
195	stat64	man/ cs/	0xc3	const char *filename	struct stat64 *statbuf	-	-	-	-
196	lstat64	man/ cs/	0xc4	const char *filename	struct stat64 *statbuf	-	-	-	-
197	fstat64	man/ cs/	0xc5	unsigned long fd	struct stat64 *statbuf	-	-	-	-
198	lchown32	man/ cs/	0xc6	?	?	?	?	?	?

好家伙，是vfork，vfork和fork类似，用于创建一个新的子进程，Unidbg想要处理多进程和多线程非常困难，这是Unidbg的阿喀琉斯之踵，期待凯神或者其他大师傅能解决这个问题。

既然目前没有办法真正实现vfork，我们只能将就一下了，实现这个vfork，里面什么都不做。为了不让我们写的垃圾vfork破坏Unidbg本身的ARM32SyscallHandler，我们选择继承ARM32SyscallHandler，在需要vfork的项目中使用自己的MyARM32SyscallHandler。

```
package com.jiuwu;

import com.github.unidbg.Emulator;
import com.github.unidbg.arm.context.EditableArm32RegisterContext;
import com.github.unidbg.linux.ARM32SyscallHandler;
import com.github.unidbg.memory.SvcMemory;

import java.util.concurrent.ThreadLocalRandom;

public class MyARM32SyscallHandler extends ARM32SyscallHandler {
    public MyARM32SyscallHandler(SvcMemory svcMemory) {
        super(svcMemory);
    }

    @Override
    protected boolean handleUnknownSyscall(Emulator emulator, int NR) {
        switch (NR) {
            case 190:
                vfork(emulator);
                return true;
        }

        return super.handleUnknownSyscall(emulator, NR);
    }

    private void vfork(Emulator<?> emulator) {
        EditableArm32RegisterContext context = (EditableArm32RegisterContext)
emulator.getContext();
        int childPid = emulator.getPid() +
ThreadLocalRandom.current().nextInt(256);
        int r0 = childPid;
        System.out.println("vfork pid=" + r0);
        context.setR0(r0);
    }
}
```

```
}
```

可以看到，我们的vfork只做了一件事，随机返回一个进程号，但我们啥都没有做，那个进程屁都没有。

我们只能期待样本没有在新进程里做什么事，否则等待我们的只有报错，没办法，哎。

接下来在我们的样本中使用MyARM32SyscallHandler

```
package com.jiuwu;

import com.github.unidbg.AndroidEmulator;
import com.github.unidbg.Emulator;
import com.github.unidbg.Module;
import com.github.unidbg.file.FileResult;
import com.github.unidbg.file.IOResolver;
import com.github.unidbg.file.linux.AndroidFileIO;
import com.github.unidbg.linux.android.AndroidARMEmulator;
import com.github.unidbg.linux.android.AndroidEmulatorBuilder;
import com.github.unidbg.linux.android.AndroidResolver;
import com.github.unidbg.linux.android.dvm.*;
import com.github.unidbg.linux.android.dvm.array.ByteArray;
import com.github.unidbg.memory.Memory;
import com.github.unidbg.memory.SvcMemory;
import com.github.unidbg.unix.UnixSyscallHandler;
import com.github.unidbg.virtualmodule.android.AndroidModule;

import javax.crypto.Cipher;
import javax.crypto.NoSuchPaddingException;
import java.io.File;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.List;

public class shumei extends AbstractJni implements IOResolver {
    private final AndroidEmulator emulator;
    private final VM vm;
    private final Module module;

    shumei() {
        // 创建模拟器实例
        //     emulator = AndroidEmulatorBuilder
        //             .for32Bit()
        //             .setRootDir(new File("target/rootfs"))
        //             .build();

        AndroidEmulatorBuilder builder = new AndroidEmulatorBuilder(false) {
            @Override
            public AndroidEmulator build() {
                return new AndroidARMEmulator(processName, rootDir,
                    backendFactories) {
                    @Override
                    protected UnixSyscallHandler<AndroidFileIO>
                    createSyscallHandler(SvcMemory svcMemory) {
                        return new MyARM32SyscallHandler(svcMemory);
                    }
                };
            }
        };
    }
}
```

```
        }

        ;
    };

    emulator = builder.setRootDir(new File("target/rootfs")).build();

    // 获取模拟器的内存操作接口
    final Memory memory = emulator.getMemory();
    // 设置系统类库解析
    memory.setLibraryResolver(new AndroidResolver(23));
    // 绑定重定向
    emulator.getSyscallHandler().addIOResolver(this);

    vm = emulator.createDalvikVM(new File("unidbg-
android/src/test/resources/shumei/com.jiuwu_1.25.0_1002500.apk"));
    new AndroidModule(emulator, vm).register(memory);
    DalvikModule dm = vm.loadLibrary(new File("unidbg-
android/src/test/resources/shumei/libssmsdk.so"), true); // 加载so到虚拟内存
    //获取本SO模块的句柄,后续需要用它
    module = dm.getModule();
    vm.setJni(this);
    vm.setVerbose(true); // 打印日志

    dm.callJNI_OnLoad(emulator); // 调用JNI OnLoad
};

@Override
public FileResult resolve(Emulator emulator, String pathname, int oflags) {
    System.out.println("lilac Path:"+pathname);
    // 具体的处理
    return null;
}

public static void main(String[] args) {
    shumei demo = new shumei();
    demo.w1();
}

public void w1(){
    List<Object> list = new ArrayList<>(10);
    list.add(vm.getJNIEnv());
    list.add(0);
    DvmObject<?> obj =
    vm.resolveClass("android/content/Context").newObject(null);
    list.add(vm.addLocalObject(obj));
}
```

```
String str2 = "
{\\"a1\\":\\"a11\\",\\"a3\\":\\"none\\",\\"a4\\":\\"4\\",\\"a2\\":\\"SRCM3hsEtSjSE1fQv1Cares092
5Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOCiXTuZJ+Va9w5pRw==\\",\\"a5\\":\\"\\",\\"a
7\\":\\"3.0.4\\",\\"a8\\":\\"\\",\\"a6\\":\\"android\\",\\"a44\\":\\"wifi\\",\\"a47\\":
[\"16, qualcomm\", \"4, qualcomm\", \"19, qualcomm\", \"19, qualcomm\", \"9, qualcomm\",
\"18, qualcomm\", \"18, qualcomm\", \"17, qualcomm\", \"22, qualcomm\", \"2, akm\", \"10, qu
alcomm\", \"20, qualcomm\", \"3, xiaomi\", \"30, qualcomm\", \"30, qualcomm\", \"33171027
,xiaomi\", \"33171027,xiaoMi\", \"33171036,xiaoMi\", \"33171036,xiaoMi\", \"11,xiaom
i\", \"5,Rohm\", \"5,Rohm\", \"6,Bosch\", \"29, qualcomm\", \"29, qualcomm\", \"1, qualco
mm\", \"35, qualcomm\", \"15, qualcomm\", \"27,xiaomi\", \"27,xiaomi\", \"33171029,xiao
Mi\", \"33171029,XiaoMi\", \"14, akm\", \"33171070,xiaomi\", \"33171070,xiaomi\", \"8,
Elliptic Labs\", \"33171031,xiaomi\"],\"a46\\":{\"cpu_abi\"::\\\"armeabi-
v7a\\\",\"serial\\\":\\\"unknown\\\",\"fingerprint\\\":\\\"Xiaomi\\\\polaris\\\\polaris:10\\\\Q
KQ1.190828.002\\\\V12.0.2.0.QDGCNXM:user\\\\release-keys\\\",\"model\\\":\\\"MIX
2S\\\",\"cpu_abi2\\\":\\\"armeabi\\\",\"brand\\\":\\\"Xiaomi\\\",\"board\\\":\\\"sdm845\\\",\"serial
_P\\\":\\\"unknown\\\",\"manufacturer\\\":\\\"Xiaomi\\\"},\"a38\\\":\\\"1.25.0\\\",\"a33\\\":\\\"ARMv8
Processor rev 13
(v81)\",\"a103\\\":\\\"faf6c8c7ad942343\\\",\"a23\\\":\\\"\\\",\"a54\\\":\\\"0000010\\\",\"a48\\\":5
905514496,\"a10\\\":\\\"10\\\",\"a11\\\":\\\"95fen\\\",\"a15\\\":\\\"false\\\",\"a17\\\":
[\\\"wlan1,,f460e217db64,\\\",\\\"wlan0,172.16.16.12,f460e296db64,fe80::f660:e2ff:fe96
:db64%wlan0\\\",\\\"p2p0,,f660e218db64,\\\"],\"a18\\\":
{\\\"ro.boot.hardware\\\":\\\"qcom\\\",\\\"gsm.sim.state\\\":\\\"LOADED,LOADED\\\",\\\"sys.usb.sta
te\\\":\\\"adb\\\",\\\"ro.debuggable\\\":\\\"0\\\"},\"a19\\\":\\\"02:00:00:00:00:00\\\",\"a9\\\":16281
28282220,\"a39\\\":\\\"com.jiuwu\\\",\"a40\\\":1627972313927,\"a45\\\":\\\"46001\\\",\"a21\\\":
\\\",\"a24\\\":\\\"6d9de21492b99db9\\\",\"a25\\\":\\\"\\\",\"a22\\\":\\\"\\\",\"a34\\\":2803200,\"a37
\\\":1295,\"a27\\\":
[\\\"1628127546162,com.jiuwu,,1,1002500,1.25.0,1628127546162\\\",\\\"1230768000000,com
.android.cts.priv.ctsshim,,0,28,9-
5374186,1230768000000\\\",\\\"1230768000000,com.miui.contentextension,,0,10164,2.4.2
,1611338104848\\\",\\\"1230768000000,com.qualcomm.qti.qcolor,,0,29,10,1230768000000\\
\",\\\"1230768000000,com.android.internal.display.cutout.emulation.corner,,0,1,1.0,
1230768000000\\\",\\\"1230768000000,com.google.android.ext.services,,0,291900801,q_p
r1-
release_am1_291900801,1230768000000\\\",\\\"1230768000000,com.qualcomm.qti.improveto
uch.service,,0,29,10,1230768000000\\\",\\\"1230768000000,com.android.internal.displa
y.cutout.emulation.double,,0,1,1.0,1230768000000\\\",\\\"1230768000000,com.android.p
roviders.telephony,,0,29,10,1230768000000\\\",\\\"1230768000000,com.android.dynsyste
m,,0,29,10,1230768000000\\\"],\"a29\\\":\\\"4.0.c2.6-00335-0914_2350_3c8fca6,4.0.c2.6-
00335-0914_2350_3c8fca6\\\",\"a32\\\":8,\"a30\\\":\\\"<unknown
ssid\\\",\"a31\\\":\\\"172.16.16.12\\\",\"a90\\\":28,\"a105\\\":
{},\"a108\\\":\\\"\\\",\"a109\\\":\\\"\\\",\"a110\\\":\\\"\\\",\"a111\\\":\\\"\\\",\"a107\\\":
{\\\"java\\\\lang\\\\reflect\\\\Modifier\\\":2,\\\"com\\\\android\\\\internal\\\\telephony\\\\
/PhoneProxy\\\":2,\\\"java\\\\lang\\\\ProcessBuilder\\\":2,\\\"com\\\\android\\\\internal\\\\
telephony\\\\PhoneSubInfo\\\":2,\\\"android\\\\location\\\\LocationManager\\\":2,\\\"com\\\\
tencent\\\\mapapi\\\\service\\\\LocationManager\\\":2,\\\"com\\\\android\\\\internal\\\\te
lephony\\\\gsm\\\\GSMPhone\\\":2},\"a20\\\":\\\"\\\",\"a49\\\":\\\"\\\",\"a52\\\":
{\\\"magisk\\\":1},\"a53\\\":{},\"a50\\\":
{},\"a60\\\":\\\"u0_a349\\\",\"a62\\\":\\\"\\\\data\\\\user\\\\0\\\\com.jiuwu\\\\files\\\",\"a55\\
\":\\\"a58929cd0e3202053f6137261ecd3c40\\\",\"a57\\\":1160259262,\"a36\\\":\\\"1080,2030,44
0\\\",\"a56\\\":\\\"CN=jiuwu, OU=jiuwu, O=jiuwu, L=上海, ST=上海,
C=CN\\\",\"a76\\\":\\\"\\\",\"a88\\\":\\\"locateServiceName:android.os.BinderProxy|phoneServ
iceName:android.os.BinderProxy\\\",\"a84\\\":\\\"3vDSuAiODgqAwBUsIqCEpuAFJ+xKBFFJ383k
+\\\\M2+M=____\\\",\"a68\\\":
[],\"a92\\\":\\\"1080,2030\\\",\"a93\\\":0,\"a95\\\":-1,\"a96\\\":\\\"du56APPx0pvUi
zMTZXVP\\\",\\\"a97\\\":\\\"SRCM3hsEtSjSE1fQv1Cares0925Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOC
iXTuZJ+Va9w5pRw==\\\",\"a98\\\":\\\"\\\",\"a99\\\":\\\"\\\",\"a100\\\":\\\"\\\",\"a101\\\":\\\"\\\",\"a102
\\\":[],\"a63\\\":\\\"InputMethodInfo{com.sohu.inputmethod.sogou.xiaomi\\\\.SogouIME,
settings:
```

```
com.sohu.inputmethod.sogou.SogouIMESettingsLauncher}\\"", \"InputMethodInfo{com.iflytek.inputmethod.miui\\/.FlyIME, settings:  
com.iflytek.inputmethod.LauncherSettingsActivity\"]}, \"a67\": {}, \"a64\":  
{} , \"suc\": \"1\" , \"enable\": \"0\" , \"service\": [] } , \"a65\": 39 , \"a66\":  
{} , \"a74\": 0 , \"a73\": 0 , \"a78\": [] , \"a75\": 0 , \"a77\":  
{} , \"a86\": \"1100100\" , \"a79\": \"\" , \"a80\": \"1628128282029-  
12295\" , \"a83\": \"1001100\" , \"a85\":  
[] , \"a69\": 15533490176 , \"a71\": 118982303744 , \"a72\":  
{} , \"temp\": 370 , \"vol\": 4095 , \"level\": 85 , \"scale\": 100 , \"status\": 2 } , \"a70\": 1568  
4485120 } ;
```

```
String str3 = "
{\\"all_atamper\\":true,\\"core_atamper\\":true,\\"hook_java_switch\\":true,\\"hook_swit
tch\\":false,\\"risk_apps\\":[\{\\"xposed\\":
{\\"pn\\":\"de.robv.android.xposed.installer\",\"uri\\\":\"\\"},\\"controllers\\":
{\\"pn\\":\"com.soft.controllers\",\"uri\\\":\"\\"},\\"apk008v\\":
{\\"pn\\":\"com.soft.apk008v\",\"uri\\\":\"\\"},\\"apk008Tool\\":
{\\"pn\\":\"com.soft.apk008Tool\",\"uri\\\":\"\\"},\\"ig\\":
{\\"pn\\":\"com.doubee.ig\",\"uri\\\":\"\\"},\\"anjian\\":
{\\"pn\\":\"com.cyjh.mobileanjian\",\"uri\\\":\"\\"},\\"rktech\\":
{\\"pn\\":\"com.ruokuai.rktech\",\"uri\\\":\"\\"},\\"magisk\\":
{\\"pn\\":\"com.topjohnwu.magisk\",\"uri\\\":\"\\"},\\"kinguser\\":
{\\"pn\\":\"com.kingroot.kinguser\",\"uri\\\":\"\\"},\\"substrate\\":
{\\"pn\\":\"com.saurik.substrate\",\"uri\\\":\"\\"},\\"touchsprite\\":
{\\"pn\\":\"com.touchsprite.android\",\"uri\\\":\"\\"},\\"scriptdroid\\":
{\\"pn\\":\"com.stardust.scriptdroid\",\"uri\\\":\"\\"},\\"toolhero\\":
{\\"pn\\":\"com.mobileuncle.toolhero\",\"uri\\\":\"\\"},\\"huluxia\\":
{\\"pn\\":\"com.huluxia.gametools\",\"uri\\\":\"\\"},\\"apkeditor\\":
{\\"pn\\":\"com.gmail.heagoo.apkeditor.pro\",\"uri\\\":\"\\"},\\"xposeddev\\":
{\\"pn\\":\"com.sollyu.xposed.hook.model.dev\",\"uri\\\":\"\\"},\\"anywhere\\":
{\\"pn\\":\"com.txy.anywhere\",\"uri\\\":\"\\"},\\"burgerzws\\":
{\\"pn\\":\"pro.burgerz.wsm.manager\",\"uri\\\":\"\\"},\\"vdloc\\":
{\\"pn\\":\"com.virtualdroid.loc\",\"uri\\\":\"\\"},\\"vdtx\\":
{\\"pn\\":\"com.virtualdroid.txl\",\"uri\\\":\"\\"},\\"vdwzs\\":
{\\"pn\\":\"com.virtualdroid.wzs\",\"uri\\\":\"\\"},\\"vdkit\\":
{\\"pn\\":\"com.virtualdroid.kit\",\"uri\\\":\"\\"},\\"vdwxg\\":
{\\"pn\\":\"com.virtualdroid.wxg\",\"uri\\\":\"\\"},\\"vdgps\\":
{\\"pn\\":\"com.virtualdroid.gps\",\"uri\\\":\"\\"},\\"a1024mloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\\"},\\"drhzg\\":
{\\"pn\\":\"com.deruhai.guangzi.noroot2\",\"uri\\\":\"\\"},\\"yggb\\":
{\\"pn\\":\"com.mcmonjmb.yggb\",\"uri\\\":\"\\"},\\"xsrv\\":
{\\"pn\\":\"xiake.xserver\",\"uri\\\":\"\\"},\\"fakeloc\\":
{\\"pn\\":\"com.dracrays.fakeloc\",\"uri\\\":\"\\"},\\"ultra\\":
{\\"pn\\":\"net.anylocation.ultra\",\"uri\\\":\"\\"},\\"locationcheater\\":
{\\"pn\\":\"com.wifi99.android.locationcheater\",\"uri\\\":\"\\"},\\"dwzs\\":
{\\"pn\\":\"com.dingweizshou\",\"uri\\\":\"\\"},\\"mockloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\\"},\\"anywhereclone\\":
{\\"pn\\":\"com.txy.anywhere.clone\",\"uri\\\":\"\\"},\\"fakelocc\\":
{\\"pn\\":\"com.dracrays.fakelocc\",\"uri\\\":\"\\"},\\"mockwxlocation\\":
{\\"pn\\":\"com.tandy.android.mockwxlocation\",\"uri\\\":\"\\"},\\"anylocation\\":
{\\"pn\\":\"net.anylocation\",\"uri\\\":\"\\"},\\"totalcontrol\\":
{\\"pn\\":\"com.sigma_rt.totalcontrol\",\"uri\\\":\"\\"},\\"ipj12\\":
{\\"pn\\":\"com.chuangdian.ipj12\",\"uri\\\":\"\\"}],\\"risk_dirs\\":[\{\\"008Mode\\":
{\\"dir\\\":\".system/008Mode\",\"type\\\":\"sdcard\"},\\"008OK\\":
{\\"dir\\\":\".system/008OK\",\"type\\\":\"sdcard\"},\\"008system\\":
{\\"dir\\\":\".system/008system\",\"type\\\":\"sdcard\"},\\"iGrimace\\":
{\\"dir\\\":\"iGrimace\",\"type\\\":\"sdcard\"},\\"touchelper\\":
{\\"dir\\\":\"/data/data/net.aisence.Touchelper\",\"type\\\":\"absolute\"},\\"elfscript\\":
{\\"dir\\\":\"/mnt/sdcard/touchelf/scripts/\",\"type\\\":\"absolute\"},\\"spritelua\\":{\\"dir\\\":\"/mnt/sdcard/TouchSprite/lua\",\"type\\\":\"absolute\"},\\"spritelog\\":{\\"dir\\\":\"/mnt/sdcard/TouchSprite/log\",\"type\\\":\"absolute\"},\\"assistant\\":{\\"dir\\\":\"/data/data/com.xxAssistant\",\"type\\\":\"absolute\"},\\"assistantscript\\":
{\\"dir\\\":\"/mnt/sdcard/com.xxAssistant/script\",\"type\\\":\"absolute\"},\\"mobileanjian\\":
{\\"dir\\\":\"/data/data/com.cyjh.mobileanjian\",\"type\\\":\"absolute\"}],\\"risk_fi
le_switch\\":true,\\"risk_files\\\":\"zb5E/i2Gv4IxR50xSBixKChu8gdkDXKei9GwOBNbN6jq3x
MULFFlAVT94COWWWHychgUuggyBRjbNG1gzb0dh171P0b7ZnqdDPKYq5NrmMJr3Fwtzccme/nV4RO0yuTb
```

f1jc3DdFuA8eOMaLkvLFfsnx13Jdu6ZY38LTdbc+h2fnf4KnsRbgcZ5JVfaeiKz5HFQvKzjKJH6x/uQ  
i190PF2kpg4uRmTDh6ev0En0RGh9Jg318Nr0xd87izNvUg5Jg941Q/FX98DYetR2RYe3Sp/9u+cT1EnE  
SikjyMxGjaJ3R1TQ701LfuNwqceVsYw99YeNkCwwTBmQII5a3/2i09HzxRxxiswvk23Txt41xmumhs5  
HDmj6D1/oeQ6oFHqsfd3c/auB0vFrxrqbNH68H9pw/b2wpYnnAJsgYxowaz1MaQj5Y21IGkzz7jSeTN2  
IJFTzPsHesHc2K4QS7OSWju/d1rCrA5BXSn05TIGXNukm2AwPEtduBeg4FpR7Lb/Vi0K0cgry4gVRPV1  
QnNbR5mjI2fs30C1sdZibJG2sZxo56BxeF8HzXDpbro3T+Nqg77E4cynk9a57kkqoeA1RaZn8yHJws4q  
97tFrusokRbcFwmVkyeJ5z1rbwLevz9fkTcyy3VIQY3E2mwR7kaAJepds1+iDeJBHZwBKUBPJqoPoiE0  
uKTnn8KmvyKjb+Jc8mYXR/mgT1r0c6Cgn6CM9BfynzrJoyTmlXzy2tm6dn66eHM5tsplzG0c3JEgvB2T  
5nSyAc9X0u9/rIbsWQ/8OUNFz2pu7vbfgyswakkPKMbksj3MsRHHE6mljv/P0rEtunth5/KwH1JQBWW  
R/1epqywjoev2fiJ5FqGTVBt6ZTESeAX+9AIUHV9nMx32sVw0VmIIjv6R8UUoa1b5EZHYcm804BEszx2  
/ke/e+1dEvw5ntT0kHvme5HIX9Qn0uz6u+gQpJds2aVHMGOXI670xhepwaMskl1tu268x53PYc+rjx  
NXNbKGGD+kJAISPF4d2U0tbVNf57cy1SIF4HK8+7FPxn6gqd4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc  
sWSmmWIQQZE9rIoUbxSFLThQMUW2tI0GFHCJVsppIQtmx6M9bTuerjd0Ii5oamMswxK3MkAyM1581u  
d05x4ycwfouRXOoxerpjvEmT4jfJJRh86UD/Ecihm6Fp5dm8r4Hg9nPQKebng/Gjl1+/n0S0dpaq/4rQ  
vIk2GWN7Q/M7BboqN7+5ou4qkcyOHaGC8H9OYpwrlhzB/IEYhgBVCePKW6bGkiPBReu72+Bmhgb5KaPN  
JYLFWcdNsN9+df7DcvpVcmntsM56HnKLym168o8XHJIhawjajkElhsqy1s0FOOu1EcN90coIPi7XQFI  
Q2jk7A1qits1bKhtp0m49jcsomHBwqqt5kNno6WF6xiNXODhIZ3diLHXHe1kfWPjpnPZzq2FugBvj0Tx  
+tftPYoGwiJvlu4SBeGez4jcfi2qkCofJm7EeMojox6BuBF3HKjUV+bugusy5BF8qFhb1azop/0++qHt  
BtGkQejeqESFZWWxjhsrHja68rPa0YDxxCl1tH4xS+38tFWKqgbKovck+2udz1auCSA0etjqfzz70fj  
C4hwJp8wCDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiV06e70sayn1kppG1RW1UmGhLe5g08WDB  
IO1MGfSJMFfn1gt90nJxpWQoymcUM6tuAKSoim0aExqsvK+SIHI/dchN6tiFaHLzesXhqXaHpbixVqDa  
D8gHN/yMR4IEY8e0ohVLwPAFZIWuGPdz3bgqQBmerdLp1ZhrZcjWLsoaskyDWW0G0RjkP/YSWK+s1dLe  
wadQpFAtt6x7c5DnkdmvmsXXF7a3fG7G0Tk8miLwSmpgIij80w/oLCbUgYDGEpjGiSG6XEHPktc6ThTs  
+Czc2QNgBi15g12NABEHQKxc3tzykwspoaamWrDe8vNCuKd+Tkk+q0zw66LTmE+maWX56TAQY50MQXOr  
H+6c5iULwda9Qn6rDSVNpTAn6KU6duxDb23QYthBd2orBq6T0Z8NLc8h6QVA9QEG7zs9j/fz/st94xi  
tuk8jkvr131f6bD646ixTx27NzzoQEt2E1s/ZM/iaAxwlaohOKKO5adtDATLyL7Ia1vdwdQz0XGwzus  
IKUjxDIrB0JzgCuGwg2Cj5cRL059Kfs0hgYv8rRgTa41vJcvuhEi6VtpFbGwv+T0C7Zx3xNPmnAVDwH  
UdPKu36z2wzzp89p6qrw7k0UwnN7XiGaV5Lv1Hcih7FnwLe107Mdvg41TprLFMLTwccwjhLf5mrIh6et  
Y5Zqp5ikVKv4vrb0s0SqqFLbz0Zj4KshyT2Yzaz7ZK5uQRF2f2u8gPYwn0oF4C8rNbbkdxAzoierX/s7m  
01AMD0Bjss1Lgc180v1jcn5u2drqQm1rkTG5r1k0140fTkoKnjyj90zxrD7/khxs6+Pwv6v3CzcdR8  
ojX+7MqmZxVEsdceHzE7gCfR17kb1H8bTzhaQPqh09vDLAo8RjtD2HHjYt2Qvjing8PtX57+/TBuIVPD  
wog6p8mi1hqzlhouzVpbhdrUYQLhh45SBT99ydfS2j6/zovv84C8sE1bq//zh3jku74boayGDzKjSr8u  
NbDZ5sP4DMFg/Zxqnku0nSjjv1P/DU1mfDZA+kzn8Iad/5sdedyjmPb2yIag0uEjVjQt0qz6FeoT2h7m  
MVLwBCMy12Wk+0tTXL2xEpA63Y7Mfxymj8R2Deax6WRz96IoT10Gr8+11Tsav16EHHanMJdy94Es+s+x  
00yvJnRybbNn1qvqu4FcE+16EeDiojoqbaczz0Ys6zkPCYIdrlMIbdxjcdxq1Zcw9FQXXNvREKf0k9PE  
DmHJQ8y2hJTTyqaSVqu7imgbOPR1GBV4Eu2/r1euLftwRImZc6cfRqre9Y0GaZgsNhYh6oK135Z1bsX  
uNaGoGr/ow32s5xuaq6o26hdxdFvbn7j30yvJ30rHEOGArj95DFnx2IURvMgYRrmUgwdCvmiNTLqZxf  
sbfbmB2kUWGKp2mwa5RWrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8Ypgbs6Khh1jwvTr7ah  
occhi1aa/9y53xuoB9cDrqBm08rj+4VFbyxkFMchY6RhoY23ok1ystQxxvdF5FjznDbHCenvmkz8ThJu  
uSP3VOuVrUHAZssuyiqocQhr8gxPsc6k4XDzohrp+Yfzq5YbLT0nv4+FmTIJ8JWzy5axUG2oACiL8LNY  
pQ1qmTCBixpjFM5iQKPSVdkC0TmZ8b0T+UQLa2YoxN5Thr0ktaTTN3GkeWq2DlmFkt0FCQcbjIawxY75  
RtUi1kCoocTFQ3xUNH7s/royb/sx1v+8ebi6L59L3x2PCvqoEXn9gsirr241oyxitrxsE1zaaVrU9Y  
Zcb+a49A602Nrywn81dRPb5t02mUQRp/Kg1IJPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWdnI  
S+Djqn9pbhb8wroyxOFF8aEhwu1o2hsgw91RwZ9umAfjEC4sSt8sc1ELaqaqwKn0oKg7sevLq25b6toF  
ARwgdd8yTXH70jPniFuF+UE143yk912LwxFM/squ/UZP97RqbwuPu+bv2bYe3hiqbkj5xv5IOxgs6H3F  
u1lp2zyGwHGrxwoaqz+4/npuJ7iLAv7y1g8s0Zwfc86hPyRirV2Lna3gr0bnnuOCsfpcRwdkmBlyhn  
1bGqoj0iurBkjUbYPQ4G8jzoquJmQ5xNyH60AQB0u7LdEDiC0HSUSI3SKzo1uESNSeE3qfv+UF87kzt  
eLj+RaqhAGN9nxstGn9F3yIUb76j13STbwwdEUzb7x8mhij9gQVLNFBR2tgrY=\", \"sensitive.ain  
fo\": true, \"sensitive.apps\": true, \"sensitive.aps\": true, \"sensitive.bssid\": tru  
e, \"sensitive.camera\": true, \"sensitive.cell\": true, \"sensitive.gps\": false, \"se  
nsitive.iccid\": true, \"sensitive.imsi\": true, \"sensitive.mac\": true, \"sensitive.  
ssid\": true, \"sensitive.tel\": false, \"white\_apps\": []}";

```

        String str4 =
    "MIIDLZCCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAYMQSwCQYDVQQGEWJDTjELMAKGA1UECwwCU00
    xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNNDAxMjAyMDMzMDE4WjAyMQs
    WCQYDVQQGEWJDTjELMAKGA1UECwwCU00xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wggEiMA0GCSqGSIb
    3DQEBAQUAA4IBDWAwggEKAoIBAQCT947yNGa4EPVheGp6hsDoU4KBKvmwacn6tqfwit/j1xaZZBSPcw4
    3jjxGuF4exM4NPJJtMft/j0IIwJeEx0YHDCJIqu/1pEPsXYb01bhwd5mq34c0RiRx1ji+g+d4rFRO/Xr
    eFRJSeB3w1djvoAMkxoygp+813zM6mzPd36zjbUIajfzkc5LoeITUCC6Db98XiN/hNmvcIwti01Sm9FE
    U1ip1fFb9NZ04vb2Z6xt/ti/rUVzWyshZC1qqVq4s9W4iGPqfTnBsxttiooRuproe2Ltb+J73kKTgjjH
    60pn0ljqd+FaMsL/sdy61ggM+w4ePTe4HF+/dv2ZzP+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
    ZA5/0RAVrhwrYFlnyrex4FjAfBgNVHSMEGDAwgbS83RQZA5/0RAVrhwrYFlnyrex4FjAMBgnVHRMEBT
    DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZo6fn+mH124C8Djm15jCrjYqOISpgk
    gsReEX2F00sxYqBuRPidycdsRNYQG44/i4PQrbwc9T/wLSOyHICaKbXXPhfw14PLRNR0LtgmCLOIveDy
    jzTn3BEF57tZCYSmphMUI0eJeV9o3yh1uURV3vbigh+0ca2Mql9m7N49dkkgeZ04FAWUp9yG+p1jf5tA
    Iwa6t1vvH1T8TKwjGtBH3jvYenKBk+W+DWZnDepg01+8Xozo0JP5u1u68sqf+cke0Bw1RfsTFU4ya
    OEBSIIZ/Stx7Q82K8M4XucAFV8PTT8i30QoGcsduEj4zape1vnNn7f";
        String str5 = "du56APPx0pvUiZMTZXVP";
        String str6 = "95fen";
        list.add(vm.addLocalObject(new StringObject(vm,str2)));
        list.add(vm.addLocalObject(new StringObject(vm,str3)));
        list.add(vm.addLocalObject(new StringObject(vm,str4)));
        list.add(vm.addLocalObject(new StringObject(vm,str5)));
        list.add(vm.addLocalObject(new StringObject(vm,str6)));
        Number number = module.callFunction(emulator,0x16f1d,list.toArray())[0];
        String result = vm.getObject(number.intValue()).getValue().toString();
        System.out.println(result);
    }
}

```

```

@Override
public DvmObject<?> callStaticObjectMethodV(BaseVM vm, DvmClass dvmClass,
String signature, VaList vaList) {
    switch (signature){
        case "android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;":{
            return vm.resolveClass("java/io/File").newObject(signature);
        }
        return super.callStaticObjectMethodV(vm, dvmClass, signature, vaList);
    }

@Override
public DvmObject<?> callObjectMethodV(BaseVM vm, DvmObject<?> dvmObject,
String signature, VaList vaList) {
    switch (signature){
        case "java/io/File->getAbsolutePath()Ljava/lang/String;":{
            String tag = dvmObject.getValue().toString();
            if(tag.equals("android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;")){
                return new StringObject(vm, "/storage/emulated/0");
            }
        }
        return super.callObjectMethodV(vm, dvmObject, signature, vaList);
    }
}

```

## 运行

```
[10:38:31 490] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/framework/edxposed.dex, oflags=0x0, mode=0x0
lilac Path:/system/framework/edxp.jar
[10:38:31 492] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/framework/edxp.jar, oflags=0x0, mode=0x0
lilac Path:/system/lib/libiriu_edxp.so
[10:38:31 495] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/lib64/libiriu_edxp.so, oflags=0x0, mode=0x0
lilac Path:/sbin/magisk/modules/riru_edxposed/module.prop
[10:38:31 496] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/magisk/modules/riru_edxposed/module.prop, of
lilac Path:/proc/self/mounts
[10:38:31 497] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/proc/self/mounts, oflags=0x0, mode=0x0
[10:38:31 501] INFO [com.github.unidbg.linux.AndroidSyscallHandler] (AndroidSyscallHandler:149) - pipe2 pipefd=unidbg@0xbffffdcb8, flags=0x0, readfd=4, writefd=3
vfork pid=46658
[10:38:31 533] WARN [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=197, svcNumber=0x0, PC=RX@0x401be1f8[libc.so]0x411f8, L
java.lang.UnsupportedOperationException Create breakpoint : com.github.unidbg.linux.file.PipedReadFileIO@16
at com.github.unidbg.file.linux.BaseAndroidFileIO.fstat(BaseAndroidFileIO.java:16)
at com.github.unidbg.linux.ARMS32SyscallHandler.fstat(ARM32SyscallHandler.java:2087)
at com.github.unidbg.linux.ARMS32SyscallHandler.hook(ARM32SyscallHandler.java:1991)
at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:301)
at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
```

下面是什么报错在等着我们呢？

阿西吧，到这一步我没法往下了，因为我的草稿并不是这么走的。来看看我分析测试时的思路吧

回退到MyARM32SyscallHandler还没补的时机点

```
[11:10:46 409] INFO [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/proc/self/mounts, oflags=0x0, mode=0x0
[11:10:46 428] INFO [com.github.unidbg.linux.AndroidSyscallHandler] (AndroidSyscallHandler:149) - pipe2 pipefd=unidbg@0xbffffdcb8, flags=0x0, readfd=4, writefd=3
[11:10:46 429] WARN [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=198, svcNumber=0x0, PC=RX@0x401beb5c[libc.so]0x41b5c, L
[11:10:46 432] WARN [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=358, svcNumber=0x0, PC=RX@0x401bedb0[libc.so]0x41db0, L
java.lang.AbstractMethodError Create breakpoint : com.github.unidbg.linux.file.PipedWriteFileIO@16
at com.github.unidbg.file.AbstractFileIO.dup2(AbstractFileIO.java:168)
at com.github.unidbg.linux.ARMS32SyscallHandler.dup3(ARM32SyscallHandler.java:2105)
at com.github.unidbg.linux.ARMS32SyscallHandler.hook(ARM32SyscallHandler.java:437)
at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:299)
at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
at unicorn.Unicorn.emu_start(Native Method)
at com.github.unidbg.arm.backend.UnicornBackend.emu_start(UnicornBackend.java:325)
at com.github.unidbg.AbstractEmulator.emulate(AbstractEmulator.java:378)
at com.github.unidbg.AbstractEmulator.eFunc(AbstractEmulator.java:446)
at com.github.unidbg.arm.AbstractARMEmulator.eFunc(AbstractARMEmulator.java:220)
at com.github.unidbg.Module.emulateFunction(Module.java:158)
at com.github.unidbg.linux.LinuxModule.callFunction(LinuxModule.java:232)
at com.jiuhu.shumei.w1(shumei.java:99)
```

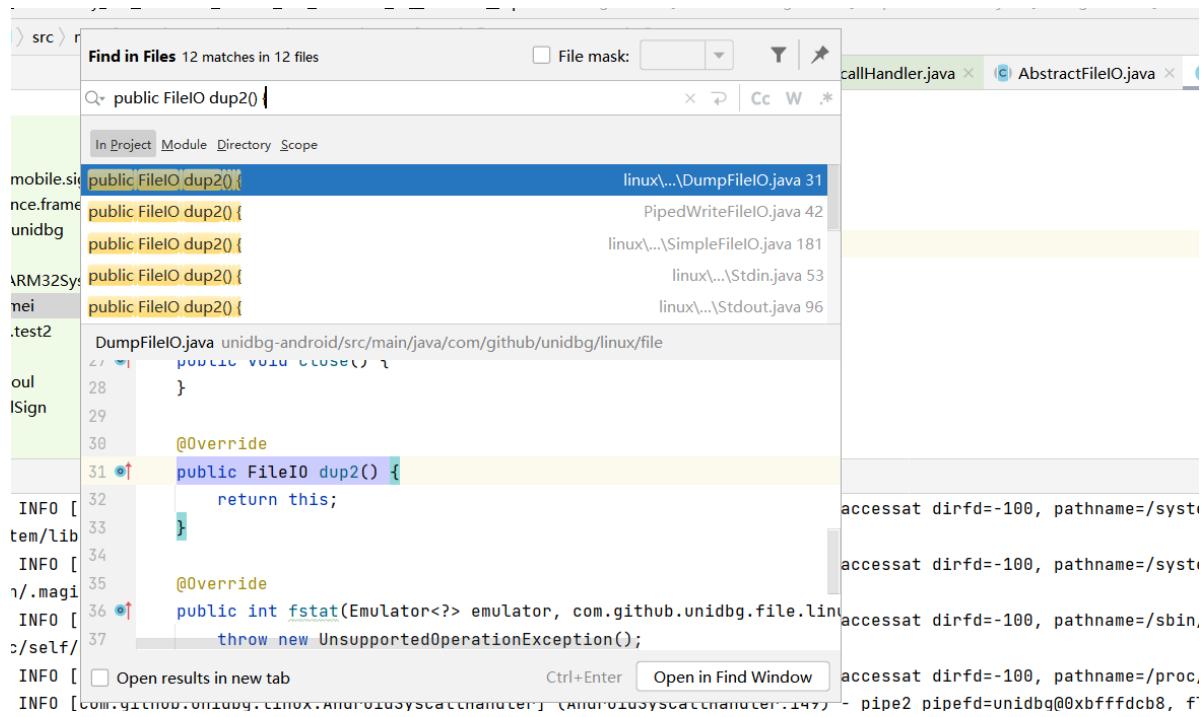
当时我选择先看报错，dup2是什么？dup2用于复制一个文件描述符，它还有一些姊妹，可以看这篇文章 [linux系统调用dup,dup2,dup3 LOVETEDA的博客-CSDN博客](#)

那为什么这儿报错？

```
153     @Override
154     public int pread(Backend backend, Pointer buffer, int count, long offset) {
155         throw new UnsupportedOperationException(getClass().getName());
156     }
157
158     @Override
159     public FileIO dup2() {
160         throw new AbstractMethodError(getClass().getName());
161     }
162
163     @Override
164     public String getPath() { throw new AbstractMethodError(getClass().getName()); }
```

这儿是个接口，报错的大意是com.github.unidbg.linux.file.PipedWriteFileIO没有实现这个dup2方法

那么有其他类型的文件形式实现了这个接口吗？可以借鉴一下吗？我们参考dumpfileIO，**return this** 完事儿。



运行代码，此时的代码

```

package com.jiuwu;

import com.github.unidbg.AndroidEmulator;
import com.github.unidbg.Emulator;
import com.github.unidbg.Module;
import com.github.unidbg.file.FileResult;
import com.github.unidbg.file.IOREsolver;
import com.github.unidbg.file.linux.AndroidFileIO;
import com.github.unidbg.linux.android.AndroidARMEmulator;
import com.github.unidbg.linux.android.AndroidEmulatorBuilder;
import com.github.unidbg.linux.android.AndroidResolver;
import com.github.unidbg.linux.android.dvm.*;
import com.github.unidbg.linux.android.dvm.array.ByteArray;
import com.github.unidbg.memory.Memory;
import com.github.unidbg.memory.SvcMemory;
import com.github.unidbg.unix.UnixSyscallHandler;
import com.github.unidbg.virtualmodule.android.AndroidModule;

import javax.crypto.Cipher;
import javax.crypto.NoSuchPaddingException;

```

```
import java.io.File;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.List;

public class shumei extends AbstractJni implements IOResolver {
    private final AndroidEmulator emulator;
    private final VM vm;
    private final Module module;

    shumei() {
        // 创建模拟器实例
        emulator = AndroidEmulatorBuilder
            .for32Bit()
            .setRootDir(new File("target/rootfs"))
            .build();

        // AndroidEmulatorBuilder builder = new AndroidEmulatorBuilder(false) {
        //     @Override
        //     public AndroidEmulator build() {
        //         return new AndroidARMEmulator(processName, rootDir,
        //             backendFactories) {
        //             @Override
        //             protected UnixSyscallHandler<AndroidFileIO>
        //             createSyscallHandler(SvcMemory svcMemory) {
        //                 return new MyARM32SyscallHandler(svcMemory);
        //             }
        //         };
        //     }
        //     ;
        //     ;
        //     ;
        //     ;
        //     emulator = builder.setRootDir(new File("target/rootfs")).build();
        // }

        // 获取模拟器的内存操作接口
        final Memory memory = emulator.getMemory();
        // 设置系统类库解析
        memory.setLibraryResolver(new AndroidResolver(23));
        // 绑定重定向
        emulator.getSyscallHandler().addIOResolver(this);

        vm = emulator.createDalvikVM(new File("unidbg-
android/src/test/resources/shumei/com.jiuwu_1.25.0_1002500.apk"));
        new AndroidModule(emulator, vm).register(memory);
        DalvikModule dm = vm.loadLibrary(new File("unidbg-
android/src/test/resources/shumei/libsmssdk.so"), true); // 加载so到虚拟内存
        //获取本SO模块的句柄,后续需要用它
        module = dm.getModule();
        vm.setJni(this);
        vm.setVerbose(true); // 打印日志

        dm.callJNI_OnLoad(emulator); // 调用JNI OnLoad
    };

    @Override
    public FileResult resolve(Emulator emulator, String pathname, int oflags) {
        System.out.println("lilac Path:"+pathname);
        // 具体的处理
    }
}
```

```
        return null;
    }

    public static void main(String[] args) {
        shumei demo = new shumei();
        demo.w1();
    }

    public void w1(){
        List<Object> list = new ArrayList<>(10);
        list.add(vm.getJNIEnv());
        list.add(0);
        DvmObject<?> obj =
            vm.resolveClass("android/content/Context").newObject(null);
        list.add(vm.addLocalObject(obj));
    }
}
```

```
String str2 = "
{\\"a1\\":\\"a11\\",\\"a3\\":\\"none\\",\\"a4\\":\\"4\\",\\"a2\\":\\"SRCM3hsEtSjSE1fQv1Cares092
5Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOCiXTuZJ+Va9w5pRw==\\",\\"a5\\":\\"\\",\\"a
7\\":\\"3.0.4\\",\\"a8\\":\\"\\",\\"a6\\":\\"android\\",\\"a44\\":\\"wifi\\",\\"a47\\":
[\"16, qualcomm\", \"4, qualcomm\", \"19, qualcomm\", \"19, qualcomm\", \"9, qualcomm\",
\"18, qualcomm\", \"18, qualcomm\", \"17, qualcomm\", \"22, qualcomm\", \"2, akm\", \"10, qu
alcomm\", \"20, qualcomm\", \"3, xiaomi\", \"30, qualcomm\", \"30, qualcomm\", \"33171027
,xiaomi\", \"33171027,xiaoMi\", \"33171036,xiaoMi\", \"33171036,xiaoMi\", \"11,xiaom
i\", \"5,Rohm\", \"5,Rohm\", \"6,Bosch\", \"29, qualcomm\", \"29, qualcomm\", \"1, qualco
mm\", \"35, qualcomm\", \"15, qualcomm\", \"27,xiaomi\", \"27,xiaomi\", \"33171029,xiao
Mi\", \"33171029,XiaoMi\", \"14, akm\", \"33171070,xiaomi\", \"33171070,xiaomi\", \"8,
Elliptic Labs\", \"33171031,xiaomi\"],\"a46\\":{\"cpu_abi\"::\\\"armeabi-
v7a\\\", \"serial\\\":\\\"unknown\\\", \"fingerprint\\\":\\\"Xiaomi\\\\polaris\\\\polaris:10\\\\Q
KQ1.190828.002\\\\V12.0.2.0.QDGCNXM:user\\\\release-keys\\\", \"model\\\":\\\"MIX
2S\\\", \"cpu_abi2\\\":\\\"armeabi\\\", \"brand\\\":\\\"Xiaomi\\\", \"board\\\":\\\"sdm845\\\", \"serial
_P\\\":\\\"unknown\\\", \"manufacturer\\\":\\\"Xiaomi\\\"},\"a38\\\":\\\"1.25.0\\\", \"a33\\\":\\\"ARMv8
Processor rev 13
(v81)\\\", \"a103\\\":\\\"faf6c8c7ad942343\\\", \"a23\\\":\\\"\\\", \"a54\\\":\\\"0000010\\\", \"a48\\\":5
905514496, \"a10\\\":\\\"10\\\", \"a11\\\":\\\"95fen\\\", \"a15\\\":\\\"false\\\", \"a17\\\":
[\\\"wlan1,,f460e217db64,\\\", \\\"wlan0,172.16.16.12,f460e296db64,fe80::f660:e2ff:fe96
:db64%wlan0\\\", \\\"p2p0,,f660e218db64,\\\"], \"a18\\\":
{\\\"ro.boot.hardware\\\":\\\"qcom\\\", \\\"gsm.sim.state\\\":\\\"LOADED,LOADED\\\", \\\"sys.usb.sta
te\\\":\\\"adb\\\", \\\"ro.debuggable\\\":\\\"0\\\"}, \"a19\\\":\\\"02:00:00:00:00:00\\\", \"a9\\\":16281
28282220, \"a39\\\":\\\"com.jiuwu\\\", \"a40\\\":1627972313927, \"a45\\\":\\\"46001\\\", \"a21\\\":
\\\", \"a24\\\":\\\"6d9de21492b99db9\\\", \"a25\\\":\\\"\\\", \"a22\\\":\\\"\\\", \"a34\\\":2803200, \"a37
\\\":1295, \"a27\\\":
[\\\"1628127546162,com.jiuwu,,1,1002500,1.25.0,1628127546162\\\", \\\"1230768000000,com
.android.cts.priv.ctsshim,,0,28,9-
5374186,1230768000000\\\", \\\"1230768000000,com.miui.contentextension,,0,10164,2.4.2
,1611338104848\\\", \\\"1230768000000,com.qualcomm.qti.qcolor,,0,29,10,1230768000000\\
\", \\\"1230768000000,com.android.internal.display.cutout.emulation.corner,,0,1,1.0,
1230768000000\\\", \\\"1230768000000,com.google.android.ext.services,,0,291900801,q_p
r1-
release_am1_291900801,1230768000000\\\", \\\"1230768000000,com.qualcomm.qti.improveto
uch.service,,0,29,10,1230768000000\\\", \\\"1230768000000,com.android.internal.displa
y.cutout.emulation.double,,0,1,1.0,1230768000000\\\", \\\"1230768000000,com.android.p
roviders.telephony,,0,29,10,1230768000000\\\", \\\"1230768000000,com.android.dynsyste
m,,0,29,10,1230768000000\\\"], \"a29\\\":\\\"4.0.c2.6-00335-0914_2350_3c8fca6,4.0.c2.6-
00335-0914_2350_3c8fca6\\\", \"a32\\\":8, \"a30\\\":\\\"<unknown
ssid>\\\", \"a31\\\":\\\"172.16.16.12\\\", \"a90\\\":28, \"a105\\\":
{}, \"a108\\\":\\\"\\\", \"a109\\\":\\\"\\\", \"a110\\\":\\\"\\\", \"a111\\\":\\\"\\\", \"a107\\\":
{\\\"java\\\\lang\\\\reflect\\\\Modifier\\\":2, \\\"com\\\\android\\\\internal\\\\telephony\\\\
/PhoneProxy\\\":2, \\\"java\\\\lang\\\\ProcessBuilder\\\":2, \\\"com\\\\android\\\\internal\\\\
telephony\\\\PhoneSubInfo\\\":2, \\\"android\\\\location\\\\LocationManager\\\":2, \\\"com\\\\
tencent\\\\mapapi\\\\service\\\\LocationManager\\\":2, \\\"com\\\\android\\\\internal\\\\te
lephony\\\\gsm\\\\GSMPhone\\\":2}, \"a20\\\":\\\"\\\", \"a49\\\":\\\"\\\", \"a52\\\":
{\\\"magisk\\\":1}, \"a53\\\":{}, \"a50\\\":
{}, \"a60\\\":\\\"u0_a349\\\", \"a62\\\":\\\"\\\\data\\\\user\\\\0\\\\com.jiuwu\\\\files\\\", \"a55\\
\":\\\"a58929cd0e3202053f6137261ecd3c40\\\", \"a57\\\":1160259262, \"a36\\\":\\\"1080,2030,44
0\\\", \"a56\\\":\\\"CN=jiuwu, OU=jiuwu, O=jiuwu, L=上海, ST=上海,
C=CN\\\", \"a76\\\":\\\"\\\", \"a88\\\":\\\"locateServiceName:android.os.BinderProxy|phoneServ
iceName:android.os.BinderProxy\\\", \"a84\\\":\\\"3vDSuAiODgqAwBUsIqCEpuAFJ+xKBFFJ383k
+\\\\M2+M=____\\\", \"a68\\\":
[], \"a92\\\":\\\"1080,2030\\\", \"a93\\\":0, \"a95\\\":-1, \"a96\\\":\\\"du56APPx0pvUi
zMTZXVP\\\", \\\"a97\\\":\\\"SRCM3hsEtSjSE1fQv1Cares0925Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOC
iXTuZJ+Va9w5pRw==\\\", \"a98\\\":\\\"\\\", \"a99\\\":\\\"\\\", \"a100\\\":\\\"\\\", \"a101\\\":\\\"\\\", \"a102
\\\":[], \"a63\\\":\\\"InputMethodInfo{com.sohu.inputmethod.sogou.xiaomi\\\\.SogouIME,
settings:
```

```
com.sohu.inputmethod.sogou.SogouIMESettingsLauncher}\\"", \"InputMethodInfo{com.iflytek.inputmethod.miui\\/.FlyIME, settings:  
com.iflytek.inputmethod.LauncherSettingsActivity\"]}, \"a67\": {}, \"a64\":  
{} , \"suc\": \"1\" , \"enable\": \"0\" , \"service\": [] } , \"a65\": 39 , \"a66\":  
{} , \"a74\": 0 , \"a73\": 0 , \"a78\": [] , \"a75\": 0 , \"a77\":  
{} , \"a86\": \"1100100\" , \"a79\": \"\" , \"a80\": \"1628128282029-  
12295\" , \"a83\": \"1001100\" , \"a85\":  
[] , \"a69\": 15533490176 , \"a71\": 118982303744 , \"a72\":  
{} , \"temp\": 370 , \"vol\": 4095 , \"level\": 85 , \"scale\": 100 , \"status\": 2 } , \"a70\": 1568  
4485120 } ;
```

```
String str3 = "
{\\"all_atamper\\":true,\\"core_atamper\\":true,\\"hook_java_switch\\":true,\\"hook_switc
tch\\":false,\\"risk_apps\\": [{"\"xposed\\":
{\\"pn\\":\"de.robv.android.xposed.installer\",\"uri\\\":\"\"}, {\\"controllers\\":
{\\"pn\\":\"com.soft.controllers\",\"uri\\\":\"\"}, {\\"apk008v\\":
{\\"pn\\":\"com.soft.apk008v\",\"uri\\\":\"\"}, {\\"apk008Tool\\":
{\\"pn\\":\"com.soft.apk008Tool\",\"uri\\\":\"\"}, {\\"ig\\":
{\\"pn\\":\"com.doubee.ig\",\"uri\\\":\"\"}, {\\"anjian\\":
{\\"pn\\":\"com.cyjh.mobilejian\\\",\"uri\\\":\"\"}, {\\"rktech\\":
{\\"pn\\":\"com.ruokuai.rktech\",\"uri\\\":\"\"}, {\\"magisk\\":
{\\"pn\\":\"com.topjohnwu.magisk\",\"uri\\\":\"\"}, {\\"kinguser\\":
{\\"pn\\":\"com.kingroot.kinguser\",\"uri\\\":\"\"}, {\\"substrate\\":
{\\"pn\\":\"com.saurik.substrate\",\"uri\\\":\"\"}, {\\"touchsprite\\":
{\\"pn\\":\"com.touchsprite.android\",\"uri\\\":\"\"}, {\\"scriptdroid\\":
{\\"pn\\":\"com.stardust.scriptdroid\",\"uri\\\":\"\"}, {\\"toolhero\\":
{\\"pn\\":\"com.mobileuncle.toolhero\",\"uri\\\":\"\"}, {\\"huluxia\\":
{\\"pn\\":\"com.huluxia.gametools\",\"uri\\\":\"\"}, {\\"apkeditor\\":
{\\"pn\\":\"com.gmail.heagoo.apkeditor.pro\",\"uri\\\":\"\"}, {\\"xposeddev\\":
{\\"pn\\":\"com.sollyu.xposed.hook.model.dev\",\"uri\\\":\"\"}, {\\"anywhere\\":
{\\"pn\\":\"com.txy.anywhere\",\"uri\\\":\"\"}, {\\"burgerzws\\":
{\\"pn\\":\"pro.burgerz.wsm.manager\",\"uri\\\":\"\"}, {\\"vdloc\\":
{\\"pn\\":\"com.virtualdroid.loc\",\"uri\\\":\"\"}, {\\"vdtxl\\":
{\\"pn\\":\"com.virtualdroid.txl\",\"uri\\\":\"\"}, {\\"vdwzs\\":
{\\"pn\\":\"com.virtualdroid.wzs\",\"uri\\\":\"\"}, {\\"vdkit\\":
{\\"pn\\":\"com.virtualdroid.kit\",\"uri\\\":\"\"}, {\\"vdwxg\\":
{\\"pn\\":\"com.virtualdroid.wxg\",\"uri\\\":\"\"}, {\\"vdgps\\":
{\\"pn\\":\"com.virtualdroid.gps\",\"uri\\\":\"\"}, {\\"a1024mlloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\"}, {\\"drhgz\\":
{\\"pn\\":\"com.deruhai.guangzi.noroot2\",\"uri\\\":\"\"}, {\\"yggb\\":
{\\"pn\\":\"com.mcmonjmb.yggb\",\"uri\\\":\"\"}, {\\"xsrv\\":
{\\"pn\\":\"xiake.xserver\",\"uri\\\":\"\"}, {\\"fakeloc\\":
{\\"pn\\":\"com.dracrays.fakeloc\",\"uri\\\":\"\"}, {\\"ultra\\":
{\\"pn\\":\"net.anylocation.ultra\",\"uri\\\":\"\"}, {\\"locationcheater\\":
{\\"pn\\":\"com.wifi99.android.locationcheater\",\"uri\\\":\"\"}, {\\"dwzs\\":
{\\"pn\\":\"com.dingweizshou\",\"uri\\\":\"\"}, {\\"mockloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\"}, {\\"anywhereclone\\":
{\\"pn\\":\"com.txy.anywhere.clone\",\"uri\\\":\"\"}, {\\"fakelocc\\":
{\\"pn\\":\"com.dracrays.fakelocc\",\"uri\\\":\"\"}, {\\"mockwxlocation\\":
{\\"pn\\":\"com.tandy.android.mockwxlocation\",\"uri\\\":\"\"}, {\\"anylocation\\":
{\\"pn\\":\"net.anylocation\",\"uri\\\":\"\"}, {\\"totalcontrol\\":
{\\"pn\\":\"com.sigma_rt.totalcontrol\",\"uri\\\":\"\"}, {\\"ipjl2\\":
{\\"pn\\":\"com.chuangdian.ipjl2\",\"uri\\\":\"\"}], {\\"risk_dirs\\": [{"\"008Mode\\":
{\\"dir\\":\".system/008Mode\", \"type\\\":\"sdcard\"}, {\\"008OK\\":
{\\"dir\\":\".system/008OK\", \"type\\\":\"sdcard\"}, {\\"008system\\":
{\\"dir\\":\".system/008system\", \"type\\\":\"sdcard\"}, {\\"iGrimace\\":
{\\"dir\\":\"iGrimace\", \"type\\\":\"sdcard\"}, {\\"touchelper\\":
{\\"dir\\\":\"/data/data/net.aisence.Touchelper\", \"type\\\":\"absolute\"}, {\\"elfscript\\":
{\\"dir\\\":\"/mnt/sdcard/touchelf/scripts/\", \"type\\\":\"absolute\"}, {\\"spritelua\\": {\\"dir\\\":\"/mnt/sdcard/TouchSprite/lua\", \"type\\\":\"absolute\"}, {\\"spritelog\\": {\\"dir\\\":\"/mnt/sdcard/TouchSprite/log\", \"type\\\":\"absolute\"}, {\\"assistant\\": {\\"dir\\\":\"/data/data/com.xxAssistant\", \"type\\\":\"absolute\"}, {\\"assistantscript\\":
{\\"dir\\\":\"/mnt/sdcard/com.xxAssistant/script\", \"type\\\":\"absolute\"}, {\\"mobilejian\\":
{\\"dir\\\":\"/data/data/com.cyjh.mobilejian\", \"type\\\":\"absolute\"}], {\\"risk_file_switch\\": true, {\\"risk_files\\": \"zb5E/i2Gv4IxR50xSBiXKChu8gdkDXKei9GwOBNbN6jq3xMULFFAvT94C0wwwhychgUgggyBRjbNG1gz0dh171P0b7ZnqdDPKYq5NrmMJr3Fwtzccme/nv4R00yuTb

```

f1jc3DdFuA8eOMaLkvLFfsxnx13Jdu6ZY38LTdbc+h2fnf4KnsRbgcZ5JVfaeiKz5HFQvKzjKJH6x/uQ  
i190PF2kpg4uRmTDh6ev0En0RGh9Jg318Nr0xd87izNvUg5Jg941Q/FX98DYetR2RYe3Sp/9u+cT1EnE  
SikjyMxGjaJ3R1TQ701LfuNwqceVsYw99YeNkCwwTBMQII5a3/2i09HzxRXXiswvk23Txt41xmumhs5  
HDmj6D1/oeQ6oFHqsfd3c/auB0vFrxrqbNH68H9pw/b2wpYnnAJsgYxowaz1MaQj5Y21IGkzz7jSeTN2  
IJFTzPsHesHc2K4QS7OSWju/d1rCrA5BXSn05TIGXNukm2AwPEtduBeg4FpR7Lb/Vi0K0cgry4gVRPV1  
QnNbR5mjI2fs30C1sdZibJG2sZxo56BxeF8HzXDpBr03T+Nqg77E4cynk9a57kkq0eA1RaZn8yHJws4q  
97tFrusokRbcFwmVkyeJ5z1rbwLevZ9fkTcyy3VIQY3E2mwR7kaAJepds1+iDeJBHZwBKUBPJqoPoiE0  
uKTnn8KmvyKjb+Jc8mYXR/mgT1r0c6Cgn6CM9BfynzrJoyTmlXzy2tm6dn66eHM5tsplzG0c3JEgvB2T  
5nSyAc9X0u9/rIbsWQ/8OUNFz2pu7vbfgyswakkPKMbksj3MsRHHE6mljv/P0rEtunth5/KwH1JQBWW  
R/1epqywjoev2fiJ5FqGTVBt6ZTESeAX+9AIUHV9nMx32sVw0VmIIjV6R8UUoa1b5EZHYcm804BEszx2  
/ke/e+1dEvw5ntT0khvme5HIX9Qn0uz6u+gQpJds2aVHMGOXI670xhepwaMskl1tu268x53PYc+rjx  
NXNbKGGD+kJAISPF4d2U0tbVNf57cy1SIF4HK8+7FPxn6gqd4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc  
sWSmmWIQQZE9rIoUbxSFLThQMUW2tI0GFHCJVsppIQtmxz6M9bTuerjd0Ii5oamMswxK3MkAyM1581u  
d05x4ycwfouRXOoxerpjvEmT4jfJJRh86UD/Ecihm6Fp5dm8r4Hg9nPQKebng/Gjl1+/n0S0dpaq/4rQ  
vIk2GWN7Q/M7BboqN7+5ou4qkcyOHaGC8H9OYpwrlhzB/IEYhgBVCePKW6bGkiPBReu72+Bmhgb5KaPN  
JYLFWcdNsN9+df7DcvpVcmNTSM56HnKLym168o8XHJIhawjajkElhsqy1sL0FOOu1EcN90coIPi7XQFI  
Q2jk7A1qits1bKhtp0m49jcsomHBwqqT5kNno6WF6xiNXODhIZ3diLHXHe1kfWPjpnPZzq2FugBvj0Tx  
+tftPYoGwiJvlu4SBeGez4jcfi2qkCofJm7EeMojox6BuBF3HKjUV+bugusy5BF8qFhb1azop/0++qHt  
BtGkQejeqESFZWWxjhsrHja68rPa0YDxxCl1tH4xS+38tFWKqgbKovck+2udz1auCSA0etjqfzz70fj  
C4hwJp8wCDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiV06e70sayn1kppG1RW1UmGhLe5g08WDB  
IO1MGfSJMFfn1gt90nJxpWQoymcUM6tuAKSoim0aExqsvK+SIHI/dchN6tiFaHLzesXhqXaHpbixVqDa  
D8gHN/yMR4IEY8e0ohVLwPAFZIWuGPdz3bgqQBmerdLp1ZhrZcjWLsoaskyDWW0G0RjkP/YSWK+s1dLe  
wadQpFAtt6x7c5DnkdmvmsXXF7a3fG7G0Tk8miLwSmpgIij80w/oLCbUgYDGEpjGiSG6XEHPktc6ThTs  
+Czc2QNgBi15g12NABEHQKxc3tzykwspoaamWrDe8vNCuKd+Tkk+q0zw66LTmE+maWX56TAQY50MQXOr  
H+6c5iULwda9Qn6rDSVNpTAn6KU6duxDb23QYthBd2orBq6T0Z8NLc8h6QVA9QEG7zs9j/fz/st94xi  
tuk8jkvr131f6bD646ixTx27NzzoQEt2E1s/ZM/iaAxwlaohOKKO5adtDATLyL7Ia1vdwdQz0XGwzus  
IKUjxDIrB0JzgCuGwg2Cj5cRL059Kfs0hgYv8rRgTa41vJcvuhEi6VtpFbGwv+T0C7Zx3xNPmnAVDwH  
UdPKu36z2wzzp89p6qrw7k0UwnN7XiGaV5Lv1Hcih7FnwLe107Mdvg41TprLFMLTwccwjhLf5mrIh6et  
Y5Zqp5ikVKv4vrb0s0SqqFLbz0Zj4KshyT2Yzaz7ZK5uQRF2f2u8gPYwn0oF4C8rNbbkdxAzoierX/s7m  
01AMD0Bjss1Lgc180v1jcn5u2drqQm1rkTG5r1k0140fTkoKnjyj90zxrD7/khxs6+Pwv6v3CzcdR8  
ojX+7MqmZxVEsdceHzE7gCfR17kb1H8bTzhaQPqh09vDLAo8Rjtd2HHjYt2Qvjing8PtX57+/TBuIVPD  
wog6p8mi1hqzlhouzVpbhdruYQLhh45SBT99ydfs2j6/zovv84C8sE1bq//zh3jku74boayGDzKjSr8u  
NbDZ5sP4DMFg/Zxqnku0nSjjv1P/DU1mfDZA+kzn8Iad/5sdedyjmPb2yIag0uEjVjQt0qz6FeoT2h7m  
MVLwBCMy12Wk+0tTXL2xEpA63Y7Mfxymj8R2Deax6WRz96IoT10Gr8+11Tsav16EHHanMJdy94Es+s+x  
00yvJnRybbNn1qvqu4FcE+16EeDiojoqbaczz0Ys6zkPCYIdrlMIbdxjcdxq1Zcw9FQXXNvREKf0k9PE  
DmHJQ8y2hJTTyqaSVqu7imgbOPR1GBV4Eu2/r1euLftwRIMzC6cfRqre9Y0GazGsnHyYh6oK135Z1bsX  
uNaGOGR/ow32s5xuaq6o26hdxdFvbwn7j30yvJ30rHEOGArj95DFnx2IURvMgYRrmUgwdCvmiNTLqZxf  
sbfbmB2kUWGKp2mwa5RWrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8YpgBS6Khh1jwvTr7ah  
occhi1aa/9y53xuoB9cDrqBm08rj+4VFbyxkFMCHy6RhoY23ok1ystQxxvdF5FjznDbHCenvmkz8Thju  
uSP3VOuVrUHAZssuyiqocQhr8gxPsc6k4XDzohrp+Yfzq5YbLT0nv4+FmTIJ8JWzy5axUG2oACiL8LNY  
pQ1qmTCBixpjFM5iQKPSVdkC0TmZ8b0T+UQLa2YoxN5Thr0ktaTTN3GkeWq2DlmFkt0FCQcbjIawxy75  
RtUi1kcooctFQ3xUNH7s/royb/sx1v+8ebi6L59L3x2PCvqoEXn9gsirr241oyxitrxsE1zaaVrU9Y  
Zcb+a49A602Nrywn81dRPb5t02mUQRp/Kg1IJPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWdnI  
S+Djqn9pbhb8wroyxOFF8aEhwu1o2hsgw91Rwz9umAfjEC4sSt8sc1ELaqaqwKn0oKg7sevLq25b6toF  
ARwgdd8yTXH70jPniFuF+UE143yk912LwxFM/squ/UZP97RqbwuPu+bv2bYe3hiqbkj5xv5IOxgs6H3F  
u1lp2zyGwHGrxwoaqz+4/npuJ7iLAv7y1g8s0zWfc86hPyRirV2LNa3gr0bNnuOCsfpcRwdkmBlyhn  
1bGqoj0iurBkjUbYPQ4G8jzoquJmQ5xNyH60AQB0u7LdEDiC0HSUSI3SKzo1uESNSeE3qfv+UF87kzt  
eLj+RaqhAGN9nxstGn9F3yIUb76j13STbwwdEUzb7x8mhij9gQVLNFBR2tgrY=\", \"sensitive.ain  
fo\": true, \"sensitive.apps\": true, \"sensitive.aps\": true, \"sensitive.bssid\": tru  
e, \"sensitive.camera\": true, \"sensitive.cell\": true, \"sensitive.gps\": false, \"se  
nsitive.iccid\": true, \"sensitive.imsi\": true, \"sensitive.mac\": true, \"sensitive.  
ssid\": true, \"sensitive.tel\": false, \"white\_apps\": []}";

```

        String str4 =
    "MIIDLZCCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAYMQSwCQYDVQQGEWJDTjELMAKGA1UECwwCU00
    xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNNDAxMjAyMDMzMDE4WjAyMQs
    WCQYDVQQGEWJDTjELMAKGA1UECwwCU00xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wggEiMA0GCSqGSIb
    3DQEBAQUAA4IBDWAwggEKAoIBAQCT947yNGa4EPVheGp6hsDou4KBKvmwacn6tqfwit/j1xaZZBSPcw4
    3jjxGuF4exM4NPJJtMft/j0IIwJeEx0YHDCJIqu/1pEPsXYb01bhwd5mq34c0RiRx1ji+g+d4rFRO/Xr
    eFRJSeB3w1djvoAMkxoygp+813zM6mzPd36zjbUIajfzkc5LoeITUCC6Db98XiN/hNmvcIwti01Sm9FE
    U1ip1fFb9NZ04vb2Z6xt/ti/rUVzWyshZC1qqVq4s9W4iGPqfTnBsxttiooRuproe2Ltb+J73kKTgjjH
    60pn0ljqd+FaMsL/sdy61ggM+w4ePTe4HF+/dv2ZzP+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
    ZA5/0RAVrhwrYFlnyrex4FjAfBgNVHSMEGDAwgbS83RQZA5/0RAVrhwrYFlnyrex4FjAMBgnVHRMEBTA
    DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZo6fn+mH124C8Djm15jCrjYqOISpgk
    gsReEX2F00sxYqbUPidycdsRNYQG44/i4PQrbwc9T/wLSOyHICaKbXXPhfw14PLRNR0LtgmCLOIveDy
    jzTn3BEF57tZCYSmphMUI0eJeV9o3yh1uURV3vbigh+0ca2Mql9m7N49dkkgeZ04FAWUp9yG+p1jf5tA
    Iwa6t1vvH1T8TKwjGtBH3jvYenKBk+W+DWZnDepg01+8Xozo0JP5u1u68sqf+cke0Bw1RfsTFU4yA
    OEBSIIZ/Stx7Q82K8M4XucAFV8PTT8i30QoGcsduEj4zape1vnNn7f";
        String str5 = "du56APPx0pvUizMTZXVP";
        String str6 = "95fen";
        list.add(vm.addLocalObject(new StringObject(vm,str2)));
        list.add(vm.addLocalObject(new StringObject(vm,str3)));
        list.add(vm.addLocalObject(new StringObject(vm,str4)));
        list.add(vm.addLocalObject(new StringObject(vm,str5)));
        list.add(vm.addLocalObject(new StringObject(vm,str6)));
        Number number = module.callFunction(emulator,0x16f1d,list.toArray())[0];
        String result = vm.getObject(number.intValue()).getValue().toString();
        System.out.println(result);
    }
}

```

```

@Override
public DvmObject<?> callStaticObjectMethodV(BaseVM vm, DvmClass dvmClass,
String signature, VaList vaList) {
    switch (signature){
        case "android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;":{
            return vm.resolveClass("java/io/File").newObject(signature);
        }
        return super.callStaticObjectMethodV(vm, dvmClass, signature, vaList);
    }

@Override
public DvmObject<?> callObjectMethodV(BaseVM vm, DvmObject<?> dvmObject,
String signature, VaList vaList) {
    switch (signature){
        case "java/io/File->getAbsolutePath()Ljava/lang/String;":{
            String tag = dvmObject.getValue().toString();
            if(tag.equals("android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;")){
                return new StringObject(vm, "/storage/emulated/0");
            }
        }
        return super.callObjectMethodV(vm, dvmObject, signature, vaList);
    }
}

```

```

lilac Path:/sbin/.magisk/modules/riru-core
[11:18:17 485] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/.magisk/modules/riru-core, oflags=0x0, mode=0
lilac Path:/system/framework/edxposed.dex
[11:18:17 487] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/framework/edxposed.dex, oflags=0x0, mode=0x
lilac Path:/system/framework/edxp.jar
[11:18:17 489] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/framework/edxp.jar, oflags=0x0, mode=0x0
lilac Path:/system/lib/libriru_edxp.so
[11:18:17 491] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/lib/libriru_edxp.so, oflags=0x0, mode=0x0
lilac Path:/system/lib64/libriru_edxp.so
[11:18:17 492] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/system/lib64/libriru_edxp.so, oflags=0x0, mode=0x0
lilac Path:/sbin/.magisk/modules/riru_edxposed/module.prop
[11:18:17 494] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/sbin/.magisk/modules/riru_edxposed/module.prop, of
lilac Path:/proc/self/mounts
[11:18:17 495] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/proc/self/mounts, oflags=0x0, mode=0x0
[11:18:17 510] INFO [com.github.unidbg.linux.AndroidSyscallHandler] (AndroidSyscallHandler:149) - pipe2 pipefd=unidbg@0xbffffdcb8, flags=0x0, readfd=4, writefd=3
[11:18:17 511] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=190, svcNumber=0x0, PC=RX@0x401beb5c[libc.so]0x41b5c, L
[11:18:17 512] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:979) - execve filename=/system/bin/sh, args=[sh, -c, cat /proc/sys/kernel/random/boot_id], exit with code: 127
Exception in thread "main" java.lang.NullPointerException Create breakpoint : Cannot invoke "com.github.unidbg.linux.Android.DvmObject.getValue()" because the return value of "co
at com.jiuwu.shumei.w1(shumei.java:100)
at com.jiuwu.shumei.main(shumei.java:80)

Process finished with exit code 1

```

这里有个大问题， execve是什么？它的执行流程是怎样的？

官方解释

execve()用来执行参数filename字符串所代表的文件路径，第二个参数系利用数组指针来传递给执行文件，最后一个参数则为传递给执行文件的新环境变量数组。

它等价于下图

```
C:\Users\pr0214>adb shell
polaris:/ $ su
polaris:/ # cat /proc/sys/kernel/random/boot_id
7c440758-9eb5-4f55-8aea-2af49230b386
```

接下来把我们的SyscallHandler加上去

```

>>> SP=0xbffffdc00 LR=RAX@0x401b5f3f[libc.so]0x38f
>>> R0=0x4 r1=0x3 r2=0x0 r3=0xbffffdc78 r4=0x0 r5=0x4 r6=0x4 r7=0xd0 r8=0xbdabce7 sb=0xecdd54c4 sl=0xbffff2bc fp=0xe7fd07b4 ip=0xbffffed90
>>> SP=0xbffffdc68 LR=RX@0x401c37f7[libc.so]0x467f7 PC=RX@0x401bec88[libc.so]0x41c88 cpsr: N=0, Z=1, C=1, V=0, T=0, mode=0b10000
[11:31:13 745] DEBUG [com.github.unidbg.linux.UnixSyscallHandler] (UnixSyscallHandler:352) - fcntl fd=4, cmd=3, arg=0
>>> R0=0x4 r1=0x401c4f91 r2=0x0 r3=0x4 r4=0x401fceac r5=0x9779 r6=0xbffffedf8 r7=0x6 r8=0xbdabce7 sb=0xecdd54c4 sl=0xbffff2bc fp=0xe7fd07b4 ip=0xbffffed90
>>> SP=0xbffffdc98 LR=RX@0x4019fe1 PC=RX@0x401be264[libc.so]0x41264 cpsr: N=0, Z=1, C=0, V=0, T=0, mode=0b10000
[11:31:13 746] DEBUG [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1963) - close fd=3
>>> R0=0x4 r1=0xbffffdc08 r2=0x0 r3=0x401fceac r5=0xbffffdc88 r6=0xbffffdc8c r7=0xc5 r8=0xffff sb=0x52d23bcd sl=0x1e79d67f fp=0xfd7edbb7 ip=0x0
>>> SP=0xbffffdc10 LR=RX@0x401b5f3f[libc.so]0x38f PC=RX@0x401be1f8[libc.so]0x411f8 cpsr: N=0, Z=0, C=1, V=0, T=0, mode=0b10000
[11:31:13 750] DEBUG [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:2005) - fstat file=PipedRead: 3, stat=unidbg@0xbffffdc10, from=RX@0x401b5f3f[libc.so]0x38f
[11:31:13 752] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=197, svcNumber=0x0, PC=RX@0x401be1f8[libc.so]0x411f8,
java.lang.UnsupportedOperationException Create breakpoint : com.github.unidbg.linux.file.PipedReadFileIO
at com.github.unidbg.file.linux.BaseAndroidFileIO.fstat(BaseAndroidFileIO.java:16)
at com.github.unidbg.linux.ARM32SyscallHandler.fstat(ARM32SyscallHandler.java:2087)
at com.github.unidbg.linux.ARM32SyscallHandler.fstat(ARM32SyscallHandler.java:1991)
at com.github.unidbg.linux.ARM32SyscallHandler.hook(ARM32SyscallHandler.java:301)
at com.github.unidbg.arm.backend.UnicornBackend$hook(UnicornBackend.java:299)
at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
at unicorn.Unicorn.emu_start(Native Method)
```

又到了这个地方，问题怎么解决呢？重写pipe2，把我们上面得到的ID填进去即可，为什么这么做呢，我现在给不了好的解释，一是因为忘记当时为什么这么想的了，二是对Unix了解太浅，感兴趣的可以看《LINUX-Unix系统编程手册》。

```

package com.jiuwu;

import com.github.unidbg.Emulator;
import com.github.unidbg.arm.context.EditableArm32RegisterContext;
import com.github.unidbg.linux.ARM32SyscallHandler;
import com.github.unidbg.linux.file.ByteArrayFileIO;
import com.github.unidbg.linux.file.DumpFileIO;
import com.github.unidbg.memory.SvcMemory;
import com.sun.jna.Pointer;

import java.util.concurrent.ThreadLocalRandom;

public class MyARM32SyscallHandler extends ARM32SyscallHandler {
    public MyARM32SyscallHandler(SvcMemory svcMemory) {
```

```

        super(svcMemory);
    }

    @Override
    protected boolean handleUnknownSyscall(Emulator emulator, int NR) {
        switch (NR) {
            case 190:
                vfork(emulator);
                return true;
        }

        return super.handleUnknownSyscall(emulator, NR);
    }

    private void vfork(Emulator<?> emulator) {
        EditableArm32RegisterContext context = (EditableArm32RegisterContext)
emulator.getContext();
        int childPid = emulator.getPid() +
ThreadLocalRandom.current().nextInt(256);
        int r0 = childPid;
        System.out.println("vfork pid=" + r0);
        context.setR0(r0);
    }

    protected int pipe2(Emulator<?> emulator) {
        EditableArm32RegisterContext context = (EditableArm32RegisterContext)
emulator.getContext();
        Pointer pipefd = context.getPointerArg(0);
        int flags = context.getIntArg(1);
        int write = getMinFd();
        this.fdMap.put(write, new DumpFileIO(write));
        int read = getMinFd();
        String stdout = "9ab5f193-ca2a-4d7e-8dc2-09e0ff1f257f\n";
        this.fdMap.put(read, new ByteArrayFileIO(0, "pipe2_read_side",
stdout.getBytes()));
        pipefd.setInt(0, read);
        pipefd.setInt(4, write);
        System.out.println("pipe2 pipefd=" + pipefd + ", flags=0x" + flags + ",
read=" + read + ", write=" + write + ", stdout=" + stdout);
        context.setR0(0);
        return 0;
    }
}

```

运行测试，发现已经到了“下一关”

```

11:42:10 180 DEBUG [com.github.unidbg.unidbg.DalvikVM] (DalvikVM$22) - getStringing pointer=0x40045a24, size=-1, encoding=UTF-8, ref=0x40045a24
[11:42:10 180] DEBUG [com.github.unidbg.unidbg.DalvikVM] (DalvikVM$20:377) - GetMethodID class=unidbg@0x17b1136d, methodName=getPublicKey, args=()
[11:42:16 180] DEBUG [com.github.unidbg.unidbg.DvmClass] (DvmClass:133) - getMethodID signature=java/security/cert/Certificate->getPublicKey()Ljava, JNIEnv->GetMethodID([java/security/cert/Certificate.getPublicKey()Ljava/security/PublicKey;) => 0x74af4233 was called from RX@0x40045a25[libmsdk.so]0x45a25
[11:42:16 180] DEBUG [com.github.unidbg.unidbg.DalvikVM] (DalvikVM$110:2402) - ExceptionCheck throwable=null
[11:42:16 180] DEBUG [com.github.unidbg.unidbg.DvmClass] (DvmClass:22:425) - CallObjectMethodV object=unidbg@0x4b5a5ed1, jmethodID=unidbg@0x74af423
[11:42:16 180] DEBUG [com.github.unidbg.unidbg.DvmMethod] (DvmMethod:callObjectMethodV) => Valist64 args=()Ljava/security/PublicKey;, shorty=[]
[11:42:16 181] WARN [com.github.unidbg.unidbg.ARMSyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=-1073746648, svcNumber=0x115, PC=un
java.lang.UnsupportedOperationException Create breakpoint : java/security/cert/Certificate->getPublicKey()Ljava/security/PublicKey;
    at com.github.unidbg.unidbg.Android.dvm.AbstractJni.callObjectMethodV(AbstractJni.java:357)
    at com.jiulu.shumei.callObjectMethodV(shumei.java:125)
    at com.github.unidbg.unidbg.Android.dvm.AbstractJni.callObjectMethodV(AbstractJni.java:224)
    at com.github.unidbg.unidbg.Android.dvm.DvmMethod.callObjectMethodV(DvmMethod.java:85)
    at com.github.unidbg.unidbg.Android.dvm.DalvikVM$22.handle(DalvikVM.java:434)
    at com.github.unidbg.unidbg.ARMSyscallHandler.hook(ARMSyscallHandler.java:183)
    at com.github.unidbg.arm.backend.UncornBackend$6.hook(UncornBackend.java:299)
    at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
    at unicorn.Unicorn.emu_start(Native Method)
    at com.github.unidbg.arm.backend.UncornBackend.emu_start(UncornBackend.java:325)
    at com.github.unidbg.AbstractEmulator.emulate(AbstractEmulator.java:370)
    at com.github.unidbg.AbstractEmulator.eFunc(AbstractEmulator.java:446)
    at com.github.unidbg.arm.AbstractARMEmulator.eFunc(AbstractARMEmulator.java:228)
    at com.github.unidbg.Module.emulateFunction(Module.java:158)
    at com.github.unidbg.linux.LinuxModule.callFunction(LinuxModule.java:232)
    at com.jiulu.shumei.w1(shumei.java:99)

```

这到底是怎么回事呢？是不是有点稀里糊涂了呢

问题是从哪里开始的？——是从vfork

我们看一下vfork开始的代码逻辑，在我们补的vfork里添加打印调用栈的代码

```

24
25
26
27
28
29     @
30         private void vfork(Emulator<?> emulator) {
31             emulator.getUnwinder().unwind();   打印调用栈
32             EditableArm32RegisterContext context = (EditableArm32RegisterContext) emulator.getContext();
33             int childPid = emulator.getPid() + ThreadLocalRandom.current().nextInt(bound: 256);
34             int r0 = childPid;
35             System.out.println("vfork pid=" + r0);
36         }
37
38     @
39         protected int pipe2(Emulator<?> emulator) {

```

运行

```

14:27:24 /70 INFO [com.github.unidbg.unidbg.ARMSyscallHandler] (ARM32SyscallHandler:1040) - Dereferenced dirfd=-100, pathname=/proc/self/mounts, flags=0
lilac Path:/proc/self/mounts
[14:29:21 799] INFO [com.github.unidbg.unidbg.ARMSyscallHandler] (ARM32SyscallHandler:1848) - faccessat dirfd=-100, pathname=/proc/self/mounts, oflags=pipe2
pipe2 pipefd=unidbg@0xbffffc8, flags=0x0, read=4, write=3, stdout=9ab5f193-ca2a-4d7e-8dc2-08e0ff1f27f

[0x4017d000][ libc.so][0x2f5c7] popen + 0xa
[0x40000000][ libmsdk.so][0x5aa83]
File closed 'pipe2_read_side' from RX@0x40196fe1[libc.so]0x19fe1
File closed 'com.github.unidbg.unidbg.file.DumpFile@0x69b794e2' from RX@0x40196fe1[libc.so]0x19fe1
[14:29:21 843] INFO [com.github.unidbg.unidbg.ARMSyscallHandler] (ARM32SyscallHandler:979) - execve filename=/system/bin/sh, args=[sh, -c, cat /proc/s
exit with code: 127
[14:29:21 843] WARN [com.github.unidbg.AbstractEmulator] (AbstractEmulator:389) - emulate RX@0x40016f1d[libmsdk.so]0x16f1d exception sp=unidbg@0xbffffd

```

好家伙，真相大白了，我们有理由相信，从vfork开始的所有问题都是popen引起的！

为什么这么说呢，首先我们看一下示例，代码在作用上等价于在adb shell中输入getprop ro.build.id

```

char value[PROP_VALUE_MAX] = {0};
std::string cmd = "getprop ro.build.id";
FILE* file = popen(cmd.c_str(), "r");
fread(value, PROP_VALUE_MAX, 1, file);
pclose(file);

```

popen会创建一个管道，调用fork产生一个子进程，在shell中运行getprop ro.build.id，在libc中看一看。

```

    v22 = 0;
    if ( _strchr(a2, 114) )
        v6 = "";
    else
        v6 = "w";
    v21 = v6;
    if ( j_pipe2(v23, v4) == -1 )
        return 0;
    }
    v18 = (int *)j_malloc(16);
    if ( !v18 )
    {
        j_close(v23);
        v5 = j_close(v24);
        *(DWORD *)j__errno(v5) = 12;
        return 0;
    }
    v7 = j_nthread_rwlock_rdlock(&pidlist_lock);
    v8 = j_vfork(v7);
    v9 = v8;
    if ( v8 == -1 )
    {
        v11 = (DWORD)((int *)void)j__errno();
        v12 = *v11;
        v13 = v11;
        j_pthread_rwlock_unlock(&pidlist_lock);
        j_free(v18);
        j_close(v23);
        j_close(v24);
        *v13 = v12;
        return 0;
    }
    if ( !v8 )
    {
        for ( i = (DWORD *)pidlist; i; i = (DWORD *)*i )
            j_close(i[2]);
    }
0002F5CE popen:70 (2F5CE)

```

可以在其函数里看到我们讨厌的这些调用，那么我们做了什么应对呢？

首先是vfork，popen新开进程只是为了跑shell而已，所以我们可以自行实现vfork，啥都不做，随便返回一个进程ID。

其次是自实现pipe2，pipe2用于进程间的通信，popen新建进程后，通过一系列操作，取得了数据（比如此处就是获取“**getprop ro.build.id**”），然后得把这个结果通过pipe2传回给主进程。所以我们重写pipe2，直接将结果硬编码写回去。

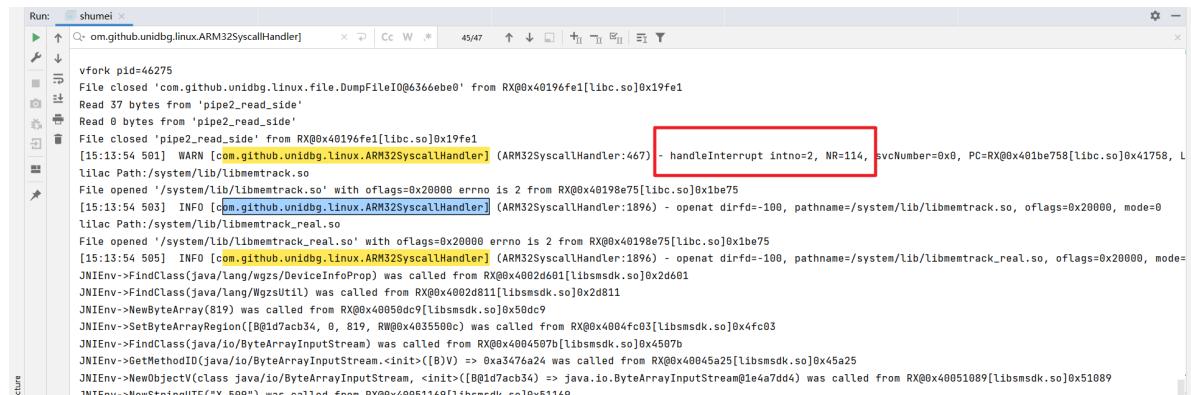


```

protected int pipe2(Emulator<?> emulator) {
    EditableArm32RegisterContext context = (EditableArm32RegisterContext) emulator.getContext();
    Pointer pipefd = context.getPointerArg(index: 0);
    int flags = context.getIntArg(index: 1);
    int write = getMinFd();
    this.fdMap.put(write, new DumpFileIO(write));
    int read = getMinFd();
    String stdout = "9ab5f193-ca2a-4d7e-8dc2-09e0ff1f257f\n";
    this.fdMap.put(read, new ByteArrayFileIO(oflags: 0, path: "pipe2_read_side", stdout.getBytes()));
    pipefd.setInt(offset: 0, read);
    pipefd.setInt(offset: 4, write);
    System.out.println("pipe2 pipefd=" + pipefd + ", flags=0x" + flags + ", read=" + read + ", write=" + write + ", stdout");
    context.setR0(0);
    return 0;
}

```

将vfork里的打印调用栈关掉，继续运行（追溯调用栈引起了报错）



```

shumei
+ om.github.unidbg.linux.ARM32SyscallHandler
  ↳ vfork pid=46275
  File closed 'com.github.unidbg.linux.file.DumpFileIO@0x196ebe0' from RX@0x40196fe1[libc.so]0x19fe1
  Read 0 bytes from 'pipe2_read_side'
  ↳ Read 0 bytes from 'pipe2_read_side'
  File closed 'pipe2_read_side' from RX@0x40196fe1[libc.so]0x19fe1
  [15:13:54 501] WARN [om.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=114, svcNumber=0x0, PC=RX@0x401be758[libc.so]0x41758, L
  lilac Path:/system/lib/libmemtrack.so
  File opened '/system/lib/libmemtrack.so' with oflags=0x20000 errno is 2 from RX@0x40198e75[libc.so]0x1be75
  [15:13:54 503] INFO [om.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/system/lib/libmemtrack.so, oflags=0x20000, mode=0
  lilac Path:/system/lib/libmemtrack_real.so
  File opened '/system/lib/libmemtrack_real.so' with oflags=0x20000 errno is 2 from RX@0x40198e75[libc.so]0x1be75
  [15:13:54 505] INFO [om.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1896) - openat dirfd=-100, pathname=/system/lib/libmemtrack_real.so, oflags=0x20000, mode=
  JNIEnv->FindClass(java/lang/NgsUtil) was called from RX@0x4002d601[libsmsdk.so]0x2d601
  JNIEnv->FindClass(java/lang/NgsUtil) was called from RX@0x4002d811[libsmsdk.so]0x2d811
  JNIEnv->NewByteArray(819) was called from RX@0x40058dc9[libsmsdk.so]0x58dc9
  JNIEnv->SetByteArrayRegion([B@1d7acb34, 0, 819, RW@0x4035500c) was called from RX@0x4004fc03[libsmsdk.so]0x4fc03
  JNIEnv->FindClass(java/io/ByteArrayInputStream) was called from RX@0x4004507b[libsmsdk.so]0x4507b
  JNIEnv->GetMethodID(java/io/ByteArrayInputStream.<init>:(B)V => 0xa3476a24 was called from RX@0x40045a25[libsmsdk.so]0x45a25
  JNIEnv->GetObjectV(class java/io/ByteArrayInputStream, <init>:([B)V => java.io.ByteArrayInputStream@1e4a7dd4) was called from RX@0x40051089[libsmsdk.so]0x51089
  JNIEnv->NewStringUTF("X..509") was called from RX@0x40051169[libsmsdk.so]0x51169

```

细心的朋友发现，这里还有一个114系统调用，查看调用表发现是wait4。Unidbg尚未实现这个系统调用？它有影响吗，这里为什么会有它？如何处理？感兴趣的可以分析一下。

我们继续往下走，补JAVA环境。

因为有JNITrace的结果，所以我们可以艺高人胆大，来看看吧

```
JNIEnv->GetStaticMethodID(JNIEnv</java/security/cert/CertificateFactory>.getInstance(Ljava/lang/String;)Ljava/security/cert/CertificateFactory;) => 0x2cba31f6 was called from RX@JNIEnv->CallStaticObjectMethod(class java/security/cert/CertificateFactory, getInstance("X.509") => java.security.cert.CertificateFactory@1cab0bf0) was called from RX@JNIEnv->GetMethodID(JNIEnv</java/security/cert/CertificateFactory>.generateCertificate(Ljava/io/InputStream;)Ljava/security/cert/Certificate;) => 0xdea2234 was called from RX@JNIEnv->GetMethodID(JNIEnv</java/security/cert/Certificate>.getPublicKey()Ljava/security/PublicKey;) => 0x74af4233 was called from RX@0x40045a25[libmsdk.so]@0x4a25 [15:27:19 769] WARN [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=-107374648, svNumber=0x115, PC=unidbg@0xffffe java.lang.UnsupportedOperationException Create breakpoint : java/security/cert/Certificate->getPublicKey()Ljava/security/PublicKey;
```

管它三七二十，就补个空的对象，只保证对象所属的类是正确的。

```
115
116
117 @Override
118 public DvmObject<?> callObjectMethodV(BaseVM vm, DvmObject<?> dvmObject, String signature, VaList vaList) {
119     switch (signature){
120         case "java/io/File->getAbsolutePath()Ljava/lang/String;":{
121             String tag = dvmObject.getValue().toString();
122             if(tag.equals("android/os/Environment->getExternalStorageDirectory()Ljava/io/File;")){
123                 return new StringObject(vm, value: "/storage/emulated/0");
124             }
125         case "java/security/cert/Certificate->getPublicKey()Ljava/security/PublicKey;":{
126             return vm.resolveClass( className: "java/security/PublicKey").newObject(signature);
127         }
128     }
129     return super.callObjectMethodV(vm, dvmObject, signature, vaList);
130 }
131
132 }
```

运行

```
JNIEnv->GetMethodID(JNIEnv</java/security/cert/Certificate>.getPublicKey()Ljava/security/PublicKey;) => 0x74af4233 was called from RX@0x40045a25[libmsdk.so]@0x51169 JNIEnv->CallObjectMethodV(JNIEnv</java/security/cert/Certificate@49e202ad, getKey() => java.security.PublicKey@1c72da34) was called from R JNIEnv->NewStringUTF("RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING") was called from RX@0x40051169[libmsdk.so]@0x51169 JNIEnv->FindClass(javax/crypto/Cipher) was called from RX@0x4004507b[libmsdk.so]@0x4507b JNIEnv->GetStaticMethodID(JNIEnv</javax/crypto/Cipher>.getInstance(Ljava/lang/String;)Ljava/crypto/Cipher;) => 0x26676b36 was called from RX@0x41 [15:33:34 178] WARN [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=-107374648, : java.lang.UnsupportedOperationException Create breakpoint : javax/crypto/Cipher->getInstance(Ljava/lang/String;)Ljava/crypto/Cipher;
at com.github.unidbg.linux.android.dvm.AbstractJni.callStaticObjectMethodV(AbstractJni.java:410)
at com.jiuwu.shumei.callStaticObjectMethodV(shumei.java:113)
at com.github.unidbg.linux.android.dvm.AbstractJni.callStaticObjectMethodV(AbstractJni.java:372)
at com.github.unidbg.linux.android.dvm.DvmMethod.callStaticObjectMethodV(DvmMethod.java:60)
at com.github.unidbg.linux.android.dvm.DalvikVM$55.handle(DalvikVM.java:1289)
at com.github.unidbg.linux.ARMSyscallHandler.hook(ARM32SyscallHandler.java:103)
at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:299)
at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
at unicorn.Unicorn.emu_start(Native Method)
at com.github.unidbg.arm.backend.UnicornBackend.emu_start(UnicornBackend.java:325)
at com.github.unidbg.AbstractEmulator.emulate(AbstractEmulator.java:379)
at com.github.unidbg.AbstractEmulator.eFunc(AbstractEmulator.java:446)
at com.github.unidbg.arm.AbstractARMEmulator.eFunc(AbstractARMEmulator.java:220)
at com.github.unidbg.Module$ModuleInfoFunction(Module.java:150)
```

获取加密类实例？照样返回一个空对象

```
104
105
106
107 @Override
108 public DvmObject<?> callStaticObjectMethodV(BaseVM vm, DvmClass dvmClass, String signature, VaList vaList) {
109     switch (signature){
110         case "android/os/Environment->getExternalStorageDirectory()Ljava/io/File;":{
111             return vm.resolveClass( className: "java/io/File").newObject(signature);
112         case "javax/crypto/Cipher->getInstance(Ljava/lang/String;)Ljava/crypto/Cipher;":{
113             return vm.resolveClass( className: "javax/crypto/Cipher").newObject(signature);
114         }
115     }
116
117     return super.callStaticObjectMethodV(vm, dvmClass, signature, vaList);
118 }
```

继续

```
0x1f765897 was called from RX@0x40045f0f[libmsdk.so]0x45f0f
JNIEnv->GetStaticFieldID([java/security/spec/MGF1ParameterSpec) was called from RX@0x4004507b[libmsdk.so]0x4507b
JNIEnv->FindClass([java/security/spec/MGF1ParameterSpec) was called from RX@0x4004507b[libmsdk.so]0x4507b
[15:38:40 677]  WARN [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=-1073746112, svcNumber=0x143
java.lang.UnsupportedOperationException Create breakpoint : java/security/spec/MGF1ParameterSpec->SHA256:Ljava/security/spec/MGF1ParameterSpec;
    at com.github.unidbg.linux.android.dvm.AbstractJni.getStaticObjectField(AbstractJni.java:83)
    at com.github.unidbg.linux.android.dvm.AbstractJni.getStaticObjectField(AbstractJni.java:45)
    at com.github.unidbg.linux.android.dvm.DvmField.getStaticObjectField(DvmField.java:39)
    at com.github.unidbg.linux.android.dvm.DalvikVM$1613)
    at com.github.unidbg.linux.ARMS32SyscallHandler.hook(ARMS32SyscallHandler.java:103)
    at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:299)
    at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
    at unicorn.Unicorn.emu_start(Native Method)
```

继续往下补两个

```
@Override
public DvmObject<?> getStaticObjectField(BaseVM vm, DvmClass dvmClass, String
signature) {
    switch (signature){
        case "java/security/spec/MGF1ParameterSpec-
>SHA256:Ljava/security/spec/MGF1ParameterSpec;":{
            return
        vm.resolveClass("java/security/spec/MGF1ParameterSpec").newObject(signature);
        }
        case "javax/crypto/spec/PSource$PSpecified-
>DEFAULT:Ljavax/crypto/spec/PSource$PSpecified;":{
            return
        vm.resolveClass("javax/crypto/spec/PSource$PSpecified").newObject(signature);
        }
    }
    return super.getStaticObjectField(vm, dvmClass, signature);
}
```

```
0x1f7651169 was called from RX@0x40051169[libmsdk.so]0x51169
JNIEnv->GetStaticObjectField(class javax/crypto/spec/PSource$PSpecified, DEFAULT Ljava/crypto/spec/PSource$PSpecified; => javax.crypto.spec.PSource$PSpecified@0xe38921c) was cal
JNIEnv->NewStringUTF("SHA-256") was called from RX@0x40051169[libmsdk.so]0x51169
JNIEnv->NewStringUTF("MGF1") was called from RX@0x40051169[libmsdk.so]0x51169
[15:38:09 923]  WARN [com.github.unidbg.linux.ARMS32SyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=-1073746124, svcNumber=0x110, PC=unidbg@0xffffe0194[lib
java.lang.UnsupportedOperationException Create breakpoint : javax/crypto/spec/AlgorithmParameterSpec-><init>(Ljava/lang/String;Ljava/lang/String;Ljava/security/spec/AlgorithmParameterSpe
    at com.github.unidbg.linux.android.dvm.AbstractJni.newObjectV(AbstractJni.java:662)
    at com.github.unidbg.linux.android.dvm.AbstractJni.newObjectV(AbstractJni.java:633)
    at com.github.unidbg.linux.android.dvm.DvmMethod.newObjectV(DvmMethod.java:199)
    at com.github.unidbg.linux.ARMS32SyscallHandler.hook(ARMS32SyscallHandler.java:103)
    at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:299)
    at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
    at unicorn.Unicorn.emu_start(Native Method)
    at com.github.unidbg.arm.backend.UnicornBackend.emu_start(UnicornBackend.java:325)
    at com.github.unidbg.AbstractEmulator.emulate(AbstractEmulator.java:370)
    at com.github.unidbg.AbstractEmulator.eFunc(AbstractEmulator.java:466)
    at com.github.unidbg.AbstractARMEmulator.eFunc(AbstractARMEmulator.java:229)
    at com.github.unidbg.Module.emulateFunction(Module.java:158)
```

一路往下

```
package com.jiuwu;

import com.github.unidbg.AndroidEmulator;
import com.github.unidbg.Emulator;
import com.github.unidbg.Module;
import com.github.unidbg.file.FileResult;
import com.github.unidbg.file.IOResolver;
import com.github.unidbg.file.linux.AndroidFileIO;
import com.github.unidbg.linux.android.AndroidARMEmulator;
import com.github.unidbg.linux.android.AndroidEmulatorBuilder;
import com.github.unidbg.linux.android.AndroidResolver;
import com.github.unidbg.linux.android.dvm.*;
import com.github.unidbg.linux.android.dvm.array.ByteArray;
```

```
import com.github.unidbg.memory.Memory;
import com.github.unidbg.memory.SvcMemory;
import com.github.unidbg.unix.UnixSyscallHandler;
import com.github.unidbg.virtualmodule.android.AndroidModule;

import javax.crypto.Cipher;
import javax.crypto.NoSuchPaddingException;
import java.io.File;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.List;

public class shumei extends AbstractJni implements IOResolver {
    private final AndroidEmulator emulator;
    private final VM vm;
    private final Module module;

    shumei() {
        // 创建模拟器实例
        //     emulator = AndroidEmulatorBuilder
        //         .for32Bit()
        //         .setRootDir(new File("target/rootfs"))
        //         .build();

        AndroidEmulatorBuilder builder = new AndroidEmulatorBuilder(false) {
            @Override
            public AndroidEmulator build() {
                return new AndroidARMEmulator(processName, rootDir,
                    backendFactories) {
                    @Override
                    protected UnixSyscallHandler<AndroidFileIO>
                    createSyscallHandler(SvcMemory svcMemory) {
                        return new MyARM32SyscallHandler(svcMemory);
                    }
                };
            }
        };

        ;
    };

    emulator = builder.setRootDir(new File("target/rootfs")).build();

    // 获取模拟器的内存操作接口
    final Memory memory = emulator.getMemory();
    // 设置系统类库解析
    memory.setLibraryResolver(new AndroidResolver(23));
    // 绑定重定向
    emulator.getSyscallHandler().addIOResolver(this);
    emulator.getSyscallHandler().setVerbose(true);

    vm = emulator.createDalvikVM(new File("unidbg-
    android/src/test/resources/shumei/com.jiuwu_1.25.0_1002500.apk"));
    new AndroidModule(emulator, vm).register(memory);
    DalvikModule dm = vm.loadLibrary(new File("unidbg-
    android/src/test/resources/shumei/libssmsdk.so"), true); // 加载so到虚拟内存
    //获取本so模块的句柄,后续需要用它
    module = dm.getModule();
    vm.setJni(this);
    vm.setVerbose(true); // 打印日志
}
```

```
        dm.callJNI_OnLoad(emulator); // 调用JNI OnLoad
    };

    @Override
    public FileResult resolve(Emulator emulator, String pathname, int oflags) {
        System.out.println("lilac Path:"+pathname);
        // 具体的处理
        return null;
    }

    public static void main(String[] args) {
        shumei demo = new shumei();
        demo.w1();
    }

    public void w1(){
        List<Object> list = new ArrayList<>(10);
        list.add(vm.getJNIEnv());
        list.add(0);
        DvmObject<?> obj =
        vm.resolveClass("android/content/Context").newObject(null);
        list.add(vm.addLocalObject(obj));
    }
}
```

```
String str2 = "
{\\"a1\\":\\"a11\\",\\"a3\\":\\"none\\",\\"a4\\":\\"4\\",\\"a2\\":\\"SRCM3hsEtSjSE1fQv1Cares092
5Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOCiXTuZJ+Va9w5pRw==\\",\\"a5\\":\\"\\",\\"a
7\\":\\"3.0.4\\",\\"a8\\":\\"\\",\\"a6\\":\\"android\\",\\"a44\\":\\"wifi\\",\\"a47\\":
[\"16, qualcomm\", \"4, qualcomm\", \"19, qualcomm\", \"19, qualcomm\", \"9, qualcomm\",
\"18, qualcomm\", \"18, qualcomm\", \"17, qualcomm\", \"22, qualcomm\", \"2, akm\", \"10, qu
alcomm\", \"20, qualcomm\", \"3, xiaomi\", \"30, qualcomm\", \"30, qualcomm\", \"33171027
,xiaomi\", \"33171027,xiaoMi\", \"33171036,xiaoMi\", \"33171036,xiaoMi\", \"11,xiaom
i\", \"5,Rohm\", \"5,Rohm\", \"6,Bosch\", \"29, qualcomm\", \"29, qualcomm\", \"1, qualco
mm\", \"35, qualcomm\", \"15, qualcomm\", \"27,xiaomi\", \"27,xiaomi\", \"33171029,xiao
Mi\", \"33171029,XiaoMi\", \"14, akm\", \"33171070,xiaomi\", \"33171070,xiaomi\", \"8,
Elliptic Labs\", \"33171031,xiaomi\"],\"a46\\":{\"cpu_abi\"::\\\"armeabi-
v7a\\\", \"serial\\\":\\\"unknown\\\", \"fingerprint\\\":\\\"Xiaomi\\\\polaris\\\\polaris:10\\\\Q
KQ1.190828.002\\\\V12.0.2.0.QDGCNXM:user\\\\release-keys\\\", \"model\\\":\\\"MIX
2S\\\", \"cpu_abi2\\\":\\\"armeabi\\\", \"brand\\\":\\\"Xiaomi\\\", \"board\\\":\\\"sdm845\\\", \"serial
_P\\\":\\\"unknown\\\", \"manufacturer\\\":\\\"Xiaomi\\\"},\"a38\\\":\\\"1.25.0\\\", \"a33\\\":\\\"ARMv8
Processor rev 13
(v81)\\\", \"a103\\\":\\\"faf6c8c7ad942343\\\", \"a23\\\":\\\"\\\", \"a54\\\":\\\"0000010\\\", \"a48\\\":5
905514496, \"a10\\\":\\\"10\\\", \"a11\\\":\\\"95fen\\\", \"a15\\\":\\\"false\\\", \"a17\\\":
[\\\"wlan1,,f460e217db64,\\\", \\\"wlan0,172.16.16.12,f460e296db64,fe80::f660:e2ff:fe96
:db64%wlan0\\\", \\\"p2p0,,f660e218db64,\\\"], \"a18\\\":
{\\\"ro.boot.hardware\\\":\\\"qcom\\\", \\\"gsm.sim.state\\\":\\\"LOADED,LOADED\\\", \\\"sys.usb.sta
te\\\":\\\"adb\\\", \\\"ro.debuggable\\\":\\\"0\\\"}, \"a19\\\":\\\"02:00:00:00:00:00\\\", \"a9\\\":16281
28282220, \"a39\\\":\\\"com.jiuwu\\\", \"a40\\\":1627972313927, \"a45\\\":\\\"46001\\\", \"a21\\\":
\\\", \"a24\\\":\\\"6d9de21492b99db9\\\", \"a25\\\":\\\"\\\", \"a22\\\":\\\"\\\", \"a34\\\":2803200, \"a37
\\\":1295, \"a27\\\":
[\\\"1628127546162,com.jiuwu,,1,1002500,1.25.0,1628127546162\\\", \\\"1230768000000,com
.android.cts.priv.ctsshim,,0,28,9-
5374186,1230768000000\\\", \\\"1230768000000,com.miui.contentextension,,0,10164,2.4.2
,1611338104848\\\", \\\"1230768000000,com.qualcomm.qti.qcolor,,0,29,10,1230768000000\\
\", \\\"1230768000000,com.android.internal.display.cutout.emulation.corner,,0,1,1.0,
1230768000000\\\", \\\"1230768000000,com.google.android.ext.services,,0,291900801,q_p
r1-
release_am1_291900801,1230768000000\\\", \\\"1230768000000,com.qualcomm.qti.improveto
uch.service,,0,29,10,1230768000000\\\", \\\"1230768000000,com.android.internal.displa
y.cutout.emulation.double,,0,1,1.0,1230768000000\\\", \\\"1230768000000,com.android.p
roviders.telephony,,0,29,10,1230768000000\\\", \\\"1230768000000,com.android.dynsyste
m,,0,29,10,1230768000000\\\"], \"a29\\\":\\\"4.0.c2.6-00335-0914_2350_3c8fca6,4.0.c2.6-
00335-0914_2350_3c8fca6\\\", \"a32\\\":8, \"a30\\\":\\\"<unknown
ssid\\\"}, \"a31\\\":\\\"172.16.16.12\\\", \"a90\\\":28, \"a105\\\":
{}, \"a108\\\":\\\"\\\", \"a109\\\":\\\"\\\", \"a110\\\":\\\"\\\", \"a111\\\":\\\"\\\", \"a107\\\":
{\\\"java\\\\lang\\\\reflect\\\\Modifier\\\":2, \\\"com\\\\android\\\\internal\\\\telephony\\\\
/PhoneProxy\\\":2, \\\"java\\\\lang\\\\ProcessBuilder\\\":2, \\\"com\\\\android\\\\internal\\\\
telephony\\\\PhoneSubInfo\\\":2, \\\"android\\\\location\\\\LocationManager\\\":2, \\\"com\\\\
tencent\\\\mapapi\\\\service\\\\LocationManager\\\":2, \\\"com\\\\android\\\\internal\\\\te
lephony\\\\gsm\\\\GSMPhone\\\":2}, \"a20\\\":\\\"\\\", \"a49\\\":\\\"\\\", \"a52\\\":
{\\\"magisk\\\":1}, \"a53\\\":{}, \"a50\\\":
{}, \"a60\\\":\\\"u0_a349\\\", \"a62\\\":\\\"\\\\data\\\\user\\\\0\\\\com.jiuwu\\\\files\\\", \"a55\\
\":\\\"a58929cd0e3202053f6137261ecd3c40\\\", \"a57\\\":1160259262, \"a36\\\":\\\"1080,2030,44
0\\\", \"a56\\\":\\\"CN=jiuwu, OU=jiuwu, O=jiuwu, L=上海, ST=上海,
C=CN\\\", \"a76\\\":\\\"\\\", \"a88\\\":\\\"locateServiceName:android.os.BinderProxy|phoneServ
iceName:android.os.BinderProxy\\\", \"a84\\\":\\\"3vDSuAiODgqAwBUsIqCEpuAFJ+xKBFFJ383k
+\\\\M2+M=____\\\", \"a68\\\":
[], \"a92\\\":\\\"1080,2030\\\", \"a93\\\":0, \"a95\\\":-1, \"a96\\\":\\\"du56APPx0pvUi
zMTZXVP\\\", \\\"a97\\\":\\\"SRCM3hsEtSjSE1fQv1Cares0925Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOC
iXTuZJ+Va9w5pRw==\\\", \"a98\\\":\\\"\\\", \"a99\\\":\\\"\\\", \"a100\\\":\\\"\\\", \"a101\\\":\\\"\\\", \"a102
\\\":[], \"a63\\\":\\\"InputMethodInfo{com.sohu.inputmethod.sogou.xiaomi\\\\.SogouIME,
settings:
```

```
com.sohu.inputmethod.sogou.SogouIMESettingsLauncher}\\"", \"InputMethodInfo{com.iflytek.inputmethod.miui\\/.FlyIME, settings:  
com.iflytek.inputmethod.LauncherSettingsActivity\"]}, \"a67\": {}, \"a64\":  
{} , \"suc\": \"1\" , \"enable\": \"0\" , \"service\": [] } , \"a65\": 39 , \"a66\":  
{} , \"a74\": 0 , \"a73\": 0 , \"a78\": [] , \"a75\": 0 , \"a77\":  
{} , \"a86\": \"1100100\" , \"a79\": \"\" , \"a80\": \"1628128282029-  
12295\" , \"a83\": \"1001100\" , \"a85\":  
[] , \"a69\": 15533490176 , \"a71\": 118982303744 , \"a72\":  
{} , \"temp\": 370 , \"vol\": 4095 , \"level\": 85 , \"scale\": 100 , \"status\": 2 } , \"a70\": 1568  
4485120 } ;
```

```
String str3 = "
{\\"all_atamper\\":true,\\"core_atamper\\":true,\\"hook_java_switch\\":true,\\"hook_switc
tch\\":false,\\"risk_apps\\": [{"\"xposed\\":
{\\"pn\\":\"de.robv.android.xposed.installer\",\"uri\\\":\"\"}, {\\"controllers\\":
{\\"pn\\":\"com.soft.controllers\",\"uri\\\":\"\"}, {\\"apk008v\\":
{\\"pn\\":\"com.soft.apk008v\",\"uri\\\":\"\"}, {\\"apk008Tool\\":
{\\"pn\\":\"com.soft.apk008Tool\",\"uri\\\":\"\"}, {\\"ig\\":
{\\"pn\\":\"com.doubee.ig\",\"uri\\\":\"\"}, {\\"anjian\\":
{\\"pn\\":\"com.cyjh.mobilejian\\\",\"uri\\\":\"\"}, {\\"rktech\\":
{\\"pn\\":\"com.ruokuai.rktech\",\"uri\\\":\"\"}, {\\"magisk\\":
{\\"pn\\":\"com.topjohnwu.magisk\",\"uri\\\":\"\"}, {\\"kinguser\\":
{\\"pn\\":\"com.kingroot.kinguser\",\"uri\\\":\"\"}, {\\"substrate\\":
{\\"pn\\":\"com.saurik.substrate\",\"uri\\\":\"\"}, {\\"touchsprite\\":
{\\"pn\\":\"com.touchsprite.android\",\"uri\\\":\"\"}, {\\"scriptdroid\\":
{\\"pn\\":\"com.stardust.scriptdroid\",\"uri\\\":\"\"}, {\\"toolhero\\":
{\\"pn\\":\"com.mobileuncle.toolhero\",\"uri\\\":\"\"}, {\\"huluxia\\":
{\\"pn\\":\"com.huluxia.gametools\",\"uri\\\":\"\"}, {\\"apkeditor\\":
{\\"pn\\":\"com.gmail.heagoo.apkeditor.pro\",\"uri\\\":\"\"}, {\\"xposeddev\\":
{\\"pn\\":\"com.sollyu.xposed.hook.model.dev\",\"uri\\\":\"\"}, {\\"anywhere\\":
{\\"pn\\":\"com.txy.anywhere\",\"uri\\\":\"\"}, {\\"burgerzws\\":
{\\"pn\\":\"pro.burgerz.wsm.manager\",\"uri\\\":\"\"}, {\\"vdloc\\":
{\\"pn\\":\"com.virtualdroid.loc\",\"uri\\\":\"\"}, {\\"vdtxl\\":
{\\"pn\\":\"com.virtualdroid.txl\",\"uri\\\":\"\"}, {\\"vdwzs\\":
{\\"pn\\":\"com.virtualdroid.wzs\",\"uri\\\":\"\"}, {\\"vdkit\\":
{\\"pn\\":\"com.virtualdroid.kit\",\"uri\\\":\"\"}, {\\"vdwxg\\":
{\\"pn\\":\"com.virtualdroid.wxg\",\"uri\\\":\"\"}, {\\"vdgps\\":
{\\"pn\\":\"com.virtualdroid.gps\",\"uri\\\":\"\"}, {\\"a1024mlloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\"}, {\\"drhgz\\":
{\\"pn\\":\"com.deruhai.guangzi.noroot2\",\"uri\\\":\"\"}, {\\"yggb\\":
{\\"pn\\":\"com.mcmonjmb.yggb\",\"uri\\\":\"\"}, {\\"xsrv\\":
{\\"pn\\":\"xiake.xserver\",\"uri\\\":\"\"}, {\\"fakeloc\\":
{\\"pn\\":\"com.dracrays.fakeloc\",\"uri\\\":\"\"}, {\\"ultra\\":
{\\"pn\\":\"net.anylocation.ultra\",\"uri\\\":\"\"}, {\\"locationcheater\\":
{\\"pn\\":\"com.wifi99.android.locationcheater\",\"uri\\\":\"\"}, {\\"dwzs\\":
{\\"pn\\":\"com.dingweizshou\",\"uri\\\":\"\"}, {\\"mockloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\"}, {\\"anywhereclone\\":
{\\"pn\\":\"com.txy.anywhere.clone\",\"uri\\\":\"\"}, {\\"fakelocc\\":
{\\"pn\\":\"com.dracrays.fakelocc\",\"uri\\\":\"\"}, {\\"mockwxlocation\\":
{\\"pn\\":\"com.tandy.android.mockwxlocation\",\"uri\\\":\"\"}, {\\"anylocation\\":
{\\"pn\\":\"net.anylocation\",\"uri\\\":\"\"}, {\\"totalcontrol\\":
{\\"pn\\":\"com.sigma_rt.totalcontrol\",\"uri\\\":\"\"}, {\\"ipjl2\\":
{\\"pn\\":\"com.chuangdian.ipjl2\",\"uri\\\":\"\"}], {\\"risk_dirs\\": [{"\"008Mode\\":
{\\"dir\\":\".system/008Mode\", \"type\\\":\"sdcard\"}, {\\"008OK\\":
{\\"dir\\":\".system/008OK\", \"type\\\":\"sdcard\"}, {\\"008system\\":
{\\"dir\\":\".system/008system\", \"type\\\":\"sdcard\"}, {\\"iGrimace\\":
{\\"dir\\":\"iGrimace\", \"type\\\":\"sdcard\"}, {\\"touchelper\\":
{\\"dir\\\":\"/data/data/net.aisence.Touchelper\", \"type\\\":\"absolute\"}, {\\"elfscript\\":
{\\"dir\\\":\"/mnt/sdcard/touchelf/scripts/\", \"type\\\":\"absolute\"}, {\\"spritelua\\": {\\"dir\\\":\"/mnt/sdcard/TouchSprite/lua\", \"type\\\":\"absolute\"}, {\\"spritelog\\": {\\"dir\\\":\"/mnt/sdcard/TouchSprite/log\", \"type\\\":\"absolute\"}, {\\"assistant\\": {\\"dir\\\":\"/data/data/com.xxAssistant\", \"type\\\":\"absolute\"}, {\\"assistantscript\\":
{\\"dir\\\":\"/mnt/sdcard/com.xxAssistant/script\", \"type\\\":\"absolute\"}, {\\"mobilejian\\":
{\\"dir\\\":\"/data/data/com.cyjh.mobilejian\", \"type\\\":\"absolute\"}], {\\"risk_file_switch\\": true, {\\"risk_files\\": \"zb5E/i2Gv4IxR50xSBiXKChu8gdkDXKei9GwOBNbN6jq3xMULFFAvT94C0wwwhychgUgggyBRjbNG1gz0dh171P0b7ZnqdDPKYq5NrmMJr3Fwtzccme/nv4R00yuTb

```

f1jc3DdFuA8eOMaLkvLFfsnx13Jdu6ZY38LTdbc+h2fnf4KnSRbgcZ5JVfaeiKz5HFQvKzjKJH6x/uQ  
i190PF2kpg4uRmTDh6ev0En0RGh9Jg318Nr0xd87izNvUg5Jg941Q/FX98DYetR2RYe3Sp/9u+cT1EnE  
SikjyMxGjaJ3R1TQ701LfuNwqceVsYw99YeNkCwwTBMQII5a3/2i09HzxRXXiswvk23Txt41xmumhs5  
HDmj6D1/oeQ6oFHqsfd3c/auB0vFrqrqbNH68H9pw/b2wpYnnAJsgYxowaz1MaQj5Y21IGkzz7jSeTN2  
IJFTzPSheHC2K4QS7OSWju/d1rCrA5BXSn05TIGXNukm2AwPEtduBeg4FpR7Lb/Vi0K0cgry4gVRPV1  
QnNBBr5mjI2fs30C1sdzbJG2sZxo56BxeF8HzXDpbro3T+Nqg77E4cynk9a57kkqoeA1RaZn8yHJws4q  
97tFrusokRbcFwmVkyeJ5z1rbwLevZ9fkTcyy3VIQY3E2mwR7kaAJepds1+iDeJBHZwBKUBPJqoPoiE0  
uKTnn8KmvyKjb+Jc8mYXR/mgT1r0c6Cgn6CM9BfynzrJoyTmlXzy2tm6dn66eHM5tsplzG0c3JEgvB2T  
5nSyAc9X0u9/rIbsWQ/8OUNFz2pu7vbfgyswakkPKMbksj3MsRHHE6mljv/P0rEtunth5/KwH1JQBWW  
R/1epqywjoev2fiJ5FqGTvbt6ZTESeAx+9AIUhv9nMx32svw0VmIIjv6R8UUoa1b5EZHYcm804BEszx2  
/ke/e+1dEvw5ntT0khvme5HIX9Qn0uz6u+gQpJds2aVHMGOXI670xhepwaMskl1tu268x53PYc+rjx  
NXNbKGGD+kJAISPF4d2u0tbVNf57cy1sIF4HK8+7FPxn6gqd4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc  
sWSmmWIQQZE9rIoUbxSFLThQMUW2tI0GFHCJVsppIQtmxx6M9bTuerjd0Ii5oamMswxK3MkAyM1581u  
d05x4ycwfouRXOoxerpjvEmT4jfJJRh86ud/Ecihm6Fp5dm8r4Hg9nPQKebng/Gjl1+/n0S0dpaq/4rQ  
vIk2GWN7Q/M7BboqN7+5ou4qkcyOHaGC8H9OYpwrlhzB/IEYhgBVCePKW6bGkiPBReu72+Bmhgb5KaPN  
JYLFWcdnsN9+df7DcvpVcmntsM56HnKLym168o8XHJIhawjajkElhsqy1s0FOOu1EcN90coIPi7XQFI  
Q2jk7A1qits1bKhtp0m49jcsomHBwqqt5kNno6WF6xiNXODhIZ3diLHXHe1kfWPjpnPZzq2FugBvj0Tx  
+tftPYoGwiJvlu4SBeGez4jcfi2qkCofJm7EeMojox6BuBF3HKjUV+bugusy5BF8qFhb1azop/0++qHt  
BtGkQejeqESFZWWxjhhsrHja68rPa0YDxxCl1tH4xS+38tFWKqgbKovck+2udz1auCSA0etjqfzz70fj  
C4hwJp8wCDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiV06e70sayn1kppG1RW1UmGhLe5g08WDB  
IO1MGfSJMFfn1gt90nJxpWQoymcUM6tuAKSoim0aExqsvK+SIHI/dchN6tiFaHLzesXhqxaHpbixVqDa  
D8gHN/yMR4IEY8e0ohVLwPAFZIWuGPdz3bgqQBmerdLp1ZhrZcjWLsoaskyDWW0G0RjkP/Yswk+s1dLe  
wadQpFAtt6x7c5DnkdmvmsxxF7a3fG7G0Tk8miLwSmpgIij80w/oLCbUgYDGEpjGiSG6XEHPktc6ThTs  
+Czc2QNgBi15g12NABEHQKxc3tzykwspoaamWrDe8vNCuKd+Tkk+q0zw66LTmE+maWX56TAQY50MQXOr  
H+6c5iULwda9Qn6rDSVNpTAn6KU6duxDb23QYthbd2orBq6T0Z8NLC8h6QwVA9QEG7zs9j/fz/st94xi  
tuk8jkvr131f6bD646ixTx27NzzoQEt2E1s/ZM/iaAxwlaohOKKO5adtDATLyL7Ia1vdwdqz0XGwzus  
IKUjxDIrB0JzgCuGwg2Cj5cRL059Kfs0hgYv8rRgTa41vJcvuhEi6VtpFbGwv+T0C7Zx3xNPmnAVDwth  
UDPKu36z2wzzp89p6qrw7k0UwnN7XiGaV5Lv1Hcih7FnwLe107Mdvg41TprLFMLTwccwjhLf5mrIh6et  
Y5Zqp5ikVKv4vrb0s0SqqFLbz0Zj4KshyT2Yzaz7ZK5uQRF2f2u8gPYwn0oF4C8rNbbkdxAzoierX/s7m  
01AMD0Bjss1Lgc180v1jCns5u2drqQm1rkTG5r1k0140fTkoKnjyj90zxrD7/khxs6+pWv6v3CzcdR8  
ojX+7MqmZxVEsdceHzE7gCfR17kb1H8bTzhaQPqh09vDLAo8RjtD2HHjYt2Qvjing8PtX57+/TBuIVPD  
wog6p8mi1hqzlhouzVpbhdruYqlhh45sbT99ydfs2j6/zovv84c8sE1bq//zh3jku74boayGDzKjsr8u  
NbDZ5sP4DMFg/Zxqnku0nSjjv1P/DU1mfDZA+kzn8Iad/5sdedyjmPb2yIag0uEjvjt0qz6FeoT2h7m  
MVLwBCMy12Wk+0tTXL2xEpA63Y7Mfxymj8R2Deax6WRz96IoT10Gr8+11Tsav16EHHanMJdy94Es+s+x  
00yvJnRybbNn1qvqu4FcE+16EeDiojoqbaczz0Ys6zkpcyIdrlmibdxjcdxq1Zcw9FQXXNrERkfoK9PE  
DmHJQ8y2hJTTyqaSVqu7imgbOPR1GBV4Eu2/r1euLftwR1mZc6cfqrre9Y0GazGsnHyYh6oK135Z1bsX  
uNaGogr/ow32s5xuaq6o26hdxdFvbwn7j30yvJ30rHEOGArj95DFnx2IURvMgYRrmUgwdCvmiNTLqZxf  
sbfbmB2kUWGKp2mwa5RwrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8Ypgbs6Khh1jwvwTr7ah  
occhi1aa/9y53xuoB9cDrqbm08rj+4VFbyxkFMchY6rhoY23ok1ystqxxvdf5FjzndbHCenvmkz8Thju  
uSP3VOuVrUHAZssuyiqocQhr8gxPsc6k4XDzohrp+Yfzq5YbLT0nv4+FmTIJ8Jwzy5axUG2oACiL8Lny  
pQ1qmTCBixpjFM5iQKPSVdkC0TmZ8b0T+UQLa2Yoxn5Thr0ktaTTN3GkeWq2DlmFkt0FCQcbjIawxy75  
RtuitkcooctFQ3xUNH7s/royb/sx1v+8ebi6L59L3x2PCvqoEXn9gsirr241oyxitrxsE1zaavrU9Y  
Zcb+a49A602Nrywn81dRPb5t02mUQRp/Kg1IJPSr5tcc36yGVYwmvCnouqmrgeNQT5QUBH7LEmQWdnI  
S+Djqn9pbhb8wroyxOFF8aehwul02hsgw91Rwz9umAfjEC4sSt8sc1ELaqaqwKnooKg7sevLq25b6toF  
ARwgdd8yTXH70jPniFuF+UE143yk912LwxFM/squ/UZP97RqbwuPu+bv2bYe3hiqbkj5xv5IOxgs6H3F  
u1lp2zyGwHGrxwoaqz+4/npkuJ7ILAV7y1g8s0zWfc86hPyRirv2Lna3gr0bnNUOCsfpcRwdkmBlyhn  
1bGqoj0iurBkjUbYPQ4G8jzoquJmQ5xNyH60AQb0u7LdEDiC0HSUSI3SKzo1uESNSeE3qfv+UF87kzt  
eLj+RaqhAGN9nxstGn9F3yIUb76j13STbwwdEUzb7x8mhij9gQVLNFBR2tgrY=\", \"sensitive.ain  
fo\": true, \"sensitive.apps\": true, \"sensitive.aps\": true, \"sensitive.bssid\": tru  
e, \"sensitive.camera\": true, \"sensitive.cell\": true, \"sensitive.gps\": false, \"se  
nsitive.iccid\": true, \"sensitive.imsi\": true, \"sensitive.mac\": true, \"sensitive.  
ssid\": true, \"sensitive.tel\": false, \"white\_apps\": []}";

```

        String str4 =
    "MIIDLZCCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAYMQSwCQYDVQQGEWJDTjELMAKGA1UECwwCU00
    xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNNDAxMjAyMDMzMDE4WjAyMQs
    WCQYDVQQGEWJDTjELMAKGA1UECwwCU00xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wggEiMA0GCSqGSIb
    3DQEBAQUAA4IBDWAwggEKAoIBAQCT947yNGA4EPVheGp6hsDoU4KBKvmwacn6tqfwit/jlxazzBSPcw4
    3jjxGuF4exM4NPJJtMft/j0IIwJeEx0YHDCJIqu/1pEPsXYb01bhwd5mq34c0RiRx1ji+g+d4rFRO/Xr
    eFRJSeB3w1djvoAMkxoygp+813zM6mzPd36zjbUIajfzkc5LoeITUCC6Db98XiN/hNmvcIwti01Sm9FE
    U1ip1fFb9NZ04vb2Z6xt/ti/rUVzWyshZC1qqVq4s9W4iGPqfTnBsxttiooRUpoe2LtB+J73kKTgJJH
    60pn0ljqd+FaMsL/sdy61ggM+w4ePTe4HF+/dv2ZZp+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
    ZA5/0RAVrhWrYFlnyrex4FjAfBgNVHSMEGDAwgbS83RQZA5/0RAVrhWrYFlnyrex4FjAMBgNVHRMEBT
    DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZo6fn+mH124C8Djm15jCRjYqOISpgk
    gsReEX2F00sxYqBuRPidycdsRNYQG44/i4PQrbwc9T/wLSOyHICaKbXXPhfw14PLRNR0LtgmcLoIveDy
    jzTn3BEF57tZCYSmphMUI0eJeV9o3yh1uURV3vbigh+0ca2Mql9m7N49dkkgeZ04FAWUp9yG+p1jf5tA
    Iwa6t1vvH1T8TKwjGtBH3jvYenKBk+W+DWZnDepg01+8Xozo0JP5u1u68sqf+cke0Bw1RfsTFU4ya
    OEBSIIZ/Stx7Q82K8M4xucAFV8PTT8i30QoGcsduEj4zape1vnNn7f";
        String str5 = "du56APPx0pvUizMTZXVP";
        String str6 = "95fen";
        list.add(vm.addLocalObject(new StringObject(vm,str2)));
        list.add(vm.addLocalObject(new StringObject(vm,str3)));
        list.add(vm.addLocalObject(new StringObject(vm,str4)));
        list.add(vm.addLocalObject(new StringObject(vm,str5)));
        list.add(vm.addLocalObject(new StringObject(vm,str6)));
        Number number = module.callFunction(emulator,0x16f1d,list.toArray())[0];
        String result = vm.getObject(number.intValue()).getValue().toString();
        System.out.println(result);
    }
}

```

```

@Override
public DvmObject<?> callStaticObjectMethodV(BaseVM vm, DvmClass dvmClass,
String signature, VaList vaList) {
    switch (signature){
        case "android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;":{
            return vm.resolveClass("java/io/File").newObject(signature);
        }
        case "javax/crypto/Cipher-
>getInstance(Ljava/lang/String;)Ljava/crypto/Cipher;":{
            return
vm.resolveClass("javax/crypto/Cipher").newObject(signature);
        }
    }
    return super.callStaticObjectMethodV(vm, dvmClass, signature, vaList);
}

@Override
public DvmObject<?> callObjectMethodV(BaseVM vm, DvmObject<?> dvmObject,
String signature, VaList vaList) {
    switch (signature){
        case "java/io/File->getAbsolutePath()Ljava/lang/String;":{
            String tag = dvmObject.getValue().toString();
            if(tag.equals("android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;")){
                return new StringObject(vm, "/storage/emulated/0");
            }
        }
        case "java/security/cert/Certificate-
>getPublicKey()Ljava/security/PublicKey;":{

```

```

        return
    vm.resolveClass("java/security/PublicKey").newObject(signature);
    }

}

return super.callObjectMethodV(vm, dvmObject, signature, vaList);
}

@Override
public DvmObject<?> getStaticObjectField(BaseVM vm, DvmClass dvmClass,
String signature) {
    switch (signature){
        case "java/security/spec/MGF1ParameterSpec-
>SHA256:Ljava/security/spec/MGF1ParameterSpec;":{
            return
    vm.resolveClass("java/security/spec/MGF1ParameterSpec").newObject(signature);
        }
        case "javax/crypto/spec/PSource$PSpecified-
>DEFAULT:Ljavax/crypto/spec/PSource$PSpecified;":{
            return
    vm.resolveClass("javax/crypto/spec/PSource$PSpecified").newObject(signature);
        }
    }
    return super.getStaticObjectField(vm, dvmClass, signature);
}

@Override
public DvmObject<?> newObjectV(BaseVM vm, DvmClass dvmClass, String
signature, VaList vaList) {
    switch (signature){
        case "javax/crypto/spec/OAEPPParameterSpec-><init>
(Ljava/lang/String;Ljava/lang/String;Ljava/security/spec/AlgorithmParameterSpec;
Ljavax/crypto/spec/PSource;)V":{
            return
    vm.resolveClass("javax/crypto/spec/OAEPPParameterSpec").newObject(signature);
        }
    }
    return super.newObjectV(vm, dvmClass, signature, vaList);
}

@Override
public void callVoidMethodV(BaseVM vm, DvmObject<?> dvmObject, String
signature, VaList vaList) {
    switch (signature){
        case "javax/crypto/Cipher-
>init(ILjava/security/Key;Ljava/security/spec/AlgorithmParameterSpec;)V":{
            vm.resolveClass("javax/crypto/Cipher").newObject(signature);
            return;
        }
    }
    super.callVoidMethodV(vm, dvmObject, signature, vaList);
}

}

```

运行

```

Run: shumei
JNIEnv->CallVoidMethodV(javacrypto.Cipher@$d5tcd8, init@xi, java.security.PublicKey@lc@2da34, javax.crypto.spec.UAEPParameterSpec@6385cb26jj)
JNIEnv->NewByteArray(16) was called from RX@0x40050dc9[libmsdk.so]@0x50dc9
JNIEnv->SetByteArrayRegion([B@28c471c, 0, 16, RW@0x402d22ec] was called from RX@0x40051de5[libmsdk.so]@0x51de5
JNIEnv->GetMethodID(javacrypto.Cipher.doFinal([B][B] => 0x15ab3b was called from RX@0x40045a25[libmsdk.so]@0x45a25
[15:43:10 571] [WARN] [com.github.unidbg.linux.ARMSyscallHandler] (ARM32SyscallHandler:467) - handleInterrupt intno=2, NR=-1073746120, svcNumber=java.lang.UnsupportedOperationException Create breakpoint: javax/crypto/Cipher->doFinal([B][B]
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethodV(AbstractJni.java:557)
    at com.jiuwu.shumei.callObjectMethodV(shumei.java:133)
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethodV(AbstractJni.java:224)
    at com.github.unidbg.linux.android.dvm.DvmMethod.callObjectMethodV(DvmMethod.java:85)
    at com.github.unidbg.linux.android.dvm.DalvikVM$22.handle(DalvikVM.java:434)
    at com.github.unidbg.linux.android.dvm.ARMSyscallHandler.hook(ARMSyscallHandler.java:103)
    at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:299)
    at unicorn.Unicorn$NewHook.onInterrupt(Unicorn.java:128)
    at unicorn.Unicorn.emu_start(Native Method)
    at com.github.unidbg.arm.backend.UnicornBackend.emu_start(UnicornBackend.java:325)
    at com.github.unidbg.AbstractEmulator.emulate(AbstractEmulator.java:370)
    at com.github.unidbg.AbstractEmulator.eFunc(AbstractEmulator.java:446)
    at com.github.unidbg.arm.AbstractARMEmulator.eFunc(AbstractARMEmulator.java:220)
    at com.github.unidbg.Module.emulateFunction(Module.java:158)
    at com.github.unidbg.linux.LinuxModule.callFunction(LinuxModule.java:232)
    at com.jiuwu.shumei.w1(shumei.java:100)

```

终于等到它了， doFinal最终返回了一个byte数组，这里我们不得不补了，因为这里返回了切切实实的数据。

在JNitrace中查看dofinal应该返回的结果

```

iqiyijnitrace2.txt jd\jnitrace1.txt smsdk\jnitrace1.txt lazada\jnitrace1.txt record.txt dy\jnitrace2.txt hookdlopen.
Q /* TID 14857 */ Cc W * 104/197 ↑ ↓ □ + - II E I T
1197 4153 ms |-> 0xb1eb177d: libmsdk.so!0x5377d (libmsdk.so:0xb1e5e000)
1198
1199
1200     /* TID 14857 */
1201 4170 ms [*] JNIEnv->GetByteArrayRegion
1202 4170 ms |- JNIEnv* : 0xba872620
1203 4170 ms |- jbyteArray : 0x109
1204 4170 ms |- jsize : 0
1205 4170 ms |- jsize : 256
1206 4170 ms |- jbyte* : 0xb30d1100
1207 4170 ms |: 0000000: 10 06 7A D9 10 2B 18 78 3B C3 24 2D 4A 37 81 C1 ...z..+x;.-J7..
1208 4170 ms |: 0000010: 58 22 B0 E8 09 8B 89 56 FF F2 07 EC 8B 04 74 6E X".....V.....tn
1209 4170 ms |: 0000020: 15 30 7D 3B 61 5B EE 9D B1 88 B4 10 2D 7C 10 2B .0};a[.....-].+
1210 4170 ms |: 0000030: EC F6 99 0A FC 95 46 4A A9 87 B6 C8 37 07 AF 8E .....FJ....7...
1211 4170 ms |: 0000040: 95 F3 13 7D B4 6D B9 00 CD 5C A6 8F D5 B8 1F AD ...}.m...\......
1212 4170 ms |: 0000050: 06 23 95 0A 24 B4 2E 39 DF 03 18 49 E8 13 0D 33 .#.$.9...I...3
1213 4170 ms |: 0000060: A2 6E 0D B6 37 FF 5F E7 F1 4F 3B 52 7F 7B 2D D3 .n..7...0;R.{-
1214 4170 ms |: 0000070: F2 FC 8F 2F DB AD AD 2C A2 D0 32 7F 0E 10 BF B7 .../....2.....
1215 4170 ms |: 0000080: 14 4E 8B 7B C4 0D 7C 58 20 C9 93 FA 17 C1 39 99 .N.{..|X ....9.
1216 4170 ms |: 0000090: 59 46 B2 F1 40 2E 52 9C E7 B4 80 3F 78 F6 02 6C YF..@.R....?x..l
1217 4170 ms |: 00000A0: B7 80 F9 A0 52 A0 DD D5 71 A1 AC 13 B0 6B 27 B4 ...R...q....k'.
1218 4170 ms |: 00000B0: AD 14 32 CE 99 EF B9 33 66 DE E4 A6 7D CC F3 02 ..2....3f...}...
1219 4170 ms |: 00000C0: A6 12 F9 02 A0 3E 06 EB E1 BA 6E B8 E8 44 79 CD .....>....n..Dy.
1220 4170 ms |: 00000D0: A2 2D 6A D9 28 34 C4 DB 0B 6A A0 CC EA 8A 5F D0 .-j.(4...j.....
1221 4170 ms |: 00000E0: FC 46 6F E5 95 B3 DC 60 38 D9 97 5B B7 AB 6E 5D .Fo....`8..[..n]
1222 4170 ms |: 00000F0: F7 84 0A 33 0C F5 72 F2 AB 32 07 B2 5F 32 70 CD ...3..r...2.._2p.
1223
1224 4170 ms -----Backtrace-----
1225 4170 ms |-> 0xb1eb0407: libmsdk.so!0x52407 (libmsdk.so:0xb1e5e000)

```

hexdump复制到CyberChef中转成hex string，然后此处补上去。

```

package com.jiuwu;

import com.github.unidbg.AndroidEmulator;
import com.github.unidbg.Emulator;
import com.github.unidbg.Module;
import com.github.unidbg.file.FileResult;
import com.github.unidbg.file.IOResolver;
import com.github.unidbg.file.linux.AndroidFileIO;
import com.github.unidbg.linux.android.AndroidARMEmulator;
import com.github.unidbg.linux.android.AndroidEmulatorBuilder;
import com.github.unidbg.linux.android.AndroidResolver;
import com.github.unidbg.linux.android.dvm.*;
import com.github.unidbg.linux.android.dvm.array.ByteArray;

```

```
import com.github.unidbg.memory.Memory;
import com.github.unidbg.memory.SvcMemory;
import com.github.unidbg.unix.UnixSyscallHandler;
import com.github.unidbg.virtualmodule.android.AndroidModule;

import javax.crypto.Cipher;
import javax.crypto.NoSuchPaddingException;
import java.io.File;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.List;

public class shumei extends AbstractJni implements IOResolver {
    private final AndroidEmulator emulator;
    private final VM vm;
    private final Module module;

    shumei() {
        // 创建模拟器实例
        //     emulator = AndroidEmulatorBuilder
        //         .for32Bit()
        //         .setRootDir(new File("target/rootfs"))
        //         .build();

        AndroidEmulatorBuilder builder = new AndroidEmulatorBuilder(false) {
            @Override
            public AndroidEmulator build() {
                return new AndroidARMEmulator(processName, rootDir,
                    backendFactories) {
                    @Override
                    protected UnixSyscallHandler<AndroidFileIO>
                    createSyscallHandler(SvcMemory svcMemory) {
                        return new MyARM32SyscallHandler(svcMemory);
                    }
                };
            }
        };

        ;
    };

    emulator = builder.setRootDir(new File("target/rootfs")).build();

    // 获取模拟器的内存操作接口
    final Memory memory = emulator.getMemory();
    // 设置系统类库解析
    memory.setLibraryResolver(new AndroidResolver(23));
    // 绑定重定向
    emulator.getSyscallHandler().addIOResolver(this);
    emulator.getSyscallHandler().setVerbose(true);

    vm = emulator.createDalvikVM(new File("unidbg-
    android/src/test/resources/shumei/com.jiuwu_1.25.0_1002500.apk"));
    new AndroidModule(emulator, vm).register(memory);
    DalvikModule dm = vm.loadLibrary(new File("unidbg-
    android/src/test/resources/shumei/libssmsdk.so"), true); // 加载so到虚拟内存
    //获取本so模块的句柄,后续需要用它
    module = dm.getModule();
    vm.setJni(this);
    vm.setVerbose(true); // 打印日志
}
```

```
        dm.callJNI_OnLoad(emulator); // 调用JNI OnLoad
    };

    @Override
    public FileResult resolve(Emulator emulator, String pathname, int oflags) {
        System.out.println("lilac Path:"+pathname);
        // 具体的处理
        return null;
    }

    public static void main(String[] args) {
        shumei demo = new shumei();
        demo.w1();
    }

    public void w1(){
        List<Object> list = new ArrayList<>(10);
        list.add(vm.getJNIEnv());
        list.add(0);
        DvmObject<?> obj =
        vm.resolveClass("android/content/Context").newObject(null);
        list.add(vm.addLocalObject(obj));
    }
}
```

```
String str2 = "
{\\"a1\\":\\"a11\\",\\"a3\\":\\"none\\",\\"a4\\":\\"4\\",\\"a2\\":\\"SRCM3hsEtSjSE1fQv1Cares092
5Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOCiXTuZJ+Va9w5pRw==\\",\\"a5\\":\\"\\",\\"a
7\\":\\"3.0.4\\",\\"a8\\":\\"\\",\\"a6\\":\\"android\\",\\"a44\\":\\"wifi\\",\\"a47\\":
[\"16, qualcomm\", \"4, qualcomm\", \"19, qualcomm\", \"19, qualcomm\", \"9, qualcomm\",
\"18, qualcomm\", \"18, qualcomm\", \"17, qualcomm\", \"22, qualcomm\", \"2, akm\", \"10, qu
alcomm\", \"20, qualcomm\", \"3, xiaomi\", \"30, qualcomm\", \"30, qualcomm\", \"33171027
,xiaomi\", \"33171027,xiaoMi\", \"33171036,xiaoMi\", \"33171036,xiaoMi\", \"11,xiaom
i\", \"5,Rohm\", \"5,Rohm\", \"6,Bosch\", \"29, qualcomm\", \"29, qualcomm\", \"1, qualco
mm\", \"35, qualcomm\", \"15, qualcomm\", \"27,xiaomi\", \"27,xiaomi\", \"33171029,xiao
Mi\", \"33171029,XiaoMi\", \"14, akm\", \"33171070,xiaomi\", \"33171070,xiaomi\", \"8,
Elliptic Labs\", \"33171031,xiaomi\"],\"a46\\":{\"cpu_abi\"::\\\"armeabi-
v7a\\\", \"serial\\\":\\\"unknown\\\", \"fingerprint\\\":\\\"Xiaomi\\\\polaris\\\\polaris:10\\\\Q
KQ1.190828.002\\\\V12.0.2.0.QDGCNXM:user\\\\release-keys\\\", \"model\\\":\\\"MIX
2S\\\", \"cpu_abi2\\\":\\\"armeabi\\\", \"brand\\\":\\\"Xiaomi\\\", \"board\\\":\\\"sdm845\\\", \"serial
_P\\\":\\\"unknown\\\", \"manufacturer\\\":\\\"Xiaomi\\\"},\"a38\\\":\\\"1.25.0\\\", \"a33\\\":\\\"ARMv8
Processor rev 13
(v81)\\\", \"a103\\\":\\\"faf6c8c7ad942343\\\", \"a23\\\":\\\"\\\", \"a54\\\":\\\"0000010\\\", \"a48\\\":5
905514496, \"a10\\\":\\\"10\\\", \"a11\\\":\\\"95fen\\\", \"a15\\\":\\\"false\\\", \"a17\\\":
[\\\"wlan1,,f460e217db64,\\\", \\\"wlan0,172.16.16.12,f460e296db64,fe80::f660:e2ff:fe96
:db64%wlan0\\\", \\\"p2p0,,f660e218db64,\\\"], \"a18\\\":
{\\\"ro.boot.hardware\\\":\\\"qcom\\\", \\\"gsm.sim.state\\\":\\\"LOADED,LOADED\\\", \\\"sys.usb.sta
te\\\":\\\"adb\\\", \\\"ro.debuggable\\\":\\\"0\\\"}, \"a19\\\":\\\"02:00:00:00:00:00\\\", \"a9\\\":16281
28282220, \"a39\\\":\\\"com.jiuwu\\\", \"a40\\\":1627972313927, \"a45\\\":\\\"46001\\\", \"a21\\\":
\\\", \"a24\\\":\\\"6d9de21492b99db9\\\", \"a25\\\":\\\"\\\", \"a22\\\":\\\"\\\", \"a34\\\":2803200, \"a37
\\\":1295, \"a27\\\":
[\\\"1628127546162,com.jiuwu,,1,1002500,1.25.0,1628127546162\\\", \\\"1230768000000,com
.android.cts.priv.ctsshim,,0,28,9-
5374186,1230768000000\\\", \\\"1230768000000,com.miui.contentextension,,0,10164,2.4.2
,1611338104848\\\", \\\"1230768000000,com.qualcomm.qti.qcolor,,0,29,10,1230768000000\\
\", \\\"1230768000000,com.android.internal.display.cutout.emulation.corner,,0,1,1.0,
1230768000000\\\", \\\"1230768000000,com.google.android.ext.services,,0,291900801,q_p
r1-
release_am1_291900801,1230768000000\\\", \\\"1230768000000,com.qualcomm.qti.improveto
uch.service,,0,29,10,1230768000000\\\", \\\"1230768000000,com.android.internal.displa
y.cutout.emulation.double,,0,1,1.0,1230768000000\\\", \\\"1230768000000,com.android.p
roviders.telephony,,0,29,10,1230768000000\\\", \\\"1230768000000,com.android.dynsyste
m,,0,29,10,1230768000000\\\"], \"a29\\\":\\\"4.0.c2.6-00335-0914_2350_3c8fca6,4.0.c2.6-
00335-0914_2350_3c8fca6\\\", \"a32\\\":8, \"a30\\\":\\\"<unknown
ssid>\\\", \"a31\\\":\\\"172.16.16.12\\\", \"a90\\\":28, \"a105\\\":
{}, \"a108\\\":\\\"\\\", \"a109\\\":\\\"\\\", \"a110\\\":\\\"\\\", \"a111\\\":\\\"\\\", \"a107\\\":
{\\\"java\\\\\\lang\\\\\\reflect\\\\\\Modifier\\\":2, \\\"com\\\\\\android\\\\\\internal\\\\\\telephony\\\\
\\PhoneProxy\\\":2, \\\"java\\\\\\lang\\\\\\ProcessBuilder\\\":2, \\\"com\\\\\\android\\\\\\internal\\\\\\
telephony\\\\\\PhoneSubInfo\\\":2, \\\"android\\\\\\location\\\\\\LocationManager\\\":2, \\\"com\\\\\\
tencent\\\\\\mapapi\\\\\\service\\\\\\LocationManager\\\":2, \\\"com\\\\\\android\\\\\\internal\\\\\\te
lephony\\\\\\gsm\\\\\\GSMPhone\\\":2}, \\\"a20\\\":\\\"\\\", \"a49\\\":\\\"\\\", \"a52\\\":
{\\\"magisk\\\":1}, \"a53\\\":{}, \"a50\\\":
{}, \"a60\\\":\\\"u0_a349\\\", \"a62\\\":\\\"\\\\\\data\\\\\\user\\\\\\0\\\\\\com.jiuwu\\\\\\files\\\", \"a55
\\\":\\\"a58929cd0e3202053f6137261ecd3c40\\\", \"a57\\\":1160259262, \"a36\\\":\\\"1080,2030,44
0\\\", \"a56\\\":\\\"CN=jiuwu, OU=jiuwu, O=jiuwu, L=上海, ST=上海,
C=CN\\\", \"a76\\\":\\\"\\\", \"a88\\\":\\\"locateServiceName:android.os.BinderProxy|phoneServ
iceName:android.os.BinderProxy\\\", \"a84\\\":\\\"3vDSuAiODgqAwBUsIqCEpuAFJ+xKBFFJ383k
+\\\\\\M2+M=____\\\", \"a68\\\":
[], \\\"a92\\\":\\\"1080,2030\\\", \\\"a93\\\":0, \\\"a95\\\":-1, \\\"a96\\\":\\\"du56APPx0pvUi
zMTZXVP\\\", \\\"a97\\\":\\\"SRCM3hsEtSjSE1fQv1Cares0925Tis1PYZFK58Ez2MNqdho6k0RLGaCyM8N1db014bFXZOC
iXTuZJ+Va9w5pRw==\\\", \\\"a98\\\":\\\"\\\", \\\"a99\\\":\\\"\\\", \\\"a100\\\":\\\"\\\", \\\"a101\\\":\\\"\\\", \\\"a102
\\\":[], \\\"a63\\\":\\\"InputMethodInfo{com.sohu.inputmethod.sogou.xiaomi\\\\\\SogouIME,
settings:
```

```
com.sohu.inputmethod.sogou.SogouIMESettingsLauncher}\\"", \"InputMethodInfo{com.iflytek.inputmethod.miui\\/.FlyIME, settings:  
com.iflytek.inputmethod.LauncherSettingsActivity\"]}, \"a67\": {}, \"a64\":  
{} , \"suc\": \"1\" , \"enable\": \"0\" , \"service\": [] } , \"a65\": 39 , \"a66\":  
{} , \"a74\": 0 , \"a73\": 0 , \"a78\": [] , \"a75\": 0 , \"a77\":  
{} , \"a86\": \"1100100\" , \"a79\": \"\" , \"a80\": \"1628128282029-  
12295\" , \"a83\": \"1001100\" , \"a85\":  
[] , \"a69\": 15533490176 , \"a71\": 118982303744 , \"a72\":  
{} , \"temp\": 370 , \"vol\": 4095 , \"level\": 85 , \"scale\": 100 , \"status\": 2 } , \"a70\": 1568  
4485120 } ;
```

```
String str3 = "
{\\"all_atamper\\":true,\\"core_atamper\\":true,\\"hook_java_switch\\":true,\\"hook_sw
itch\\":false,\\"risk_apps\\":[\{\\"xposed\\":
{\\"pn\\":\"de.robv.android.xposed.installer\",\"uri\\\":\"\\"},\\"controllers\\":
{\\"pn\\":\"com.soft.controllers\",\"uri\\\":\"\\"},\\"apk008v\\":
{\\"pn\\":\"com.soft.apk008v\",\"uri\\\":\"\\"},\\"apk008Tool\\":
{\\"pn\\":\"com.soft.apk008Tool\",\"uri\\\":\"\\"},\\"ig\\":
{\\"pn\\":\"com.doubee.ig\",\"uri\\\":\"\\"},\\"anjian\\":
{\\"pn\\":\"com.cyjh.mobileanjian\",\"uri\\\":\"\\"},\\"rktech\\":
{\\"pn\\":\"com.ruokuai.rktech\",\"uri\\\":\"\\"},\\"magisk\\":
{\\"pn\\":\"com.topjohnwu.magisk\",\"uri\\\":\"\\"},\\"kinguser\\":
{\\"pn\\":\"com.kingroot.kinguser\",\"uri\\\":\"\\"},\\"substrate\\":
{\\"pn\\":\"com.saurik.substrate\",\"uri\\\":\"\\"},\\"touchsprite\\":
{\\"pn\\":\"com.touchsprite.android\",\"uri\\\":\"\\"},\\"scriptdroid\\":
{\\"pn\\":\"com.stardust.scriptdroid\",\"uri\\\":\"\\"},\\"toolhero\\":
{\\"pn\\":\"com.mobileuncle.toolhero\",\"uri\\\":\"\\"},\\"huluxia\\":
{\\"pn\\":\"com.huluxia.gametools\",\"uri\\\":\"\\"},\\"apkeditor\\":
{\\"pn\\":\"com.gmail.heagoo.apkeditor.pro\",\"uri\\\":\"\\"},\\"xposeddev\\":
{\\"pn\\":\"com.sollyu.xposed.hook.model.dev\",\"uri\\\":\"\\"},\\"anywhere\\":
{\\"pn\\":\"com.txy.anywhere\",\"uri\\\":\"\\"},\\"burgerzws\\":
{\\"pn\\":\"pro.burgerz.wsm.manager\",\"uri\\\":\"\\"},\\"vdloc\\":
{\\"pn\\":\"com.virtualdroid.loc\",\"uri\\\":\"\\"},\\"vdtx\\":
{\\"pn\\":\"com.virtualdroid.txl\",\"uri\\\":\"\\"},\\"vdwzs\\":
{\\"pn\\":\"com.virtualdroid.wzs\",\"uri\\\":\"\\"},\\"vdkit\\":
{\\"pn\\":\"com.virtualdroid.kit\",\"uri\\\":\"\\"},\\"vdwxg\\":
{\\"pn\\":\"com.virtualdroid.wxg\",\"uri\\\":\"\\"},\\"vdgps\\":
{\\"pn\\":\"com.virtualdroid.gps\",\"uri\\\":\"\\"},\\"a1024mloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\\"},\\"drhzg\\":
{\\"pn\\":\"com.deruhai.guangzi.noroot2\",\"uri\\\":\"\\"},\\"yggb\\":
{\\"pn\\":\"com.mcmonjmb.yggb\",\"uri\\\":\"\\"},\\"xsrv\\":
{\\"pn\\":\"xiake.xserver\",\"uri\\\":\"\\"},\\"fakeloc\\":
{\\"pn\\":\"com.dracrays.fakeloc\",\"uri\\\":\"\\"},\\"ultra\\":
{\\"pn\\":\"net.anylocation.ultra\",\"uri\\\":\"\\"},\\"locationcheater\\":
{\\"pn\\":\"com.wifi99.android.locationcheater\",\"uri\\\":\"\\"},\\"dwzs\\":
{\\"pn\\":\"com.dingweizshou\",\"uri\\\":\"\\"},\\"mockloc\\":
{\\"pn\\":\"top.a1024bytes.mockloc.ca.pro\",\"uri\\\":\"\\"},\\"anywhereclone\\":
{\\"pn\\":\"com.txy.anywhere.clone\",\"uri\\\":\"\\"},\\"fakelocc\\":
{\\"pn\\":\"com.dracrays.fakelocc\",\"uri\\\":\"\\"},\\"mockwxlocation\\":
{\\"pn\\":\"com.tandy.android.mockwxlocation\",\"uri\\\":\"\\"},\\"anylocation\\":
{\\"pn\\":\"net.anylocation\",\"uri\\\":\"\\"},\\"totalcontrol\\":
{\\"pn\\":\"com.sigma_rt.totalcontrol\",\"uri\\\":\"\\"},\\"ipj12\\":
{\\"pn\\":\"com.chuangdian.ipj12\",\"uri\\\":\"\\"}],\\"risk_dirs\\":[\{\\"008Mode\\":
{\\"dir\\\":\".system/008Mode\",\"type\\\":\"sdcard\"},\\"008OK\\":
{\\"dir\\\":\".system/008OK\",\"type\\\":\"sdcard\"},\\"008system\\":
{\\"dir\\\":\".system/008system\",\"type\\\":\"sdcard\"},\\"iGrimace\\":
{\\"dir\\\":\"iGrimace\",\"type\\\":\"sdcard\"},\\"touchelper\\":
{\\"dir\\\":\"/data/data/net.aisence.Touchelper\",\"type\\\":\"absolute\"},\\"elfscript\\":
{\\"dir\\\":\"/mnt/sdcard/touchelf/scripts/\",\"type\\\":\"absolute\"},\\"spritelua\\":{\\"dir\\\":\"/mnt/sdcard/TouchSprite/lua\",\"type\\\":\"absolute\"},\\"spritelog\\":{\\"dir\\\":\"/mnt/sdcard/TouchSprite/log\",\"type\\\":\"absolute\"},\\"assistant\\":{\\"dir\\\":\"/data/data/com.xxAssistant\",\"type\\\":\"absolute\"},\\"assistantscript\\":
{\\"dir\\\":\"/mnt/sdcard/com.xxAssistant/script\",\"type\\\":\"absolute\"},\\"mobileanjian\\":
{\\"dir\\\":\"/data/data/com.cyjh.mobileanjian\",\"type\\\":\"absolute\"}],\\"risk_fi
le_switch\\":true,\\"risk_files\\\":\"zb5E/i2Gv4IxR50xSBixKChu8gdkDXKei9GwOBNbN6jq3x
MULFFlAVt94COWwwwhychgUuggyBRjbNG1gzb0dh171P0b7ZnqdDPKYq5NrmMJr3Fwtzccme/nV4RO0yuTb
```

f1jc3DdFuA8eOMaLkvLFFsxnx13Jdu6ZY38LTdbc+h2fnf4KnSRbgcZ5JVfaeiKz5HFQvKzjKJH6x/uQ  
i190PF2kpg4uRmTDh6ev0En0RGh9Jg318Nr0xd87izNvUg5Jg941Q/FX98DYetR2RYe3Sp/9u+cT1EnE  
SikjyMxGjaJ3R1TQ701LfuNwqceVsYw99YeNkCwwTBMQII5a3/2i09HzxRXXiswvk23Txt41xmumhs5  
HDmj6D1/oeQ6oFHqsfd3c/auB0vFrxrqbNH68H9pw/b2wpYnnAJsgYxowaz1MaQj5Y21IGkzz7jSeTN2  
IJFTzPSheHC2K4QS7OSWju/d1rCrA5BXSn05TIGXNukm2AwPEtduBeg4FpR7Lb/Vi0K0cgry4gVRPV1  
QnNBBr5mjI2fs30C1sdzbJG2sZxo56BxeF8HzXDpbro3T+Nqg77E4cynk9a57kkqoeA1RaZn8yHJws4q  
97tFrusokRbcFwmVkyeJ5z1rbwLevZ9fkTcyy3VIQY3E2mwR7kaAJepds1+iDeJBHZwBKUBPJqoPoiE0  
uKTnn8KmvyKjb+Jc8mYXR/mgT1r0c6Cgn6CM9BfynzrJoyTmlXzy2tm6dn66eHM5tsplzG0c3JEgvB2T  
5nSyAc9X0u9/rIbsWQ/8OUNFz2pu7vbfgyswakkPKMbksj3MsRHHE6m1jv/P0rEtunth5/KwH1JQBWW  
R/1epqywjoev2fiJ5FqGTvbt6ZTESeAx+9AIUhv9nMx32svw0VmIIjv6R8UUoa1b5EZHYcm804BEszx2  
/ke/e+1dEvw5ntT0khvme5HIX9Qn0uz6u+gQpJds2aVHMGOXI670xhepwaMskl1tu268x53PYc+rjx  
NXNbKGGD+kJAISPF4d2u0tbVNf57cy1sIF4HK8+7FPxn6gqd4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc  
sWSmmWIQQZE9rIoUbxSFLThQMUW2tI0GFHCJVsppIQtmxx6M9bTuerjd0Ii5oamMswxK3MkAyM1581u  
d05x4ycwfouRXOoxerpjvEmT4jfJJRh86ud/Ecihm6Fp5dm8r4Hg9nPQKebng/Gjl1+/n0S0dpaq/4rQ  
vIk2GWN7Q/M7BboqN7+5ou4qkcyOHaGC8H9OYpwrlhzB/IEYhgBVCePKW6bGkiPBReu72+Bmhgb5KaPN  
JYLFWcdnsN9+df7DcvpVcmntsM56HnKLym168o8XHJIhawjajkElhsqy1s0FOOu1EcN90coIPi7XQFI  
Q2jk7A1qits1bKhtp0m49jcsomHBwqqt5kNno6WF6xiNXODhIZ3diLHXHe1kfWPjpnPZzq2FugBvj0Tx  
+tftPYoGwiJvlu4SBeGez4jcfi2qkCofJm7EeMojox6BuBF3HKjUV+bugusy5BF8qFhb1azop/0++qHt  
BtGkQejeqESFZWWxjhhsrHja68rPa0YDxxCl1tH4xS+38tFWKqgbKovck+2udz1auCSA0etjqfzz70fj  
C4hwJp8wCDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiV06e70sayn1kppG1RW1UmGhLe5g08WDB  
IO1MGfSJMFfn1gt90nJxpWQoymcUM6tuAKSoim0aExqsvK+SIHI/dchN6tiFaHLzesXhqXaHpbixVqDa  
D8gHN/yMR4IeY8e0ohVLwPAFZIWuGPdz3bgqQBmerdLp1zHrzCjWLsoaskyDWW0G0RjkP/YSWK+s1dLe  
wadQpFAtt6x7c5DnkdmvmsxxF7a3fG7G0Tk8miLwSmpgIij80w/oLCbUgYDGEpjGiSG6XEHPktc6ThTs  
+Czc2QNgBi15g12NABEHQKxc3tzykwspoaamWrDe8vNCuKd+Tkk+q0zw66LTmE+maWX56TAQY50MQXOr  
H+6c5iULwda9Qn6rDSVNpTAn6KU6duxDb23QYthBd2orBq6T0Z8NLc8h6QWA9QEG7zs9j/fz/st94xi  
tuk8jkvr131f6bD646ixTx27NzzoQEt2E1s/ZM/iaAxwlaohOKKO5adtDATLyL7Ia1vdwdqz0XGwzus  
IKUjxDIrB0JzgCuGwg2Cj5cRL059Kfs0hgYv8rRgTa41vJcvuhEi6VtpFbGwv+T0C7Zx3xNPmnAVDwth  
UDPKu36z2wzzp89p6qrw7k0UwnN7XiGaV5Lv1Hcih7FnwLe107Mdvg41TprLFMLTwccwjhLf5mrIh6et  
Y5Zqp5ikVKv4vrb0s0SqqFLbzozJ4KshyT2Yzaz7ZK5uQRF2f2u8gPYwn0oF4C8rNbbkdxAzoierX/s7m  
01AMD0Bjss1Lgc180v1jCns5u2drqQm1rkTG5r1k0140fTkoKnjyj90zxrD7/khxs6+pWv6v3CzcdR8  
ojX+7MqmZxVEsdceHzE7gCfR17kb1H8bTzhaQPqh09vDLAo8RjtD2HHjYt2Qvjing8PtX57+/TBuIVPD  
wog6p8mi1hqzlhouzVpbhdrUYQLhh45SBT99ydfs2j6/zovv84C8sE1bq//zh3jku74boayGDzKjsr8u  
NbDZ5sP4DMFg/Zxqnku0nSjjv1P/DU1mfDZA+kzn8Iad/5sdedyjmPb2yIag0uEjVjQt0qz6FeoT2h7m  
MVLwBCMy12Wk+0tTXL2xEpA63Y7Mfxymj8R2Deax6WRz96IoT10Gr8+11Tsav16EHHanMJdy94Es+s+x  
00yvJnRybbNn1qvqu4FcE+16EeDiojoqbaczz0Ys6zkPCY1DrLMibdxjcdxq1Zcw9FQXXNvREKf0k9PE  
DmHJQ8y2hJTTyqaSVqu7imgbOPR1GBV4Eu2/r1euLftwR1mZc6cfRqre9Y0GazGsnHyYh6oK135Z1bsX  
uNaGOGr/ow32s5xuaq6o26hdxdFvbwn7j30yvJ30rHEOGArj95DFnx2IURvMgYRrmUgwdCvmiNTLqZXF  
sbfbmB2kUWGKp2mwa5RWrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8YpgBS6Khh1jwvwTr7ah  
occhi1aa/9y53xuoB9cDrqBm08rj+4VFbyxkFMCHy6rhoY23ok1ystQxxvdF5FjznDbHCenvmkz8Thju  
uSP3VOuVrUHAZssuyiqocQhr8gxPsc6k4XDzohrp+Yfzq5YbLT0nv4+FmTIJ8JWzy5axUG2oACiL8LNY  
pQ1qmTCBixpjFM5iQKPSVdkC0TmZ8b0T+UQLa2Yoxn5Thr0ktaTTN3GkeWq2DlmFkt0FCQcbjIawxy75  
RtuitkcooctFQ3xUNH7s/royb/sx1v+8ebi6L59L3x2PCvqoEXn9gsirr241oyxitrxsE1zaaVrU9Y  
Zcb+a49A602Nrywn81dRPb5t02mUQRp/Kg1IJPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWdnI  
S+Djqn9pbhb8wroyxOFF8aEhwu1o2hsgw91RwZ9umAfjEC4sSt8sc1ELaqaqwKnooKg7sevLq25b6toF  
ARwgdd8yTXH70jPniFuF+UE143yk912LwxFM/squ/UZP97RqbwuPu+bv2bYe3hiqbkj5xv5IOxgs6H3F  
u1lp2zyGwHGrxwoaqz+4/npkuJ7ILAV7y1g8s0Zwfc86hPyRIRv2LNa3gr0bNNUOCsfpcRwdkmBlyhn  
1bGqoj0iurBkjUbYPQ4G8jzoquJmQ5xNyH60AQB0u7LdEDiC0HSUSI3SKzo1uESNSeE3qfv+UF87kzt  
eLj+RaqhAGN9nxstGn9F3yIUb76j13STbwwdEUzb7x8mhij9gQVLNFBR2tgrY=\", \"sensitive.ain  
fo\": true, \"sensitive.apps\": true, \"sensitive.aps\": true, \"sensitive.bssid\": tru  
e, \"sensitive.camera\": true, \"sensitive.cell\": true, \"sensitive.gps\": false, \"se  
nsitive.iccid\": true, \"sensitive.imsi\": true, \"sensitive.mac\": true, \"sensitive.  
ssid\": true, \"sensitive.tel\": false, \"white\_apps\": []}";

```

        String str4 =
    "MIIDLZCCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAYMQSwCQYDVQQGEWJDTjELMAKGA1UECwwCU00
    xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNNDAxMjAyMDMzMDE4WjAyMQs
    WCQYDVQQGEWJDTjELMAKGA1UECwwCU00xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wggEiMA0GCSqGSIb
    3DQEBAQUAA4IBDWAwggEKAoIBAQCT947yNGA4EPVheGp6hsDoU4KBKvmwacn6tqfwit/jlxazzBSPcw4
    3jjxGuF4exM4NPJJtMft/j0IIwJeEx0YHDCJIqu/1pEPsXYb01bhwd5mq34c0RiRx1ji+g+d4rFRO/Xr
    eFRJSeB3w1djvoAMkxoygp+813zM6mzPd36zjbUIajfzkc5LoeITUCC6Db98XiN/hNmvcIwti01Sm9FE
    U1ip1fFb9NZ04vb2Z6xt/ti/rUVzWyshZC1qqVq4s9W4iGPqfTnBsxttiooRUpoe2LtB+J73kKTgJJH
    60pn0ljqd+FaMsL/sdy61ggM+w4ePTe4HF+/dv2ZZp+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
    ZA5/0RAVrhWrYFlnyrex4FjAfBgNVHSMEGDAwgbS83RQZA5/0RAVrhWrYFlnyrex4FjAMBgNVHRMEBT
    DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZo6fn+mH124C8Djm15jCRjYqOISpgk
    gsReEX2F00sxYqBuRPidycdsRNYQG44/i4PQrbwc9T/wLSOyHICaKbXXPhfw14PLRNR0LtgmcLoIveDy
    jzTn3BEF57tZCYSmphMUI0eJeV9o3yh1uURV3vbigh+0ca2Mql9m7N49dkkgeZ04FAWUp9yG+p1jf5tA
    Iwa6t1vvH1T8TKwjGtBH3jvYenKBk+W+DWZnDepg01+8Xozo0JP5u1u68sqf+cke0Bw1RfsTFU4ya
    OEBSIIZ/Stx7Q82K8M4xucAFV8PTT8i30QoGcsduEj4zape1vnNn7f";
        String str5 = "du56APPx0pvUiZMTZXVP";
        String str6 = "95fen";
        list.add(vm.addLocalObject(new StringObject(vm,str2)));
        list.add(vm.addLocalObject(new StringObject(vm,str3)));
        list.add(vm.addLocalObject(new StringObject(vm,str4)));
        list.add(vm.addLocalObject(new StringObject(vm,str5)));
        list.add(vm.addLocalObject(new StringObject(vm,str6)));
        Number number = module.callFunction(emulator,0x16f1d,list.toArray())[0];
        String result = vm.getObject(number.intValue()).getValue().toString();
        System.out.println(result);
    }
}

```

```

@Override
public DvmObject<?> callStaticObjectMethodV(BaseVM vm, DvmClass dvmClass,
String signature, VaList vaList) {
    switch (signature){
        case "android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;":{
            return vm.resolveClass("java/io/File").newObject(signature);
        }
        case "javax/crypto/Cipher-
>getInstance(Ljava/lang/String;)Ljava/crypto/Cipher;":{
            return
vm.resolveClass("javax/crypto/Cipher").newObject(signature);
        }
    }
    return super.callStaticObjectMethodV(vm, dvmClass, signature, vaList);
}

@Override
public DvmObject<?> callObjectMethodV(BaseVM vm, DvmObject<?> dvmObject,
String signature, VaList vaList) {
    switch (signature){
        case "java/io/File->getAbsolutePath()Ljava/lang/String;":{
            String tag = dvmObject.getValue().toString();
            if(tag.equals("android/os/Environment-
>getExternalStorageDirectory()Ljava/io/File;")){
                return new StringObject(vm, "/storage/emulated/0");
            }
        }
        case "java/security/cert/Certificate-
>getPublicKey()Ljava/security/PublicKey;":{

```

```

        return
    vm.resolveClass("java/security/PublicKey").newObject(signature);
    }
    case "javax/crypto/Cipher->doFinal([B)[B]:":
        byte[] result =
hexStringToByteArray("10067ad9102b18783bc3242d4a3781c15822b0e8098b8956fff207ec8b
04746e15307d3b615bee9db188b4102d7c102becf6990afc95464aa987b6c83707af8e95f3137db4
6db900cd5ca68fd5b81fad0623950a24b42e39df031849e8130d33a26e0db637ff5fe7f14f3b527f
7b2dd3f2fc8f2fdbabad2ca2d0327f0e10bfb7144e8b7bc40d7c5820c993fa17c139995946b2f140
2e529ce7b4803f78f6026cb780f9a052a0ddd571a1ac13b06b27b4ad1432ce99efb93366dee4a67d
ccf302a612f902a03e06eb1ba6eb8e84479cda22d6ad92834c4db0b6aa0cce8a5fd0fc466fe595
b3dc6038d9975bb7ab6e5df7840a330cf572f2ab3207b25f3270cd");
        return new ByteArray(vm, result);
    }

}
return super.callObjectMethodV(vm, dvmObject, signature, vaList);
}

public static byte[] hexStringToByteArray(String s) {
    int len = s.length();
    byte[] data = new byte[len / 2];
    for (int i = 0; i < len; i += 2) {
        data[i / 2] = (byte) ((Character.digit(s.charAt(i), 16) << 4)
                + Character.digit(s.charAt(i+1), 16));
    }
    return data;
}

@Override
public DvmObject<?> getStaticObjectField(BaseVM vm, DvmClass dvmClass,
String signature) {
    switch (signature){
        case "java/security/spec/MGF1ParameterSpec-
>SHA256:Ljava/security/spec/MGF1ParameterSpec;":{
            return
    vm.resolveClass("java/security/spec/MGF1ParameterSpec").newObject(signature);
        }
        case "javax/crypto/spec/PSource$PSpecified-
>DEFAULT:Ljavax/crypto/spec/PSource$PSpecified;":{
            return
    vm.resolveClass("javax/crypto/spec/PSource$PSpecified").newObject(signature);
        }
    }
    return super.getStaticObjectField(vm, dvmClass, signature);
}

@Override
public DvmObject<?> newObjectV(BaseVM vm, DvmClass dvmClass, String
signature, VaList vaList) {
    switch (signature){
        case "javax/crypto/spec/OAEPParameterSpec-><init>
(Ljava/lang/String;Ljava/lang/String;Ljava/security/spec/AlgorithmParameterSpec;
Ljavax/crypto/spec/PSource;)V":{
            return
    vm.resolveClass("javax/crypto/spec/OAEPParameterSpec").newObject(signature);
        }
    }
}

```

```
        }

        return super.newObjectV(vm, dvmClass, signature, vaList);
    }

    @Override
    public void callVoidMethodV(BaseVM vm, DvmObject<?> dvmObject, String
signature, VaList vaList) {
        switch (signature){
            case "javax/crypto/Cipher-
>init(ILjava/security/Key;Ljava/security/spec/AlgorithmParameterSpec;)V":{
                vm.resolveClass("javax/crypto/Cipher").newObject(signature);
                return;
            }
        }
        super.callVoidMethodV(vm, dvmObject, signature, vaList);
    }

}
```

```
JNIEnv->GetMethodID(javajava/crypto/spec/OAEPParameterSpec.<init>({Ljava/lang/String;Ljava/lang/String;Ljava/security/spec/AlgorithmParameterSpec;Ljavax/crypto/spec/PSource;)V) => 0x
JNIEnv->GetClass(javajava/security/spec/MGF1ParameterSpec) was called from RX@0x404507b[libmsdk.so]x4507b
JNIEnv->GetStaticFieldID(javajava/security/spec/MGF1ParameterSpec,SHA256Ljava/security/spec/MGF1ParameterSpec;) => 0x1f765897 was called from RX@0x4045f0f[libmsdk.so]x45f0f
JNIEnv->GetStaticObjectField(class java/security/spec/MGF1ParameterSpec,SHA256 Ljava/security/spec/MGF1ParameterSpec; => java.security.spec.MGF1ParameterSpec@221af3c8) was calle
JNIEnv->GetClass(javajava/crypto/spec/PSource$PSpecified) was called from RX@0x404507b[libmsdk.so]x4507b
JNIEnv->GetStaticFieldID(javajava/crypto/spec/PSource$PSpecified,DEFAULTLTjavajava/crypto/spec/PSource$PSpecified;) => 0xaea42f9d9 was called from RX@0x4045ff[libmsdk.so]x45ff0f
JNIEnv->GetStaticObjectField(class javajava/crypto/spec/PSource$PSpecified, DEFAULT Ljavajava/crypto/spec/PSource$PSpecified; => javax.crypto.spec.PSource$PSpecified@62bd765) was calle
JNIEnv->NewStringUTF("SHA-256") was called from RX@0x4051169[libmsdk.so]x0j51169
JNIEnv->NewStringUTF("MGF1") was called from RX@0x4051169[libmsdk.so]x0j51169
JNIEnv->NewObject(javajava/crypto/spec/OAEPParameterSpec,<init>("SHA-256","MGF1", java.security.spec.MGF1ParameterSpec@221af3c8, javajava/crypto/spec/PSource$PSpecified@62bd76
JNIEnv->GetMethodID(javajava/crypto/Cipher.init(ILjava/security/Key;Ljava/security/spec/AlgorithmParameterSpec;)V) => 0x4444f9e5 was called from RX@0x40845a25[libmsdk.so]x45a25
JNIEnv->CallVoidMethodV(javajava.crypto.Cipher@9d6c7c, init(0x1, java.security.PublicKey@797badd3, javajava.crypto.spec.OAEPParameterSpec@dd5b207)) was called from RX@0x4084920b[lib
JNIEnv->NewByteArray(32) was called from RX@0x40850d9[libmsdk.so]x0j50d9
JNIEnv->SetByteArrayRegion([B@586fd99, 0, 32, RN@0x0403131ec) was called from RX@0x4051de5[libmsdk.so]x0j51de5
JNIEnv->GetMethodID(javajava/crypto/Cipher.doFinal([B){B} => 0x13ab3b was called from RX@0x40845a25[libmsdk.so]x45a25
JNIEnv->CallObjectMethod(javajava.crypto.Cipher@19dc67c2, doFinal([B@58fd99)) => [0xb61272d4] was called from RX@0x40849ae9[libmsdk.so]x0j49ae9
JNIEnv->GetArrayLength([B@b61272d4 => 256) was called from RX@0x4085377d[libmsdk.so]x0j5377d
JNIEnv->GetByteArrayRegion([B@b61272d4, 0, 256, RN@0x0403c20b) was called from RX@0x40052407[libmsdk.so]x0j52407
JNIEnv->NewStringUTF("("+"organization": "du56APXp0vUiZMTZXPV", "os": "android", "appID": "95fen", "encode": 2, "compress": 3, "data": "ooll0VizBuZikK8laArQHYufW3rlWxK58lhu9TvmmW\|\\jlsZVYJX
{"organization": "du56APXp0vUiZMTZXPV", "os": "android", "appID": "95fen", "encode": 2, "compress": 3, "data": "ooll0VizBuZikK8laArQHYufW3rlWxK58lhu9TvmmW\|\\jlsZVYJXjVpTQ15LP5zI6mCM4ejEXI

Process finished with exit code 0
```

出结果了，但这里我们不验证它的对错，学习和研究Unidbg才是我们的重心。

想一下我们这样补JAVA环境是怎么一回事儿？一个人要吃十个包子才能饱，我们图省事，所以前面九个包子都没管，直接给它空气，当他吃第十个包子时，我们还是塞给他空气，顺便给了他一个“你饱了”的信号，大概就是这事儿。

这样补环境比较丑陋，而且不稳健，容易出问题，我们这儿只是演示一下，如果中间的jAVA方法很多很复杂，那可以这么做，这大概就是“过程没关系，结果对就行。”

之后的小红书环境补充中，会展示另外一个思路，他想吃十个包子，那就给他十个包子，每个包子都实实在在的那种，怎么做呢？敬请期待喽。

最后再看一个文件检查

最后再看一个文件检查

```
Run: shumei
Q: lilac pa
Read 37 bytes from 'pipe2_read_side'
Read 0 bytes from 'pipe2_read_side'
File closed 'pipe2_read_side' from RX@0x40196fe1[libc.so]0x19fe1
[15:47:26 188]  WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32Sysca
lilac Path:/system/lib/libmemtrack.so
File opened '/system/lib/libmemtrack.so' with oflags=0x20000 errno is 2 from F
[15:47:26 190]  INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32Sysca
lilac Path:/system/lib/libmemtrack_real.so
File opened '/system/lib/libmemtrack_real.so' with oflags=0x20000 errno is 2 +
[15:47:26 192]  INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32Sysca
JNIEnv->FindClass(java/lang/wgzs/DeviceInfoProp) was called from RX@0x4002d601
JNIEnv->FindClass(java/lang/WgzsUtil) was called from RX@0x4002d811[libsmsdk.s
JNIEnv->NewByteArray(819) was called from RX@0x40050dc9[libsmsdk.so]0x50dc9
```

这两个文件是Riru的特征文件，Riru是啥？

## Riru

Riru only does one thing, inject into zygote in order to allow modules to run their codes in apps or the system server.

The name, Riru, comes from a character. ([https://www.pixiv.net/member\\_illust.php?mode=medium&illust\\_id=74128856](https://www.pixiv.net/member_illust.php?mode=medium&illust_id=74128856))

## Requirements