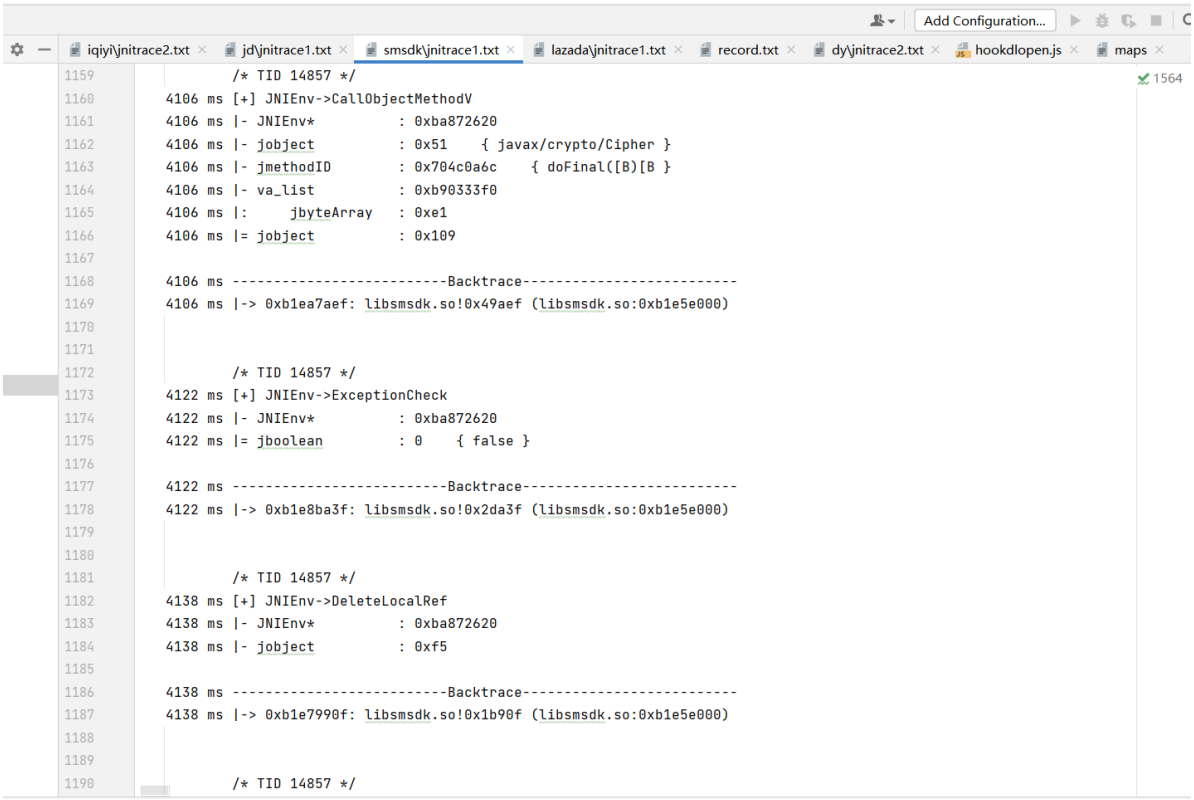
怎么用Unidbg把数美SDK里的函数跑起来？本篇做了这方面的尝试和分析，感谢我的朋友nu11进行审稿和技术指导。

样本链接：https://pan.baidu.com/s/1IIFUQ9X2MiFScbWbJoXpLw
提取码：te2q

com.ishumei.dfp.SMSDK

```java
package com.ishumei.dfp;

import android.content.Context;
import androidx.annotation.Keep;

@Keep
public class SMSDK {
    static {
        try {
            System.loadLibrary("smsdk");
        } catch (Throwable unused) {
        }
    }

    public static String v1(Context context, String str, String str2, String str3, String str4, String str5) {
        return new SMSDK().w1(context, str, str2, str3, str4, str5);
    }

    public static String v3(Context context, String str, String str2, String str3, String str4) {
        try {
            return new SMSDK().w3(context, str, str2, str3, str4);
        } catch (Throwable unused) {
            return "";
        }
    }

    private native String w3(Context context, String str, String str2, String str3, String str4);

    private native String x6(String str, String str2);

    public static String xx6(String str, String str2) {
        try {
            return new SMSDK().x6(str, str2);
        } catch (Throwable unused) {
            return "";
        }
    }

    public native String w1(Context context, String str, String str2, String str3, String str4, String str5);
}
```

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。



接下来进入Unidbg

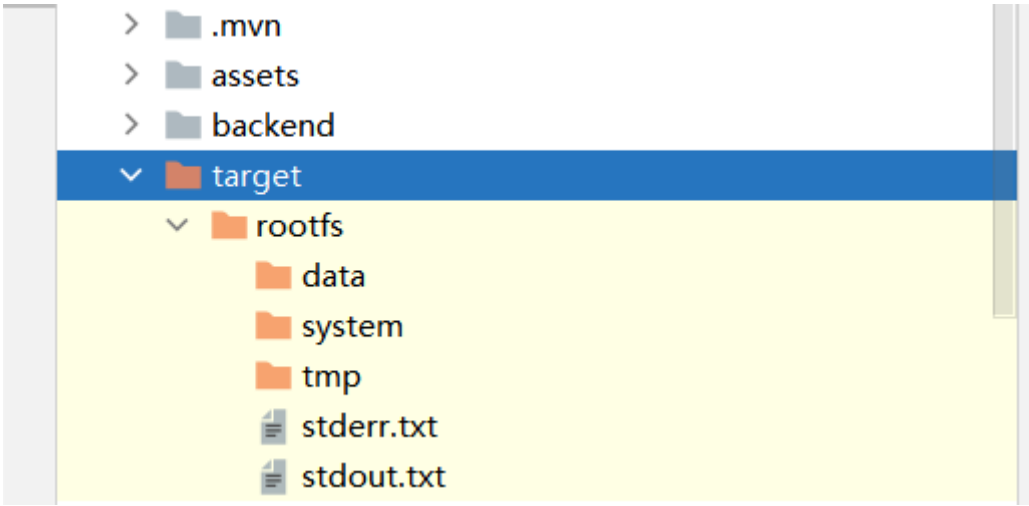
```
package com.jiuwu;

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/libsmsdk.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。

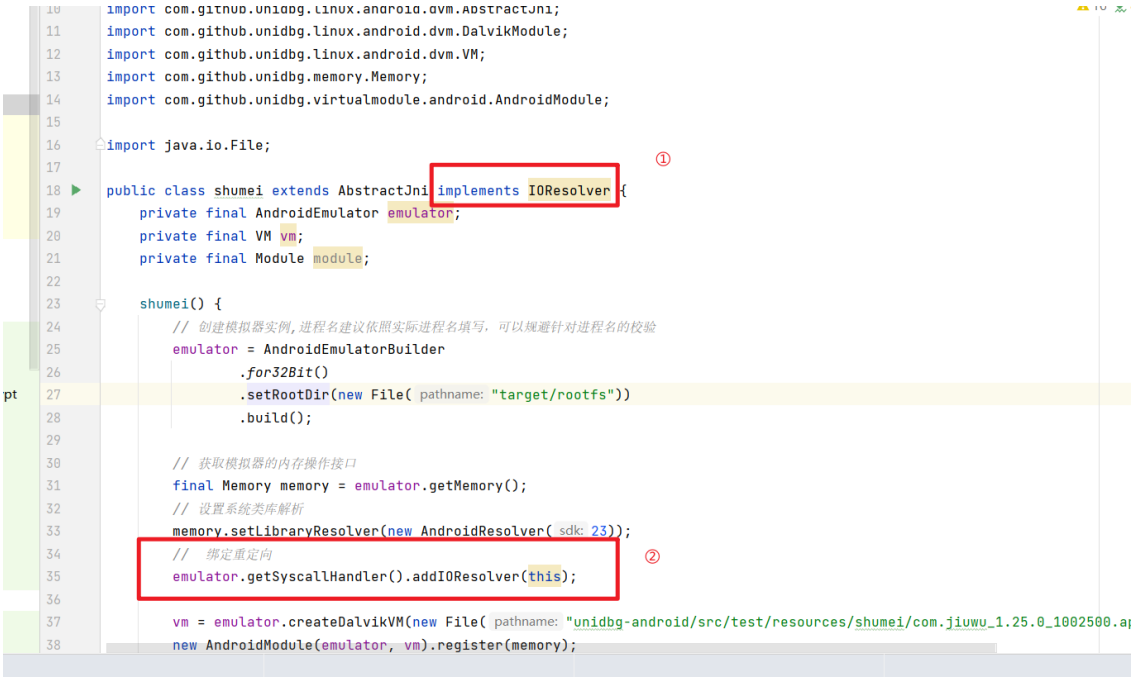
  初始化模拟器中的 **setRootDir(new File("target/rootfs"))** 是指定当前项目的文件系统位置，运行测试你会在Unidbg目录中看到它。假设要访问tmp/a.txt，你可以将电脑里的a.txt 通过adb pull出来，然后放在target/rootfs/tmp下，Unidbg即可完成该样本中对该文件的访问。

  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。



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der

我们这里两种文件重定向都使用了，会冲突吗？

——并不。

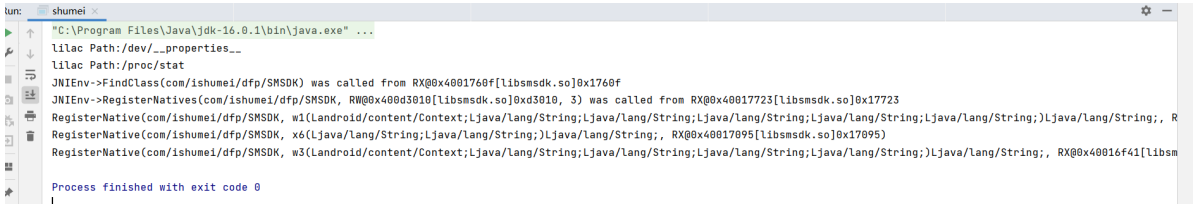
你可以通过虚拟文件系统补tmp/a.txt，然后通过代码补tmp/b.txt，这是完全没问题的，怎么方便怎么来。

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



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JNIOnLoad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\":\"all\",\"a3\":\"none\",\"a4\":\"4\",\"a2\":\"SRcM3hsEtSjSE1fQv1CaresO92
5Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOCiXTuZJ+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
(v8l)\",\"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_aml_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\
":\"a58929cd0e32020053f6137261ecd3c40\",\"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\":\"3vDSuAiODgqAwBuSIqCEpuAFlJ+xKBFFJ383k
+\\/M2+M=___\",\"a68\":
[],\"a92\":\"1080,2030\",\"a93\":0,\"a95\":-1,\"a96\":\"dU56APPxOpvUizMTZXVP\",\
"a97\":\"SRcM3hsEtSjSE1fQv1CaresO925Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOC
iXTuZJ+Va9w5pRw==\",\"a98\":\"\",\"a99\":\"\",\"a100\":\"\",\"a101\":\"\",\"a102
\":[],\"a63\":[\"InputMethodInfo{com.sohu.inputmethod.sogou.xiaomi\\/.SogouIME,
settings:
```

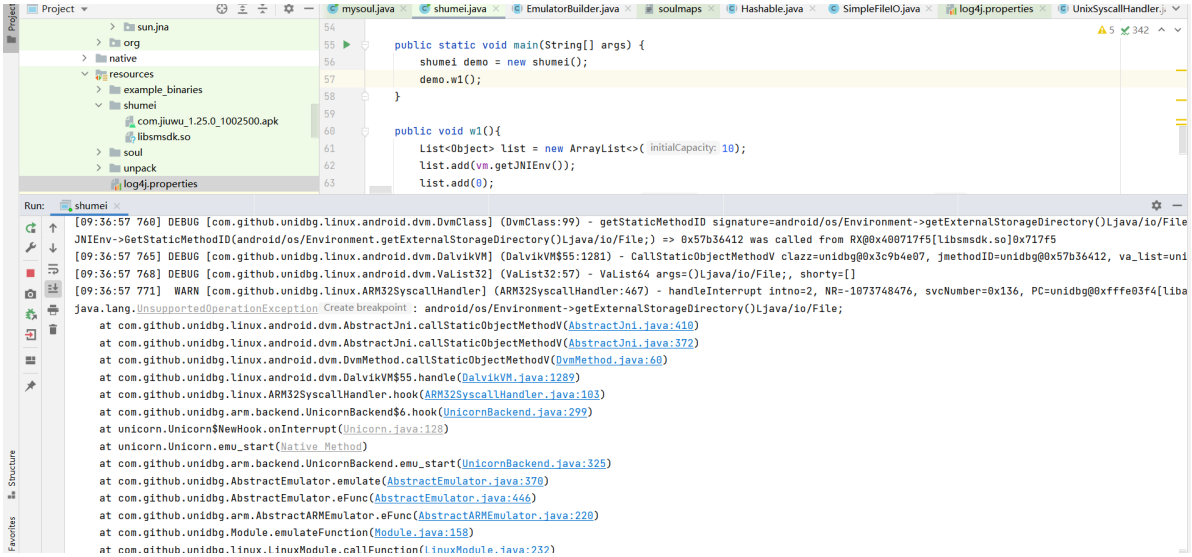
com.sohu.inputmethod.sogou.SogouIMESettingsLauncher}\",\"InputMethodInfo{com.iflytek.inputmethod.miui\\/.FlyIME, settings: com.iflytek.inputmethod.LauncherSettingsActivity}\"],\"a67\":{},\"a64\":{\"suc\":\"1\",\"enable\":\"0\",\"service\":[]},\"a65\":39,\"a66\":{},\"a74\":0,\"a73\":0,\"a78\":[],\"a75\":0,\"a77\":{},\"a86\":\"110010O\",\"a79\":\"\",\"a80\":\"1628128282029-12295\",\"a83\":\"1001100\",\"a85\":[],\"a69\":15533490176,\"a71\":118982303744,\"a72\":{\"temp\":370,\"vol\":4095,\"level\":85,\"scale\":100,\"status\":2},\"a70\":15684485120}";

```
    String str3 = "
{\"all_atamper\":true,\"core_atamper\":true,\"hook_java_switch\":true,\"hook_swi
tch\":false,\"risk_apps\":[{\"xposed\":
{\"pn\":\"de.robv.android.xposed.installer\",\"uri\":\"\"}},{\"controllers\":
{\"pn\":\"com.soft.controllers\",\"uri\":\"\"}},{\"apkOO8v\":
{\"pn\":\"com.soft.apkOO8v\",\"uri\":\"\"}},{\"apkOO8Tool\":
{\"pn\":\"com.soft.apkOO8Tool\",\"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\":\"\"}},{\"burgerzwsm\":
{\"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\":\"\"}},{\"a1O24mloc\":
{\"pn\":\"top.a1O24bytes.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.a1O24bytes.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\":[{\"OO8Mode\":
{\"dir\":\".system/OO8Mode\",\"type\":\"sdcard\"}},{\"OO8OK\":
{\"dir\":\".system/OO8OK\",\"type\":\"sdcard\"}},{\"OO8system\":
{\"dir\":\".system/OO8system\",\"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/i2Gv4IxR5OxSBiXKcHu8gdkDXKei9GwOBNbN6jq3x
MUlFFlAvT94COwwWhychgUggyBRjbNG1gzOdh171POb7ZnqdDPKYq5NrmMJr3Fwtzccme/nV4ROOyuTb
```

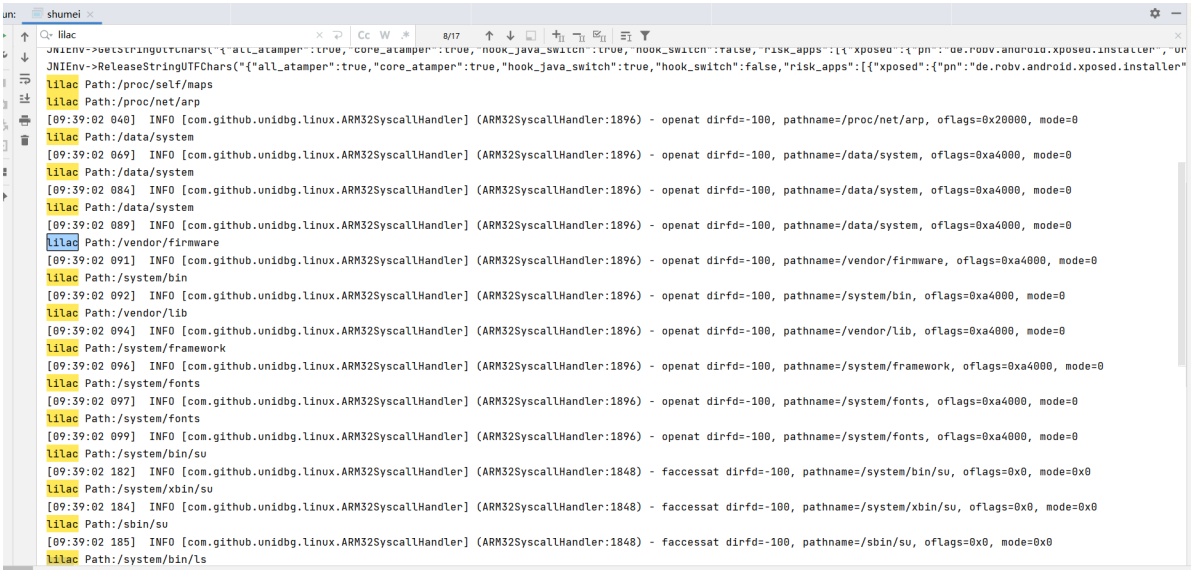
fljc3DdFUa8eOMaLkVLFfsXnxl3Jdu6ZY38LTdbc+h2fnf4KnSRbgcZ5JVFaeiKZ5HFQvKZjKJH6x/UQ
il9OPf2kpg4uRmTDh6evOEnORGh9Jg3l8Nr0xd87iZNvUg5Jg94lQ/FX98DYetR2RYe3Sp/9u+CTlEnE
SikjyMxGjAJ3R1TQ7O1LfuNwqceVsYw99YeNkCwWwTBMQII5a3/2iO9HzxRXXisWVk23TXt41xmumhs5
HDmj6D1/oeQ6oFHqSfd3C/aUbOvFrxrqbNH68H9pW/b2wpYnnAJSgYxoWaz1MaQJ5Y21IGkzZ7jSeTN2
IJFTzPsHesHc2K4QS7OSWju/d1rCrA5BXSnO5TIGXNukm2AwPEtduBeg4FpR7Lb/VIOKOcgrg4gVRPVl
QnNBr5mJI2fS3OC1sDZibJG2sZxo56BXeF8HzXDPBrO3T+Nqg77E4cynk9a57kkqOeA1RaZn8yHJWs4q
97tFrUsokRbcFwmVkYeJ5z1rbWLeVZ9fkTcyy3VIQY3E2mwR7kaAJepdSl+iDeJBHZwBKUBPJqoPoiEO
uKTnn8KmvyKJb+Jc8mYxR/mgT1rOc6Cgn6CM9BfynZrJoyTmlXzy2tm6dN66eHM5tsplzGOc3JEgvB2T
5nSyAc9XOu9/rIbsWQ/8OUNFz2pu7vBfgysWakkPKMbkSj3MsRHHZE6mljv/POrEtuNth5/KwH1JQBWW
R/lepqywjoev2fiJ5FqGTVBt6ZTESeAX+9AIUHv9nMx32sVwOVmIIjV6R8UUOa1b5EZHYCm8O4BEszx2
/ke/e+1dEvw5ntTOkHvme5HIX9QnOuZ6u+gQpJds2aVHMGOXSI67OxzhepwaMskLltU268x53PYc+rjX
NXNbkGGD+kJAISPF4d2UOtbVNFs7Cy1SIF4HK8+7FPxn6gqD4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc
sWSmmyWIQQzE9rIoUbxSFLThQMUW2tI0GfHCJVsppIQtmxx6M9bTuerjdOIi5oamMswxK3MkAyMl58lU
dO5x4ycwfouRXOoxerpjvEmT4jfJJRh86Ud/Ecihm6Fp5dm8r4Hg9nPQKebng/GjL1+/n0SOdpaq/4rQ
vIk2GWN7Q/M7BboqN7+5oU4qkcYOHaGC8H9OYpwRlhZB/IEYHgBVCePKW6bGkiPBReu72+Bmhgb5KaPN
JYLFHWcdsN9+Df7DcVpVCmnTSM56HnKLym168o8XHJIhawjajkElhsqYlsL0FOOUlEcN9OcoIPi7XQFI
Q2jk7A1qiTsIbKHtpOm49jCsomHBWqqT5kNno6WF6xiNXODhIz3diLHXHelkfWPJpnPZzq2FUgBvJOtX
+tftPYoGwIjvlu4SBeGeZ4jCfi2qkCofJm7EeMojox6BuBF3HKjUV+bUgusy5BF8qFHblazop/O++qHt
BtGkQejeqESFZWwXjhsrHja68rPaK0YDxXClitH4xS+38tFWKqgbKoVck+2uDZlauCSA0etJqfzz7Ofj
C4hwJp8WcDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiVO6e7OsayNlkppG1RW1UmGhLe5gO8WDB
IO1MGfSJMffnlgt9OnJxpWQOymcUM6tUAKSoimOaEXqsvK+SIHI/dchN6tiFaHLZesXhqXaHpbiXVqDa
D8gHN/yMR4IeY8eOohVLwPAFZIWuGPdz3bgqQBmerdLp1ZHrZCjWLsOAsKYDWWOGORjkP/YSWK+S1dLe
WadQpFAtt6X7c5DnKdmvmSXXF7a3fG7GOTk8miLwSMpgIij8Ow/oLCbUgYDGEpjGiSG6XEHPktc6ThTs
+CzC2QNgBi15g12NABEHQKxc3tzykwSpoaamWrDe8vNCuKd+TkK+q0zw66LTmE+maWX56TAQY5OMQXOr
H+6c5iULwda9Qn6rDSVNpTaN6KU6dUXDb23QYthBd2oRbq6T0Z8NLc8h6QWVA9QEG7zS9j/fz/st94Xi
tuK8jKvr13lf6bD646ixTx27NZzoQEtd2ElS/ZM/iAaxWlaohOKKO5adtDATLyL7IalvdwdQZ0XGwzuS
IKUjxDIrBOJZgCuGWg2Cj5cRLO59KfS0hgYv8rRgTa4lvJcvuhEi6VTpFbGwV+TOC7ZX3xNPmnAVDWth
UdPKu36z2wzzp89p6qRw7kOUWnN7XIgaV5Lv1Hcih7FNWLe1O7Mdvg41TprLFMLTwcCwjhLf5mrIh6et
Y5ZQp5ikVKv4VrBsOSqqFLbZoZJ4KSHyT2YzaZ7ZK5uQRf2f2u8gPYWnOOF4C8rNbbkdxAzoierX/s7m
O1AMdOBJsS1LGcl8OVljCns5u2dRqQm1rkTG5r1kO14OfTkOKnjyjqo7ZXRd7/khXS6+PWv6v3CzcdR8
ojX+7MqmZXVEsdcEHzE7gCfRl7kb1H8bTZhaQPqhO9vDLAo8RJTd2HHjYt2QvjinG8PtX57+/TBuIvPD
Wog6p8milhqzLHOuZVpbhdrUYQLHh45SbT99ydFS2J6/ZOvV84C8sE1bq//Zh3JKu74bOayGDzKjSr8u
NbDZ5sP4DMFg/ZXqnkUOnSJJVlP/DUlMfdZA+kzN8Iad/5SDEDyjmPb2yIag0uEJVjQt0qz6FeoT2h7m
MVLwBCMyl2WK+OtTXL2xEpA63Y7MfxyMj8R2DeaX6WRz96IoTlOGr8+11TsavI6EHHanMJdY94Es+s+x
OOyvJnRybbNnlqvqu4FcE+l6EeDiojoqbaczZ0YS6zkPCYIDrLMIbdXjCdxq1ZCw9FQXXNVrEKfOk9PE
DmHJQ8y2hJTTyqaSVqU7imgbOPRlGBV4Eu2/r1euLftwRImZc6cfRqre9Y0GaZGsNHyYh6oKl35Z1bsX
uNaGOgR/ow32s5xUaq6O26hdxdFVbWn7j3OyVJ3OrHEOGArj95DFnx2IURvMgRYrmUgwdCvmiNTLqZXf
sbfmB2kUWGKp2mWa5RWrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8YpgBS6KHhljwVwTr7ah
OCChIlaa/9y53XuoB9cDrqBmO8rj+4VFbyxkFMcHy6RhoY23OklYstQxXvdf5FjzNdbHCenVMkz8ThJU
uSP3VOuVrUHAZssuyiqocQhr8gxPsC6k4XDZohrp+Yfzq5YbLTOnv4+FmTIJ8JWZy5axUG2oACiL8LNy
pQlqmTCBixpjFM5iQKPSVdkCOTmZ8bOT+UQLa2YOXn5Thr0ktaTTN3GkeWq2DlmFktOFCQCbjIaWxY75
RtUitKcooctFQ3xUNH7s/ROyb/sXlV+8ebi6L59L3x2PCvqOEXnQ9gSirr24loYXitrxXsE1zaaVrU9Y
ZcB+a49A6O2Nrywn81dRPb5tO2mUQRp/Kg1IJPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWDnI
S+Djqn9pbhb8wroyxOFF8aEhwulo2hsgW91RwZ9umAFjEC4sSt8sc1ELaqaqWKnooKg7seVLq25b6toF
ARWgdd8yTXH7OjPniFuF+UEl43yK912LWXfM/squU/UZP97RqbWuPu+bv2bYe3hiqBkJ5xv5IOxgS6H3F
uIlpP2zyGwHGrXWOaqZ+4/npkuJ7ILAV7y1g8SOZWfc86hPyRIrV2LNa3gr0bNnUOCsfpcRwdkmBlyhn
lbGqojOiUrBkjUbYPQ4G8jzoqUJmQ5xNyH6OAQBOu7LdEDiCOHSUSI3SKzo1uESNSeE3qfV+UF87kZti
eLj+RaqhAGN9nxstGn9F3yIUb76Jl3STbwwdEUzB7X8mhij9gQVLNFBR2tgrY=\",\"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/jOIIwJeExOYHDCJIqU/1pEPsXYbOlBhwD5mq34cORiRxlji+g+D4rFRO/Xr
efRJSeB3W1djvOAMkXoygp+813ZM6mzPd36zjbUIaJfzkC5LOeITUcC6Db98XiN/hNmvciWtiO1Sm9FE
U1ip1fFb9NZO4vb2Z6Xt/ti/rUVzWyshZClqqVq4s9W4iGPqfTnBsxttiooRUproe2LtB+J73kKTgJJH
6OpnOljqd+FaMsL/sddY6lggM+w4ePTe4HF+/dV2ZZp+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
ZA5/ORAVrhWrYFlnyreX4FjAfBgNVHSMEGDAWgBS83RQZA5/ORAVrhWrYFlnyreX4FjAMBgNVHRMEBTA
DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZO6fn+mH124C8Djm15jCRjYqOISpgk
gsReEX2FOOsxYqBuRPidycdsRNyQG44/i4PQrBwc9T/wLSOyHICaKbXXPhfWl4PLRNROLtgmCLoIveDy
jzTn3BEf57tZCYSmpHMUIOeJeV9o3yhluURv3Vbiqh+0ca2MqL9m7N49DkkgeZO4FAWUp9yG+p1jf5tA
1wa6t1vvH1T8TKvWjGtBH3jVYenKBk+W+DWzZnDepgOl+8BXozOOJP5U1u68Sqf+cke0BwlRfsTFU4yA
oEBsIIZ/Stx7Q82K8M4XucAFV8PTT8i3OQoGcSduEj4zape1vNn7f";
    String str5 = "dU56APPxOpvUizMTZXVP";
    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。



先别急着补AVA调用，看一下文件访问



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

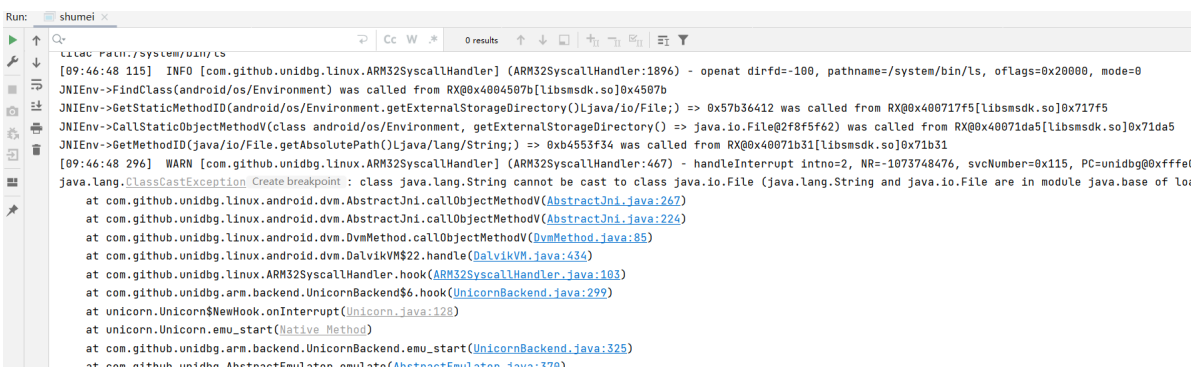
Google可知，Environment.getExternalStorageDirectory() 获取的是SD卡文件

```
@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



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

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

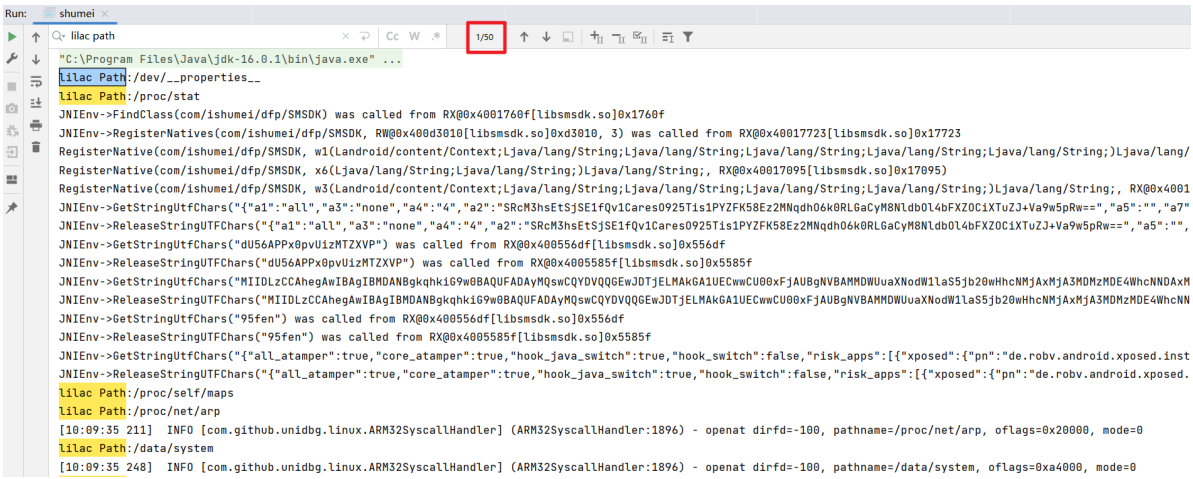
- Google，既然它是Android标准API，上网搜一下
- JNItrace看一下，前面我们阐述过怎么用JNItrace看参数和返回值，你会用了吗？

```
    /* 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: libsmsdk.so!0x71df5 (libsmsdk.so:0xb1e5e000)


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

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


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

2716 ms --------------------------Backtrace--------------------------
2716 ms |-> 0xb1ecf567: libsmsdk.so!0x71567 (libsmsdk.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: libsmsdk.so!0x1ddff (libsmsdk.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: libsmsdk.so!0x71edd (libsmsdk.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。

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



来看看

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

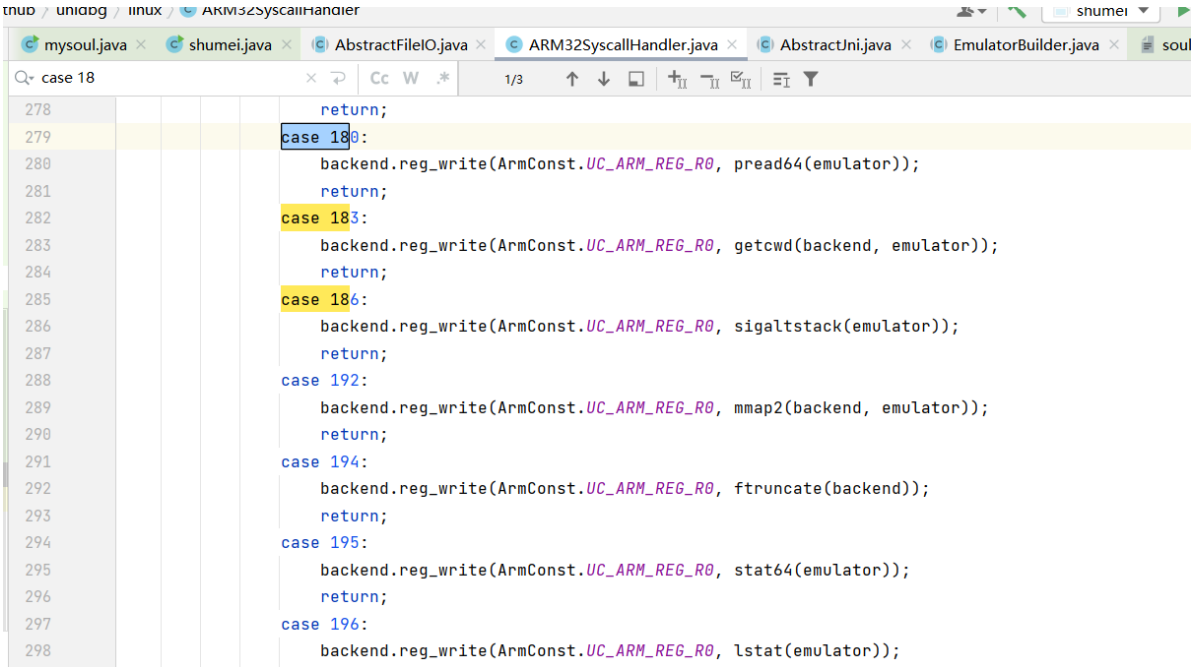
上面的文件访问也基本是EDxposed、xposed、Magisk相关

再往上面看看

像是检测应用分身

接下来处理糟糕的报错

NR = 190，190是什么系统调用？Unidbg尚未实现



查一下表 Chromium OS Docs - Linux System Call Table (googlesource.com)

				*filename				
183	getcwd	man/ cs/	0xb7	char *buf	unsigned long size	-	-	-
184	capget	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vofrk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/libsmsdk.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\":\"all\",\"a3\":\"none\",\"a4\":\"4\",\"a2\":\"SRcM3hsEtSjSE1fQv1CaresO92
5Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOCiXTuZJ+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
(v8l)\",\"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_aml_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\
":\"a58929cd0e32020053f6137261ecd3c40\",\"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\":\"3vDSuAiODgqAwBuSIqCEpuAFlJ+xKBFFJ383k
+\\/M2+M=___\",\"a68\":
[],\"a92\":\"1080,2030\",\"a93\":0,\"a95\":-1,\"a96\":\"dU56APPxOpvUizMTZXVP\",\
"a97\":\"SRcM3hsEtSjSE1fQv1CaresO925Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOC
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\":\"110010O\",\"a79\":\"\",\"a80\":\"1628128282029-12295\",\"a83\":\"1001100\",\"a85\":[],\"a69\":15533490176,\"a71\":118982303744,\"a72\":{\"temp\":370,\"vol\":4095,\"level\":85,\"scale\":100,\"status\":2},\"a70\":15684485120}";

```
        String str3 = "
{\"all_atamper\":true,\"core_atamper\":true,\"hook_java_switch\":true,\"hook_swi
tch\":false,\"risk_apps\":[{\"xposed\":
{\"pn\":\"de.robv.android.xposed.installer\",\"uri\":\"\"}},{\"controllers\":
{\"pn\":\"com.soft.controllers\",\"uri\":\"\"}},{\"apkOO8v\":
{\"pn\":\"com.soft.apkOO8v\",\"uri\":\"\"}},{\"apkOO8Tool\":
{\"pn\":\"com.soft.apkOO8Tool\",\"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\":\"\"}},{\"burgerzwsm\":
{\"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\":\"\"}},{\"a1024mloc\":
{\"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\":[{\"OO8Mode\":
{\"dir\":\".system/OO8Mode\",\"type\":\"sdcard\"}},{\"OO8OK\":
{\"dir\":\".system/OO8OK\",\"type\":\"sdcard\"}},{\"OO8system\":
{\"dir\":\".system/OO8system\",\"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/i2Gv4IxR5OxSBiXKcHu8gdkDXKei9GwOBNbN6jq3x
MUlFFlAvT94COwwWhychgUggyBRjbNG1gzOdh171P0b7ZnqdDPKYq5NrmMJr3Fwtzccme/nV4RO0yuTb
```

fljc3DdFUa8eOMaLkVLFfsXnxl3Jdu6ZY38LTdbc+h2fnf4KnSRbgcZ5JVFaeiKZ5HFQvKZjKJH6x/UQ
il9OPf2kpg4uRmTDh6evOEnORGh9Jg3l8Nr0xd87iZNvUg5Jg94lQ/FX98DYetR2RYe3Sp/9u+CTlEnE
SikjyMxGjAJ3R1TQ7O1LfuNwqceVsYw99YeNkCwWwTBMQII5a3/2iO9HzxRXXisWVk23TXt41xmumhs5
HDmj6D1/oeQ6oFHqSfd3C/aUbOvFrxrqbNH68H9pW/b2wpYnnAJSgYxoWaz1MaQJ5Y21IGkzZ7jSeTN2
IJFTzPsHesHc2K4QS7OSWju/d1rCrA5BXSnO5TIGXNukm2AwPEtduBeg4FpR7Lb/VIOKOcgrg4gVRPVl
QnNBr5mJI2fS3OC1sDZibJG2sZxo56BXeF8HzXDPBrO3T+Nqg77E4cynk9a57kkqOeA1RaZn8yHJWs4q
97tFrUsokRbcFwmVkYeJ5z1rbWLeVZ9fkTcyy3VIQY3E2mwR7kaAJepdSl+iDeJBHZwBKUBPJqoPoiEO
uKTnn8KmvyKJb+Jc8mYxR/mgT1rOc6Cgn6CM9BfynZrJoyTmlXzy2tm6dN66eHM5tsplzGOc3JEgvB2T
5nSyAc9XOu9/rIbsWQ/8OUNFz2pu7vBfgysWakkPKMbkSj3MsRHHZE6mljv/POrEtuNth5/KwH1JQBWW
R/lepqywjoev2fiJ5FqGTVBt6ZTESeAX+9AIUHv9nMx32sVwOVmIIjV6R8UUOa1b5EZHYCm8O4BEszx2
/ke/e+1dEvw5ntTOkHvme5HIX9QnOuZ6u+gQpJds2aVHMGOXSI67OxzhepwaMskLltU268x53PYc+rjX
NXNbkGGD+kJAISPF4d2UOtbVNFs7Cy1SIF4HK8+7FPxn6gqD4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc
sWSmmyWIQQzE9rIoUbxSFLThQMUW2tI0GfHCJVsppIQtmxx6M9bTuerjdOIi5oamMswxK3MkAyMl58lU
dO5x4ycwfouRXOoxerpjvEmT4jfJJRh86Ud/Ecihm6Fp5dm8r4Hg9nPQKebng/GjL1+/n0SOdpaq/4rQ
vIk2GWN7Q/M7BboqN7+5oU4qkcYOHaGC8H9OYpwRlhZB/IEYHgBVCePKW6bGkiPBReu72+Bmhgb5KaPN
JYLFHWcdsN9+Df7DcVpVCmnTSM56HnKLym168o8XHJIhawjajkElhsqYlsL0FOOUlEcN9OcoIPi7XQFI
Q2jk7A1qiTsIbKHtpOm49jCsomHBWqqT5kNno6WF6xiNXODhIz3diLHXHelkfWPJpnPZzq2FUgBvJOtX
+tftPYoGwIjvlu4SBeGeZ4jCfi2qkCofJm7EeMojox6BuBF3HKjUV+bUgusy5BF8qFHblazop/O++qHt
BtGkQejeqESFZWwXjhsrHja68rPaK0YDxXClitH4xS+38tFWKqgbKoVck+2uDZlauCSA0etJqfzz7Ofj
C4hwJp8WcDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiVO6e7OsayNlkppG1RW1UmGhLe5gO8WDB
IO1MGfSJMffnlgt9OnJxpWQOymcUM6tUAKSoimOaEXqsvK+SIHI/dchN6tiFaHLZesXhqXaHpbiXVqDa
D8gHN/yMR4IeY8eOohVLwPAFZIWuGPdz3bgqQBmerdLp1ZHrZCjWLsOAsKYDWWOGORjkP/YSWK+S1dLe
WadQpFAtt6X7c5DnKdmvmSXXF7a3fG7GOTk8miLwSMpgIij8Ow/oLCbUgYDGEpjGiSG6XEHPktc6ThTs
+CzC2QNgBi15g12NABEHQKxc3tzykwSpoaamWrDe8vNCuKd+TkK+q0zw66LTmE+maWX56TAQY5OMQXOr
H+6c5iULwda9Qn6rDSVNpTaN6KU6dUXDb23QYthBd2oRbq6T0Z8NLc8h6QWVA9QEG7zS9j/fz/st94Xi
tuK8jKvr13lf6bD646ixTx27NZzoQEtd2ElS/ZM/iAaxWlaohOKKO5adtDATLyL7IalvdwdQZ0XGwzuS
IKUjxDIrBOJZgCuGWg2Cj5cRLO59KfS0hgYv8rRgTa4lvJcvuhEi6VTpFbGwV+TOC7ZX3xNPmnAVDWth
UdPKu36z2wzzp89p6qRw7kOUWnN7XIgaV5Lv1Hcih7FNWLe1O7Mdvg41TprLFMLTwcCwjhLf5mrIh6et
Y5ZQp5ikVKv4VrBsOSqqFLbZoZJ4KSHyT2YzaZ7ZK5uQRf2f2u8gPYWnOOF4C8rNbbkdxAzoierX/s7m
O1AMdOBJsS1LGcl8OVljCns5u2dRqQm1rkTG5r1kO14OfTkOKnjyjqo7ZXRd7/khXS6+PWv6v3CzcdR8
ojX+7MqmZXVEsdcEHzE7gCfRl7kb1H8bTZhaQPqhO9vDLAo8RJTd2HHjYt2QvjinG8PtX57+/TBuIvPD
Wog6p8milhqzLHOuZVpbhdrUYQLHh45SbT99ydFS2J6/ZOvV84C8sE1bq//Zh3JKu74bOayGDzKjSr8u
NbDZ5sP4DMFg/ZXqnkUOnSJJVlP/DUlMfdZA+kzN8Iad/5SDEDyjmPb2yIag0uEJVjQt0qz6FeoT2h7m
MVLwBCMyl2WK+OtTXL2xEpA63Y7MfxyMj8R2DeaX6WRz96IoTlOGr8+11TsavI6EHHanMJdY94Es+s+x
OOyvJnRybbNnlqvqu4FcE+l6EeDiojoqbaczZ0YS6zkPCYIDrLMIbdXjCdxq1ZCw9FQXXNVrEKfOk9PE
DmHJQ8y2hJTTyqaSVqU7imgbOPRlGBV4Eu2/r1euLftwRImZc6cfRqre9Y0GaZGsNHyYh6oKl35Z1bsX
uNaGOgR/ow32s5xUaq6O26hdxdFVbWn7j3OyVJ3OrHEOGArj95DFnx2IURvMgRYrmUgwdCvmiNTLqZXf
sbfmB2kUWGKp2mWa5RWrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8YpgBS6KHhljwVwTr7ah
OCChIlaa/9y53XuoB9cDrqBmO8rj+4VFbyxkFMcHy6RhoY23OklYstQxXvdf5FjzNdbHCenVMkz8ThJU
uSP3VOuVrUHAZssuyiqocQhr8gxPsC6k4XDZohrp+Yfzq5YbLT0nv4+FmTIJ8JWZy5axUG2oACiL8LNy
pQlqmTCBixpjFM5iQKPSVdkCOTmZ8bOT+UQLa2YOXn5Thr0ktaTTN3GkeWq2DlmFktOFCQCbjIaWxY75
RtUitKcooctFQ3xUNH7s/ROyb/sXlV+8ebi6L59L3x2PCvqOEXnQ9gSirr24loYXitrxXsE1zaaVrU9Y
ZcB+a49A6O2Nrywn81dRPb5tO2mUQRp/Kg1IJPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWDnI
S+Djqn9pbhb8wroyxOFF8aEhwulo2hsgW91RwZ9umAFjEC4sSt8sc1ELaqaqWKnooKg7seVLq25b6toF
ARWgdd8yTXH7OjPniFuF+UEl43yK912LWXfM/squU/UZP97RqbWuPu+bv2bYe3hiqBkJ5xv5IOxgS6H3F
uIlpP2zyGwHGrXWOaqZ+4/npkuJ7ILAV7y1g8SOZWfc86hPyRIrV2LNa3gr0bNnUOCsfpcRwdkmBlyhn
lbGqojOiUrBkjUbYPQ4G8jzoqUJmQ5xNyH6OAQBOu7LdEDiCOHSUSI3SKzo1uESNSeE3qfV+UF87kZti
eLj+RaqhAGN9nxstGn9F3yIUb76Jl3STbwwdEUzB7X8mhij9gQVLNFBR2tgrY=\",\"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\":[]}";

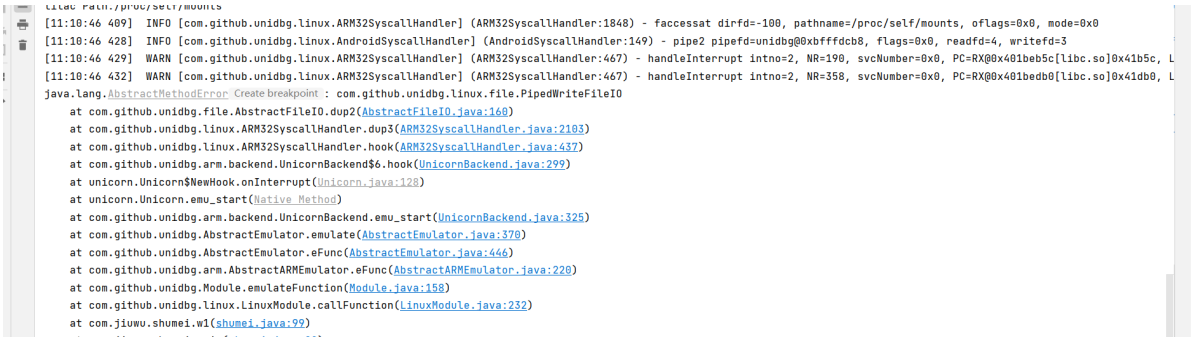
```
        String str4 =
"MIIDLzCCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJDTjELMAkGA1UECwwCU00
xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNNDAxMjAyMDMzMDE4WjAyMQs
wCQYDVQQGEwJDTjELMAkGA1UECwwCU00xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wggEiMA0GCSqGSIb
3DQEBAQUAA4IBDwAwggEKAoIBAQCT947yNGa4EPvheGp6hsDoU4kBKvmwacn6tqfWit/jlXaZZBSPcw4
3jjxGuF4eXM4NPJJtMft/j0IIwJeExOYHDCJIqU/1pEPsXYbOlBhwD5mq34cORiRxlji+g+D4rFRO/Xr
efRJSeB3W1djvOAMkXoygp+813ZM6mzPd36zjbUIaJfzkC5LOeITUcC6Db98XiN/hNmvciWtiO1Sm9FE
U1ip1fFb9NZO4vb2Z6Xt/ti/rUVzWyshZClqqVq4s9W4iGPqfTnBsxttiooRUproe2LtB+J73kKTgJJH
6OpnOljqd+FaMsL/sddY6lggM+w4ePTe4HF+/dV2ZZp+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
ZA5/ORAVrhWrYFlnyreX4FjAfBgNVHSMEGDAWgBS83RQZA5/ORAVrhWrYFlnyreX4FjAMBgNVHRMEBTA
DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZO6fn+mH124C8Djm15jCRjYqOISpgk
gsReEX2FOOsxYqBuRPidycdsRNyQG44/i4PQrBwc9T/wLSOyHICaKbXXPhfWl4PLRNROLtgmCLoIveDy
jzTn3BEf57tZCYSmpHMUIOeJeV9o3yhluURv3Vbiqh+0ca2MqL9m7N49DkkgeZO4FAWUp9yG+p1jf5tA
1wa6t1vvH1T8TKvWjGtBH3jVYenKBk+W+DWzZnDepgOl+8BXozOOJP5U1u68Sqf+cke0BwlRfsTFU4yA
oEBsIIZ/Stx7Q82K8M4XucAFV8PTT8i3OQoGcSduEj4zape1vNn7f";
        String str5 = "dU56APPxOpvUizMTZXVP";
        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

下面是什么报错在等着我们呢?

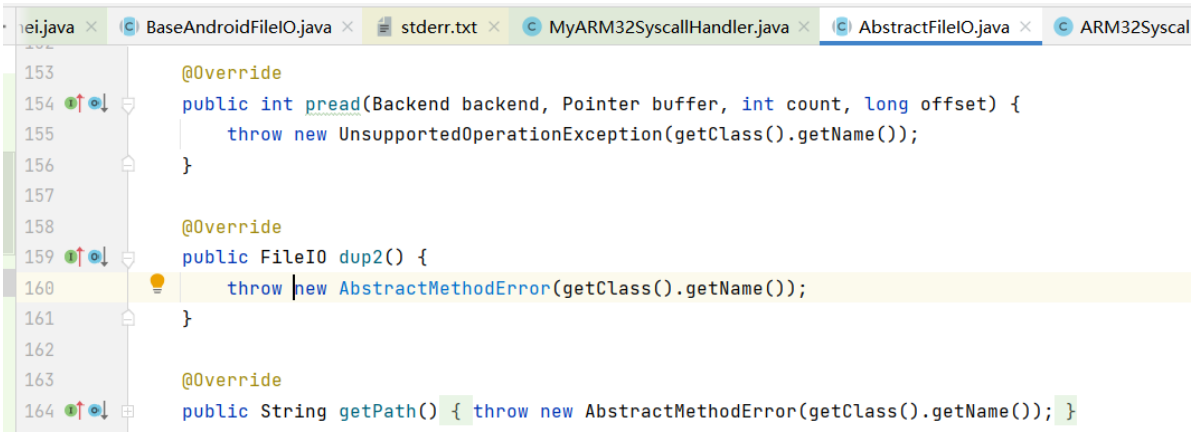
阿西吧，到这一步我没法往下了，因为我的草稿并不是这么走的。来看看我分析测试时的思路吧

回退到MyARM32SyscallHandler还没补的时机点



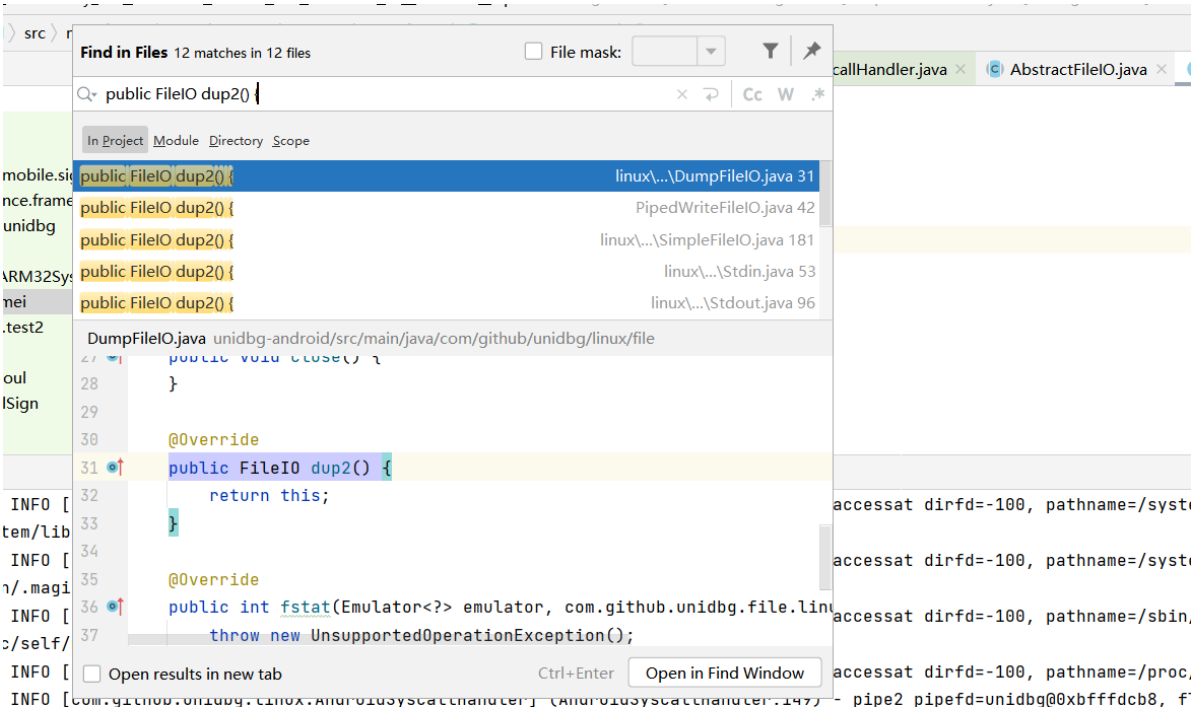
当时我选择先看报错，dup2是什么？dup2用于复制一个文件描述符，它还有一些姊妹，可以看这篇文章 [linux系统调用dup,dup2,dup3_LOVETEDA的博客-CSDN博客]

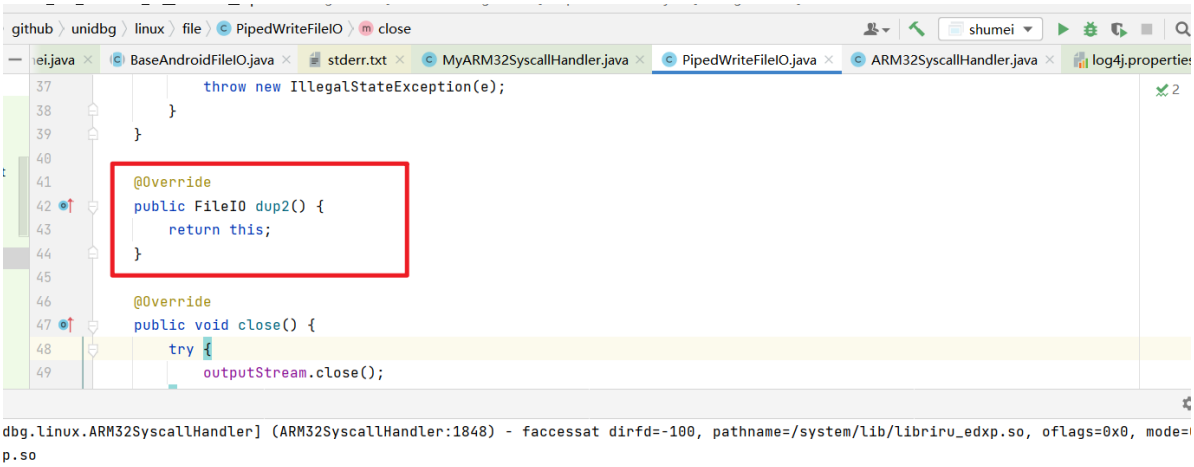
那为什么这儿报错?



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;
```

```java
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/libsmsdk.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\":\"all\",\"a3\":\"none\",\"a4\":\"4\",\"a2\":\"SRcM3hsEtSjSE1fQv1CaresO92
5Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOCiXTuZJ+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
(v8l)\",\"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_aml_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\
":\"a58929cd0e32020053f6137261ecd3c40\",\"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\":\"3vDSuAiODgqAwBuSIqCEpuAFlJ+xKBFFJ383k
+\\/M2+M=___\",\"a68\":
[],\"a92\":\"1080,2030\",\"a93\":0,\"a95\":-1,\"a96\":\"dU56APPxOpvUizMTZXVP\",\
"a97\":\"SRcM3hsEtSjSE1fQv1CaresO925Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOC
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\":\"110010O\",\"a79\":\"\",\"a80\":\"1628128282029-12295\",\"a83\":\"1001100\",\"a85\":[],\"a69\":15533490176,\"a71\":118982303744,\"a72\":{\"temp\":370,\"vol\":4095,\"level\":85,\"scale\":100,\"status\":2},\"a70\":15684485120}";

```
        String str3 = "
{\"all_atamper\":true,\"core_atamper\":true,\"hook_java_switch\":true,\"hook_swi
tch\":false,\"risk_apps\":[{\"xposed\":
{\"pn\":\"de.robv.android.xposed.installer\",\"uri\":\"\"}},{\"controllers\":
{\"pn\":\"com.soft.controllers\",\"uri\":\"\"}},{\"apkOO8v\":
{\"pn\":\"com.soft.apkOO8v\",\"uri\":\"\"}},{\"apkOO8Tool\":
{\"pn\":\"com.soft.apkOO8Tool\",\"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\":\"\"}},{\"burgerzwsm\":
{\"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\":\"\"}},{\"a1024mloc\":
{\"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\":[{\"OO8Mode\":
{\"dir\":\".system/OO8Mode\",\"type\":\"sdcard\"}},{\"OO8OK\":
{\"dir\":\".system/OO8OK\",\"type\":\"sdcard\"}},{\"OO8system\":
{\"dir\":\".system/OO8system\",\"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/i2Gv4IxR5OxSBiXKcHu8gdkDXKei9GwOBNbN6jq3x
MUlFFlAvT94COwwWhychgUggyBRjbNG1gzOdh171P0b7ZnqdDPKYq5NrmMJr3Fwtzccme/nV4RO0yuTb
```

fljc3DdFUa8eOMaLkVLFfsXnxl3Jdu6ZY38LTdbc+h2fnf4KnSRbgcZ5JVFaeiKZ5HFQvKZjKJH6x/UQ
il9OPf2kpg4uRmTDh6evOEnORGh9Jg3l8Nr0xd87iZNvUg5Jg94lQ/FX98DYetR2RYe3Sp/9u+CTlEnE
SikjyMxGjAJ3R1TQ7O1LfuNwqceVsYw99YeNkCwWwTBMQII5a3/2iO9HzxRXXisWVk23TXt41xmumhs5
HDmj6D1/oeQ6oFHqSfd3C/aUbOvFrxrqbNH68H9pW/b2wpYnnAJSgYxoWaz1MaQJ5Y21IGkzZ7jSeTN2
IJFTzPsHesHc2K4QS7OSWju/d1rCrA5BXSnO5TIGXNukm2AwPEtduBeg4FpR7Lb/VIOKOcgrg4gVRPVl
QnNBr5mJI2fS3OC1sDZibJG2sZxo56BXeF8HzXDPBrO3T+Nqg77E4cynk9a57kkqOeA1RaZn8yHJWs4q
97tFrUsokRbcFwmVkYeJ5z1rbWLeVZ9fkTcyy3VIQY3E2mwR7kaAJepdSl+iDeJBHZwBKUBPJqoPoiEO
uKTnn8KmvyKJb+Jc8mYxR/mgT1rOc6Cgn6CM9BfynZrJoyTmlXzy2tm6dN66eHM5tsplzGOc3JEgvB2T
5nSyAc9XOu9/rIbsWQ/8OUNFz2pu7vBfgysWakkPKMbkSj3MsRHHZE6mljv/POrEtuNth5/KwH1JQBWW
R/lepqywjoev2fiJ5FqGTVBt6ZTESeAX+9AIUHv9nMx32sVwOVmIIjV6R8UUOa1b5EZHYCm8O4BEszx2
/ke/e+1dEvw5ntTOkHvme5HIX9QnOuZ6u+gQpJds2aVHMGOXSI67OxzhepwaMskLltU268x53PYc+rjX
NXNbkGGD+kJAISPF4d2UOtbVNFs7Cy1SIF4HK8+7FPxn6gqD4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc
sWSmmyWIQQzE9rIoUbxSFLThQMUW2tI0GfHCJVsppIQtmxx6M9bTuerjdOIi5oamMswxK3MkAyMl58lU
dO5x4ycwfouRXOoxerpjvEmT4jfJJRh86Ud/Ecihm6Fp5dm8r4Hg9nPQKebng/GjL1+/n0SOdpaq/4rQ
vIk2GWN7Q/M7BboqN7+5oU4qkcYOHaGC8H9OYpwRlhZB/IEYHgBVCePKW6bGkiPBReu72+Bmhgb5KaPN
JYLFHWcdsN9+Df7DcVpVCmnTSM56HnKLym168o8XHJIhawjajkElhsqYlsL0FOOUlEcN9OcoIPi7XQFI
Q2jk7A1qiTsIbKHtpOm49jCsomHBWqqT5kNno6WF6xiNXODhIz3diLHXHelkfWPJpnPZzq2FUgBvJOtX
+tftPYoGwIjvlu4SBeGeZ4jCfi2qkCofJm7EeMojox6BuBF3HKjUV+bUgusy5BF8qFHblazop/O++qHt
BtGkQejeqESFZWwXjhsrHja68rPaK0YDxXClitH4xS+38tFWKqgbKoVck+2uDZlauCSA0etJqfzz7Ofj
C4hwJp8WcDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiVO6e7OsayNlkppG1RW1UmGhLe5gO8WDB
IO1MGfSJMffnlgt9OnJxpWQOymcUM6tUAKSoimOaEXqsvK+SIHI/dchN6tiFaHLZesXhqXaHpbiXVqDa
D8gHN/yMR4IeY8eOohVLwPAFZIWuGPdz3bgqQBmerdLp1ZHrZCjWLsOAsKYDWWOGORjkP/YSWK+S1dLe
WadQpFAtt6X7c5DnKdmvmSXXF7a3fG7GOTk8miLwSMpgIij8Ow/oLCbUgYDGEpjGiSG6XEHPktc6ThTs
+CzC2QNgBi15g12NABEHQKxc3tzykwSpoaamWrDe8vNCuKd+TkK+q0zw66LTmE+maWX56TAQY5OMQXOr
H+6c5iULwda9Qn6rDSVNpTaN6KU6dUXDb23QYthBd2oRbq6T0Z8NLc8h6QWVA9QEG7zS9j/fz/st94Xi
tuK8jKvr13lf6bD646ixTx27NZzoQEtd2ElS/ZM/iAaxWlaohOKKO5adtDATLyL7IalvdwdQZ0XGwzuS
IKUjxDIrBOJZgCuGWg2Cj5cRLO59KfS0hgYv8rRgTa4lvJcvuhEi6VTpFbGwV+TOC7ZX3xNPmnAVDWth
UdPKu36z2wzzp89p6qRw7kOUWnN7XIgaV5Lv1Hcih7FNWLe1O7Mdvg41TprLFMLTwcCwjhLf5mrIh6et
Y5ZQp5ikVKv4VrBsOSqqFLbZoZJ4KSHyT2YzaZ7ZK5uQRf2f2u8gPYWnOOF4C8rNbbkdxAzoierX/s7m
O1AMdOBJsS1LGcl8OVljCns5u2dRqQm1rkTG5r1kO14OfTkOKnjyjqo7ZXRd7/khXS6+PWv6v3CzcdR8
ojX+7MqmZXVEsdcEHzE7gCfRl7kb1H8bTZhaQPqhO9vDLAo8RJTd2HHjYt2QvjinG8PtX57+/TBuIvPD
Wog6p8milhqzLHOuZVpbhdrUYQLHh45SbT99ydFS2J6/ZOvV84C8sE1bq//Zh3JKu74bOayGDzKjSr8u
NbDZ5sP4DMFg/ZXqnkUOnSJJVlP/DUlMfdZA+kzN8Iad/5SDEDyjmPb2yIag0uEJVjQt0qz6FeoT2h7m
MVLwBCMyl2WK+OtTXL2xEpA63Y7MfxyMj8R2DeaX6WRz96IoTlOGr8+11TsavI6EHHanMJdY94Es+s+x
OOyvJnRybbNnlqvqu4FcE+l6EeDiojoqbaczZ0YS6zkPCYIDrLMIbdXjCdxq1ZCw9FQXXNVrEKfOk9PE
DmHJQ8y2hJTTyqaSVqU7imgbOPRlGBV4Eu2/r1euLftwRImZc6cfRqre9Y0GaZGsNHyYh6oKl35Z1bsX
uNaGOgR/ow32s5xUaq6O26hdxdFVbWn7j3OyVJ3OrHEOGArj95DFnx2IURvMgRYrmUgwdCvmiNTLqZXf
sbfmB2kUWGKp2mWa5RWrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8YpgBS6KHhljwVwTr7ah
OCChIlaa/9y53XuoB9cDrqBmO8rj+4VFbyxkFMcHy6RhoY23OklYstQxXvdf5FjzNdbHCenVMkz8ThJU
uSP3VOuVrUHAZssuyiqocQhr8gxPsC6k4XDZohrp+Yfzq5YbLTOnv4+FmTIJ8JWZy5axUG2oACiL8LNy
pQlqmTCBixpjFM5iQKPSVdkCOTmZ8bOT+UQLa2YOXn5Thr0ktaTTN3GkeWq2DlmFktOFCQCbjIaWxY75
RtUitKcooctFQ3xUNH7s/ROyb/sXlV+8ebi6L59L3x2PCvqOEXnQ9gSirr24loYXitrxXsE1zaaVrU9Y
ZcB+a49A6O2Nrywn81dRPb5tO2mUQRp/Kg1IJPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWDnI
S+Djqn9pbhb8wroyxOFF8aEhwulo2hsgW91RwZ9umAFjEC4sSt8sc1ELaqaqWKnooKg7seVLq25b6toF
ARWgdd8yTXH7OjPniFuF+UEl43yK912LWXfM/squU/UZP97RqbWuPu+bv2bYe3hiqBkJ5xv5IOxgS6H3F
uIlpP2zyGwHGrXWOaqZ+4/npkuJ7ILAV7y1g8SOZWfc86hPyRIrV2LNa3gr0bNnUOCsfpcRwdkmBlyhn
lbGqojOiUrBkjUbYPQ4G8jzoqUJmQ5xNyH6OAQBOu7LdEDiCOHSUSI3SKzo1uESNSeE3qfV+UF87kZti
eLj+RaqhAGN9nxstGn9F3yIUb76Jl3STbwwdEUzB7X8mhij9gQVLNFBR2tgrY=\",\"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\":[]}";

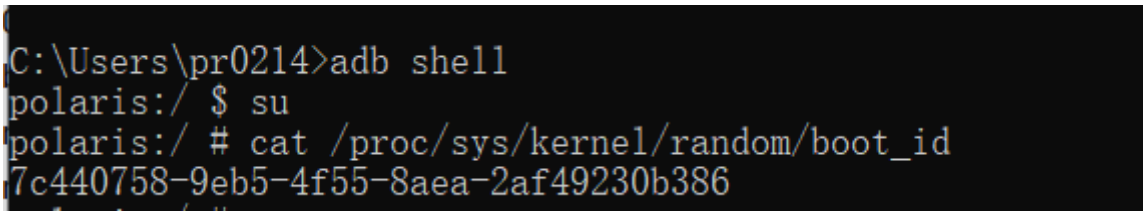
```
        String str4 =
"MIIDLzCCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJDTjELMAkGA1UECwwCU00
xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNNDAxMjAyMDMzMDE4WjAyMQs
wCQYDVQQGEwJDTjELMAkGA1UECwwCU00xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wggEiMA0GCSqGSIb
3DQEBAQUAA4IBDwAwggEKAoIBAQCT947yNGa4EPvheGp6hsDoU4kBKvmwacn6tqfWit/jlXaZZBSPcw4
3jjxGuF4eXM4NPJJtMft/j0IIwJeExOYHDCJIqU/1pEPsXYbOlBhwD5mq34cORiRxlji+g+D4rFRO/Xr
efRJSeB3W1djvOAMkXoygp+813ZM6mzPd36zjbUIaJfzkC5LOeITUcC6Db98XiN/hNmvciWtiO1Sm9FE
U1ip1fFb9NZO4vb2Z6Xt/ti/rUVzWyshZClqqVq4s9W4iGPqfTnBsxttiooRUproe2LtB+J73kKTgJJH
6OpnOljqd+FaMsL/sddY6lggM+w4ePTe4HF+/dV2ZZp+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
ZA5/ORAVrhWrYFlnyreX4FjAfBgNVHSMEGDAWgBS83RQZA5/ORAVrhWrYFlnyreX4FjAMBgNVHRMEBTA
DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZO6fn+mH124C8Djm15jCRjYqOISpgk
gsReEX2FOOsxYqBuRPidycdsRNyQG44/i4PQrBwc9T/wLSOyHICaKbXXPhfWl4PLRNROLtgmCLoIveDy
jzTn3BEf57tZCYSmpHMUIOeJeV9o3yhluURv3Vbiqh+0ca2MqL9m7N49DkkgeZO4FAWUp9yG+p1jf5tA
1wa6t1vvH1T8TKvWjGtBH3jVYenKBk+W+DWzZnDepgOl+8BXozOOJP5U1u68Sqf+cke0BwlRfsTFU4yA
oEBsIIZ/Stx7Q82K8M4XucAFV8PTT8i3OQoGcSduEj4zape1vNn7f";
        String str5 = "dU56APPxOpvUizMTZXVP";
        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);
    }

}
```

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



接下来把我们的SyscallHandler加上去

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“

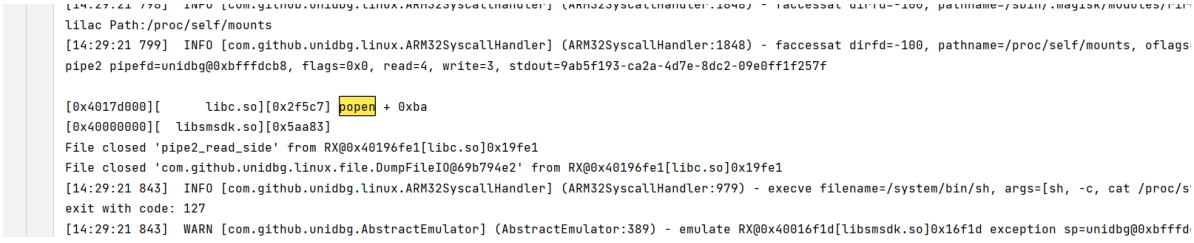
这到底是怎么回事呢？是不是有点稀里糊涂了呢

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          return super.handleUnknownSyscall(emulator, NR);
27      }
28
29  @   private void vfork(Emulator<?> emulator) {
30          emulator.getUnwinder().unwind();   打印调用栈
31          EditableArm32RegisterContext context = (EditableArm32RegisterContext) emulator.getCont
32          int childPid = emulator.getPid() + ThreadLocalRandom.current().nextInt( bound: 256);
33          int r0 = childPid;
34          System.out.println("vfork pid=" + r0);
35          context.setR0(r0);
36      }
37
38  @   protected int pipe2(Emulator<?> emulator) {
39          EditableArm32RegisterContext context = (EditableArm32RegisterContext) emulator.getCont
```

运行



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。

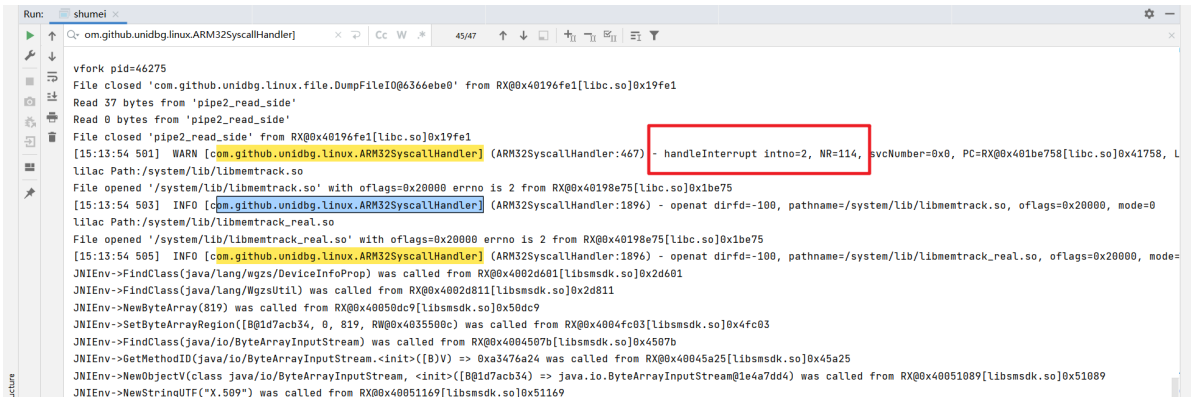
```
{
  v22 = 0;
  if ( j_strrchr(a2, 114) )
    v6 = "r";
  else
    v6 = "w";
  v21 = v6;
  if ( j_pipe2(&v23, v4) == -1 )
    return 0;
}
v18 = (int *)j_malloc(16);
if ( !v18 )
{
  j_close(v23);
  v5 = j_close(v24);
  *(_DWORD *)j___errno(v5) = 12;
  return 0;
}
v7 = j_pthread_rwlock_rdlock(&pidlist_lock);
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。

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）



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。

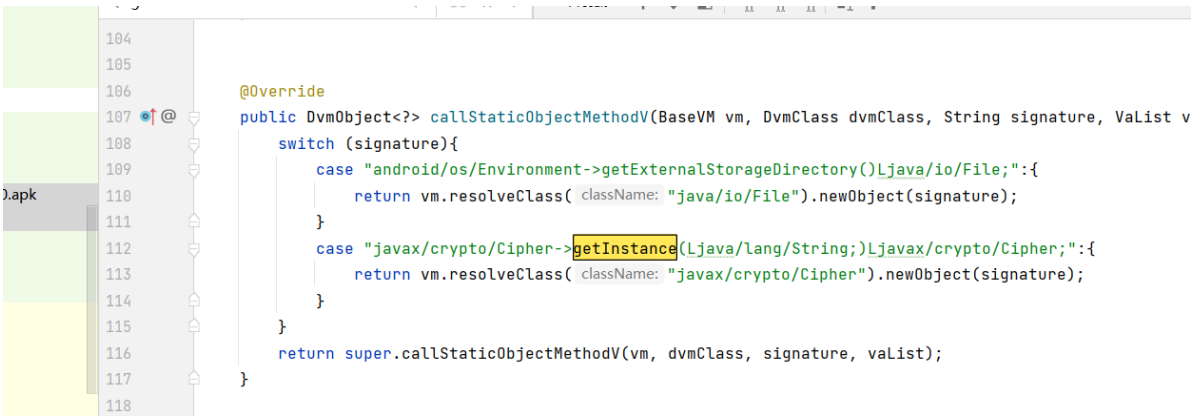
我们继续往下走，补AVA环境。

因为有JNItrace的结果，所以我们可以艺高人胆大，来看看吧

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。

运行

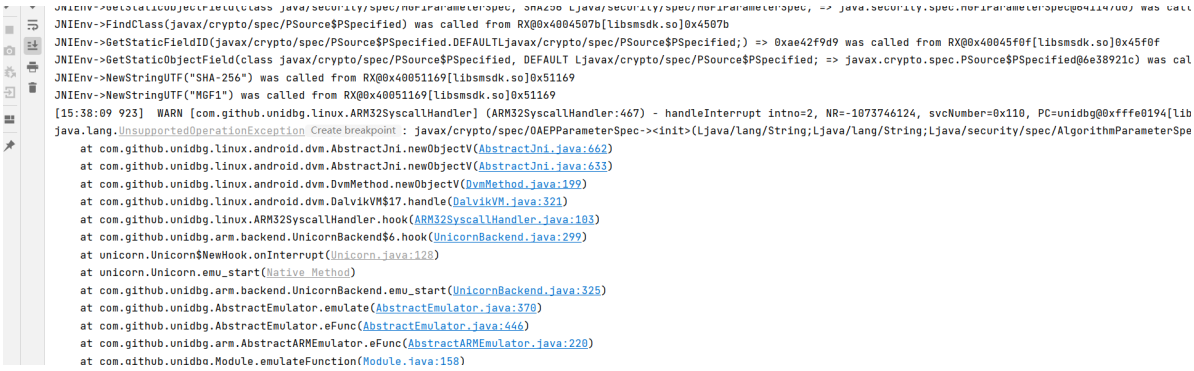
获取加密类实例？照样返回一个空对象



继续

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);
}
```



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/libsmsdk.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\":\"all\",\"a3\":\"none\",\"a4\":\"4\",\"a2\":\"SRcM3hsEtSjSE1fQv1CaresO92
5Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOCiXTuZJ+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
(v8l)\",\"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_aml_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\
":\"a58929cd0e32020053f6137261ecd3c40\",\"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\":\"3vDSuAiODgqAwBuSIqCEpuAFlJ+xKBFFJ383k
+\\/M2+M=___\",\"a68\":
[],\"a92\":\"1080,2030\",\"a93\":0,\"a95\":-1,\"a96\":\"dU56APPxOpvUizMTZXVP\",\
"a97\":\"SRcM3hsEtSjSE1fQv1CaresO925Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOC
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\":\"110010O\",\"a79\":\"\",\"a80\":\"1628128282029-12295\",\"a83\":\"1001100\",\"a85\":[],\"a69\":15533490176,\"a71\":118982303744,\"a72\":{\"temp\":370,\"vol\":4095,\"level\":85,\"scale\":100,\"status\":2},\"a70\":15684485120}";

```
        String str3 = "
{\"all_atamper\":true,\"core_atamper\":true,\"hook_java_switch\":true,\"hook_swi
tch\":false,\"risk_apps\":[{\"xposed\":
{\"pn\":\"de.robv.android.xposed.installer\",\"uri\":\"\"}},{\"controllers\":
{\"pn\":\"com.soft.controllers\",\"uri\":\"\"}},{\"apkOO8v\":
{\"pn\":\"com.soft.apkOO8v\",\"uri\":\"\"}},{\"apkOO8Tool\":
{\"pn\":\"com.soft.apkOO8Tool\",\"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\":\"\"}},{\"burgerzwsm\":
{\"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\":\"\"}},{\"a1O24mloc\":
{\"pn\":\"top.a1O24bytes.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.a1O24bytes.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\":[{\"OO8Mode\":
{\"dir\":\".system/OO8Mode\",\"type\":\"sdcard\"}},{\"OO8OK\":
{\"dir\":\".system/OO8OK\",\"type\":\"sdcard\"}},{\"OO8system\":
{\"dir\":\".system/OO8system\",\"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/i2Gv4IxR5OxSBiXKcHu8gdkDXKei9GwOBNbN6jq3x
MUlFFlAvT94COwwWhychgUggyBRjbNG1gzOdh171POb7ZnqdDPKYq5NrmMJr3Fwtzccme/nV4ROOyuTb
```

fljc3DdFUa8eOMaLkVLFfsXnxl3Jdu6ZY38LTdbc+h2fnf4KnSRbgcZ5JVFaeiKZ5HFQvKZjKJH6x/UQ
il9OPf2kpg4uRmTDh6evOEnORGh9Jg3l8Nr0xd87iZNvUg5Jg94lQ/FX98DYetR2RYe3Sp/9u+CTlEnE
SikjyMxGjAJ3R1TQ7O1LfuNwqceVsYw99YeNkCwWwTBMQII5a3/2iO9HzxRXXisWVk23TXt41xmumhs5
HDmj6D1/oeQ6oFHqSfd3C/aUbOvFrxrqbNH68H9pW/b2wpYnnAJSgYxoWaz1MaQJ5Y21IGkzZ7jSeTN2
IJFTzPsHesHc2K4QS7OSWju/d1rCrA5BXSnO5TIGXNukm2AwPEtduBeg4FpR7Lb/VIOKOcgrg4gVRPVl
QnNBr5mJI2fS3OC1sDZibJG2sZxo56BXeF8HzXDPBrO3T+Nqg77E4cynk9a57kkqOeA1RaZn8yHJWs4q
97tFrUsokRbcFwmVkYeJ5z1rbWLeVZ9fkTcyy3VIQY3E2mwR7kaAJepdSl+iDeJBHZwBKUBPJqoPoiEO
uKTnn8KmvyKJb+Jc8mYxR/mgT1rOc6Cgn6CM9BfynZrJoyTmlXzy2tm6dN66eHM5tsplzGOc3JEgvB2T
5nSyAc9XOu9/rIbsWQ/8OUNFz2pu7vBfgysWakkPKMbkSj3MsRHHZE6mljv/POrEtuNth5/KwH1JQBWW
R/lepqywjoev2fiJ5FqGTVBt6ZTESeAX+9AIUHv9nMx32sVwOVmIIjV6R8UUOa1b5EZHYCm8O4BEszx2
/ke/e+1dEvw5ntTOkHvme5HIX9QnOuZ6u+gQpJds2aVHMGOXSI67OxzhepwaMskLltU268x53PYc+rjX
NXNbkGGD+kJAISPF4d2UOtbVNFs7Cy1SIF4HK8+7FPxn6gqD4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc
sWSmmyWIQQzE9rIoUbxSFLThQMUW2tI0GfHCJVsppIQtmxx6M9bTuerjdOIi5oamMswxK3MkAyMl58lU
dO5x4ycwfouRXOoxerpjvEmT4jfJJRh86Ud/Ecihm6Fp5dm8r4Hg9nPQKebng/GjL1+/n0SOdpaq/4rQ
vIk2GWN7Q/M7BboqN7+5oU4qkcYOHaGC8H9OYpwRlhZB/IEYHgBVCePKW6bGkiPBReu72+Bmhgb5KaPN
JYLFHWcdsN9+Df7DcVpVCmnTSM56HnKLym168o8XHJIhawjajkElhsqYlsL0FOOUlEcN9OcoIPi7XQFI
Q2jk7A1qiTsIbKHtpOm49jCsomHBWqqT5kNno6WF6xiNXODhIz3diLHXHelkfWPJpnPZzq2FUgBvJOtX
+tftPYoGwIjvlu4SBeGeZ4jCfi2qkCofJm7EeMojox6BuBF3HKjUV+bUgusy5BF8qFHblazop/O++qHt
BtGkQejeqESFZWwXjhsrHja68rPaK0YDxXClitH4xS+38tFWKqgbKoVck+2uDZlauCSA0etJqfzz7Ofj
C4hwJp8WcDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiVO6e7OsayNlkppG1RW1UmGhLe5gO8WDB
IO1MGfSJMffnlgt9OnJxpWQOymcUM6tUAKSoimOaEXqsvK+SIHI/dchN6tiFaHLZesXhqXaHpbiXVqDa
D8gHN/yMR4IeY8eOohVLwPAFZIWuGPdz3bgqQBmerdLp1ZHrZCjWLsOAsKYDWWOGORjkP/YSWK+S1dLe
WadQpFAtt6X7c5DnKdmvmSXXF7a3fG7GOTk8miLwSMpgIij8Ow/oLCbUgYDGEpjGiSG6XEHPktc6ThTs
+CzC2QNgBi15g12NABEHQKxc3tzykwSpoaamWrDe8vNCuKd+TkK+q0zw66LTmE+maWX56TAQY5OMQXOr
H+6c5iULwda9Qn6rDSVNpTaN6KU6dUXDb23QYthBd2oRbq6T0Z8NLc8h6QWVA9QEG7zS9j/fz/st94Xi
tuK8jKvr13lf6bD646ixTx27NZzoQEtd2ElS/ZM/iAaxWlaohOKKO5adtDATLyL7IalvdwdQZ0XGwzuS
IKUjxDIrBOJZgCuGWg2Cj5cRLO59KfS0hgYv8rRgTa4lvJcvuhEi6VTpFbGwV+TOC7ZX3xNPmnAVDWth
UdPKu36z2wzzp89p6qRw7kOUWnN7XIgaV5Lv1Hcih7FNWLe1O7Mdvg41TprLFMLTwcCwjhLf5mrIh6et
Y5ZQp5ikVKv4VrBsOSqqFLbZoZJ4KSHyT2YzaZ7ZK5uQRf2f2u8gPYWnOOF4C8rNbbkdxAzoierX/s7m
O1AMdOBJsS1LGcl8OVljCns5u2dRqQm1rkTG5r1kO14OfTkOKnjyjqo7ZXRd7/khXS6+PWv6v3CzcdR8
ojX+7MqmZXVEsdcEHzE7gCfRl7kb1H8bTZhaQPqhO9vDLAo8RJTd2HHjYt2QvjinG8PtX57+/TBuIvPD
Wog6p8milhqzLHOuZVpbhdrUYQLHh45SbT99ydFS2J6/ZOvV84C8sE1bq//Zh3JKu74bOayGDzKjSr8u
NbDZ5sP4DMFg/ZXqnkUOnSJJVlP/DUlMfdZA+kzN8Iad/5SDEDyjmPb2yIag0uEJVjQt0qz6FeoT2h7m
MVLwBCMyl2WK+OtTXL2xEpA63Y7MfxyMj8R2DeaX6WRz96IoTlOGr8+11TsavI6EHHanMJdY94Es+s+x
OOyvJnRybbNnlqvqu4FcE+l6EeDiojoqbaczZOYS6zkPCYIDrLMIbdXjCdxq1ZCw9FQXXNVrEKfOk9PE
DmHJQ8y2hJTTyqaSVqU7imgbOPRlGBV4Eu2/r1euLftwRImZc6cfRqre9YOGaZGsNHyYh6oKl35Z1bsX
uNaGOgR/ow32s5xUaq6O26hdxdFVbWn7j3OyVJ3OrHEOGArj95DFnx2IURvMgRYrmUgwdCvmiNTLqZXf
sbfmB2kUWGKp2mWa5RWrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8YpgBS6KHhljwVwTr7ah
OCChIlaa/9y53XuoB9cDrqBmO8rj+4VFbyxkFMcHy6RhoY23OklYstQxXvdf5FjzNdbHCenVMkz8ThJU
uSP3VOuVrUHAZssuyiqocQhr8gxPsC6k4XDZohrp+Yfzq5YbLTOnv4+FmTIJ8JWZy5axUG2oACiL8LNy
pQlqmTCBixpjFM5iQKPSVdkCOTmZ8bOT+UQLa2YOXn5Thr0ktaTTN3GkeWq2DlmFktOFCQCbjIaWxY75
RtUitKcooctFQ3xUNH7s/ROyb/sXlV+8ebi6L59L3x2PCvqOEXnQ9gSirr24loYXitrxXsE1zaaVrU9Y
ZcB+a49A6O2Nrywn81dRPb5tO2mUQRp/Kg1IJPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWDnI
S+Djqn9pbhb8wroyxOFF8aEhwulo2hsgW91RwZ9umAFjEC4sSt8sc1ELaqaqWKnooKg7seVLq25b6toF
ARWgdd8yTXH7OjPniFuF+UEl43yK912LWXfM/squU/UZP97RqbWuPu+bv2bYe3hiqBkJ5xv5IOxgS6H3F
uIlpP2zyGwHGrXWOaqZ+4/npkuJ7ILAV7y1g8SOZWfc86hPyRIrV2LNa3gr0bNnUOCsfpcRwdkmBlyhn
lbGqojOiUrBkjUbYPQ4G8jzoqUJmQ5xNyH6OAQBOu7LdEDiCOHSUSI3SKzo1uESNSeE3qfV+UF87kZti
eLj+RaqhAGN9nxstGn9F3yIUb76Jl3STbwwdEUzB7X8mhij9gQVLNFBR2tgrY=\",\"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\":[]}";

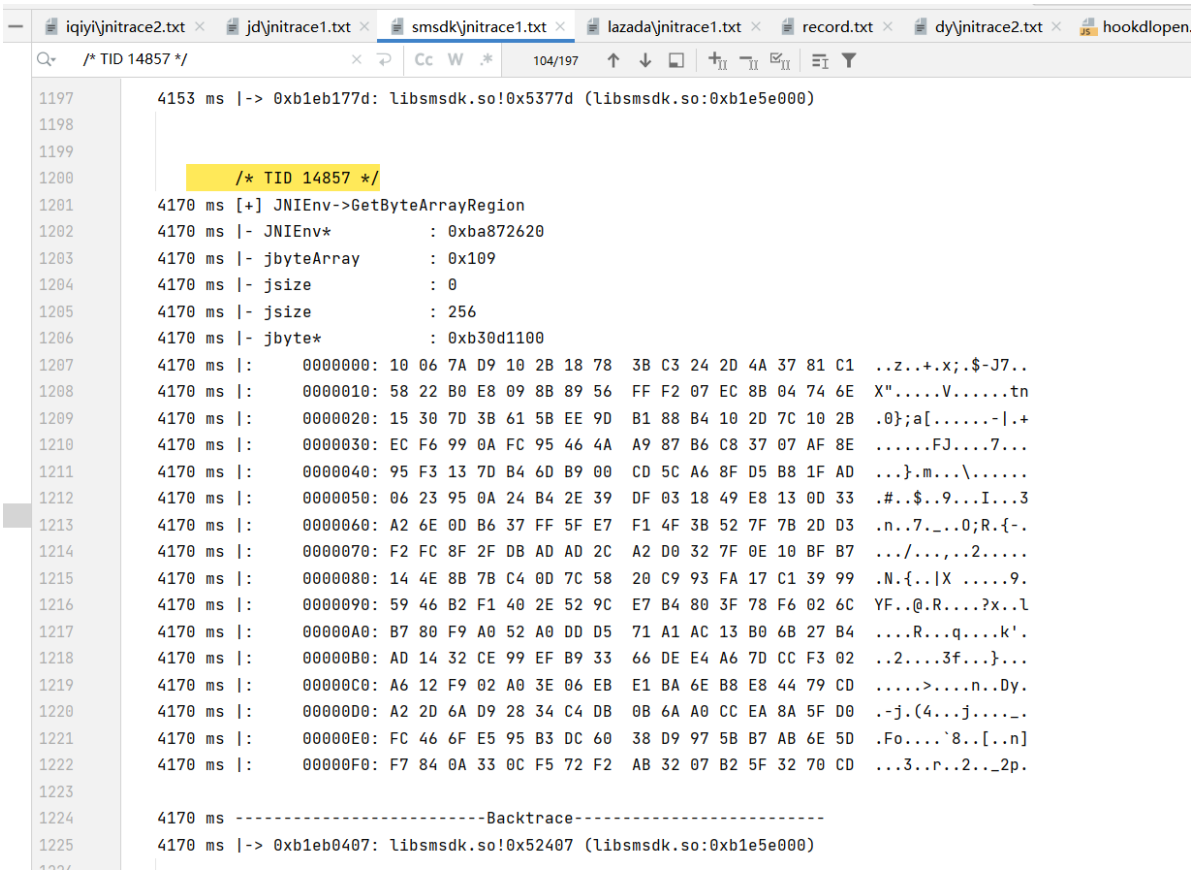
```
        String str4 =
"MIIDLzCCAhegAwIBAgIBMDANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJDTjELMAkGA1UECwwCU00
xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wHhcNMjAxMjA3MDMzMDE4WhcNNDAxMjAyMDMzMDE4WjAyMQs
wCQYDVQQGEwJDTjELMAkGA1UECwwCU00xFjAUBgNVBAMMDWUuaXNodW1laS5jb20wggEiMA0GCSqGSIb
3DQEBAQUAA4IBDwAwggEKAoIBAQCT947yNGa4EPvheGp6hsDoU4kBKvmwacn6tqfWit/jlXaZZBSPcw4
3jjxGuF4eXM4NPJJtMft/jOIIwJeExOYHDCJIqU/1pEPsXYbOlBhwD5mq34cORiRxlji+g+D4rFRO/Xr
efRJSeB3W1djvOAMkXoygp+813ZM6mzPd36zjbUIaJfzkC5LOeITUcC6Db98XiN/hNmvciWtiO1Sm9FE
U1ip1fFb9NZO4vb2Z6Xt/ti/rUVzWyshZClqqVq4s9W4iGPqfTnBsxttiooRUproe2LtB+J73kKTgJJH
6OpnOljqd+FaMsL/sddY6lggM+w4ePTe4HF+/dV2ZZp+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
ZA5/ORAVrhWrYFlnyreX4FjAfBgNVHSMEGDAWgBS83RQZA5/ORAVrhWrYFlnyreX4FjAMBgNVHRMEBTA
DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZO6fn+mH124C8Djm15jCRjYqOISpgk
gsReEX2FOOsxYqBuRPidycdsRNyQG44/i4PQrBwc9T/wLSOyHICaKbXXPhfWl4PLRNROLtgmCLoIveDy
jzTn3BEf57tZCYSmpHMUIOeJeV9o3yhluURv3Vbiqh+0ca2MqL9m7N49DkkgeZO4FAWUp9yG+p1jf5tA
1wa6t1vvH1T8TKvWjGtBH3jVYenKBk+W+DWzZnDepgOl+8BXozOOJP5U1u68Sqf+cke0BwlRfsTFU4yA
oEBsIIZ/Stx7Q82K8M4XucAFV8PTT8i3OQoGcSduEj4zape1vNn7f";
        String str5 = "dU56APPxOpvUizMTZXVP";
        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;)Ljavax/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/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);
    }

}
```

运行

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



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/libsmsdk.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\":\"all\",\"a3\":\"none\",\"a4\":\"4\",\"a2\":\"SRcM3hsEtSjSE1fQv1CaresO92
5Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOCiXTuZJ+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
(v8l)\",\"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_aml_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\
":\"a58929cd0e32020053f6137261ecd3c40\",\"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\":\"3vDSuAiODgqAwBuSIqCEpuAFlJ+xKBFFJ383k
+\\/M2+M=___\",\"a68\":
[],\"a92\":\"1080,2030\",\"a93\":0,\"a95\":-1,\"a96\":\"dU56APPxOpvUizMTZXVP\",\
"a97\":\"SRcM3hsEtSjSE1fQv1CaresO925Tis1PYZFK58Ez2MNqdhO6kORLGaCyM8NldbOl4bFXZOC
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\":\"110010O\",\"a79\":\"\",\"a80\":\"1628128282029-12295\",\"a83\":\"1001100\",\"a85\":[],\"a69\":15533490176,\"a71\":118982303744,\"a72\":{\"temp\":370,\"vol\":4095,\"level\":85,\"scale\":100,\"status\":2},\"a70\":15684485120}";

```
        String str3 = "
{\"all_atamper\":true,\"core_atamper\":true,\"hook_java_switch\":true,\"hook_swi
tch\":false,\"risk_apps\":[{\"xposed\":
{\"pn\":\"de.robv.android.xposed.installer\",\"uri\":\"\"}},{\"controllers\":
{\"pn\":\"com.soft.controllers\",\"uri\":\"\"}},{\"apkOO8v\":
{\"pn\":\"com.soft.apkOO8v\",\"uri\":\"\"}},{\"apkOO8Tool\":
{\"pn\":\"com.soft.apkOO8Tool\",\"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\":\"\"}},{\"burgerzwsm\":
{\"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\":\"\"}},{\"a1O24mloc\":
{\"pn\":\"top.a1O24bytes.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.a1O24bytes.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\":[{\"OO8Mode\":
{\"dir\":\".system/OO8Mode\",\"type\":\"sdcard\"}},{\"OO8OK\":
{\"dir\":\".system/OO8OK\",\"type\":\"sdcard\"}},{\"OO8system\":
{\"dir\":\".system/OO8system\",\"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/i2Gv4IxR5OxSBiXKcHu8gdkDXKei9GwOBNbN6jq3x
MUlFFlAvT94COwwWhychgUggyBRjbNG1gzOdh171POb7ZnqdDPKYq5NrmMJr3Fwtzccme/nV4ROOyuTb
```

fljc3DdFUa8eOMaLkVLFfsXnxl3Jdu6ZY38LTdbc+h2fnf4KnSRbgcZ5JVFaeiKZ5HFQvKZjKJH6x/UQ
il9OPf2kpg4uRmTDh6evOEnORGh9Jg3l8Nr0xd87iZNvUg5Jg94lQ/FX98DYetR2RYe3Sp/9u+CTlEnE
SikjyMxGjAJ3R1TQ7O1LfuNwqceVsYw99YeNkCwWwTBMQII5a3/2iO9HzxRXXisWVk23TXt41xmumhs5
HDmj6D1/oeQ6oFHqSfd3C/aUbOvFrxrqbNH68H9pW/b2wpYnnAJSgYxoWaz1MaQJ5Y21IGkzZ7jSeTN2
IJFTzPsHesHc2K4QS7OSWju/d1rCrA5BXSnO5TIGXNukm2AwPEtduBeg4FpR7Lb/VIOKOcgrg4gVRPVl
QnNBr5mJI2fS3OC1sDZibJG2sZxo56BXeF8HzXDPBrO3T+Nqg77E4cynk9a57kkqOeA1RaZn8yHJWs4q
97tFrUsokRbcFwmVkYeJ5z1rbWLeVZ9fkTcyy3VIQY3E2mwR7kaAJepdSl+iDeJBHZwBKUBPJqoPoiEO
uKTnn8KmvyKJb+Jc8mYxR/mgT1rOc6Cgn6CM9BfynZrJoyTmlXzy2tm6dN66eHM5tsplzGOc3JEgvB2T
5nSyAc9XOu9/rIbsWQ/8OUNFz2pu7vBfgysWakkPKMbkSj3MsRHHZE6mljv/POrEtuNth5/KwH1JQBWW
R/lepqywjoev2fiJ5FqGTVBt6ZTESeAX+9AIUHv9nMx32sVwOVmIIjV6R8UUOa1b5EZHYCm8O4BEszx2
/ke/e+1dEvw5ntTOkHvme5HIX9QnOuZ6u+gQpJds2aVHMGOXSI67OxzhepwaMskLltU268x53PYc+rjX
NXNbkGGD+kJAISPF4d2UOtbVNFs7Cy1SIF4HK8+7FPxn6gqD4bG+5BK5QLH6x2CUPkIn0LpaScvt4nvc
sWSmmyWIQQzE9rIoUbxSFLThQMUW2tI0GfHCJVsppIQtmxx6M9bTuerjdOIi5oamMswxK3MkAyMl58lU
dO5x4ycwfouRXOoxerpjvEmT4jfJJRh86Ud/Ecihm6Fp5dm8r4Hg9nPQKebng/GjL1+/n0SOdpaq/4rQ
vIk2GWN7Q/M7BboqN7+5oU4qkcYOHaGC8H9OYpwRlhZB/IEYHgBVCePKW6bGkiPBReu72+Bmhgb5KaPN
JYLFHWcdsN9+Df7DcVpVCmnTSM56HnKLym168o8XHJIhawjajkElhsqYlsL0FOOUlEcN9OcoIPi7XQFI
Q2jk7A1qiTsIbKHtpOm49jCsomHBWqqT5kNno6WF6xiNXODhIz3diLHXHelkfWPJpnPZzq2FUgBvJOtX
+tftPYoGwIjvlu4SBeGeZ4jCfi2qkCofJm7EeMojox6BuBF3HKjUV+bUgusy5BF8qFHblazop/O++qHt
BtGkQejeqESFZWwXjhsrHja68rPaK0YDxXClitH4xS+38tFWKqgbKoVck+2uDZlauCSA0etJqfzz7Ofj
C4hwJp8WcDPvdxdQFC4ZX+gQr7VeQyBITYmMqW9x+kFtI7YiVO6e7OsayNlkppG1RW1UmGhLe5gO8WDB
IO1MGfSJMffnlgt9OnJxpWQOymcUM6tUAKSoimOaEXqsvK+SIHI/dchN6tiFaHLZesXhqXaHpbiXVqDa
D8gHN/yMR4IeY8eOohVLwPAFZIWuGPdz3bgqQBmerdLp1ZHrZCjWLsOAsKYDWWOGORjkP/YSWK+S1dLe
WadQpFAtt6X7c5DnKdmvmSXXF7a3fG7GOTk8miLwSMpgIij8Ow/oLCbUgYDGEpjGiSG6XEHPktc6ThTs
+CzC2QNgBi15g12NABEHQKxc3tzykwSpoaamWrDe8vNCuKd+TkK+q0zw66LTmE+maWX56TAQY5OMQXOr
H+6c5iULwda9Qn6rDSVNpTaN6KU6dUXDb23QYthBd2oRbq6T0Z8NLc8h6QWVA9QEG7zS9j/fz/st94Xi
tuK8jKvr13lf6bD646ixTx27NZzoQEtd2ElS/ZM/iAaxWlaohOKKO5adtDATLyL7IalvdwdQZ0XGwzuS
IKUjxDIrBOJZgCuGWg2Cj5cRLO59KfS0hgYv8rRgTa4lvJcvuhEi6VTpFbGwV+TOC7ZX3xNPmnAVDWth
UdPKu36z2wzzp89p6qRw7kOUWnN7XIgaV5Lv1Hcih7FNWLe1O7Mdvg41TprLFMLTwcCwjhLf5mrIh6et
Y5ZQp5ikVKv4VrBsOSqqFLbZoZJ4KSHyT2YzaZ7ZK5uQRf2f2u8gPYWnOOF4C8rNbbkdxAzoierX/s7m
O1AMdOBJsS1LGcl8OVljCns5u2dRqQm1rkTG5r1kO14OfTkOKnjyjqo7ZXRd7/khXS6+PWv6v3CzcdR8
ojX+7MqmZXVEsdcEHzE7gCfRl7kb1H8bTZhaQPqhO9vDLAo8RJTd2HHjYt2QvjinG8PtX57+/TBuIvPD
Wog6p8milhqzLHOuZVpbhdrUYQLHh45SbT99ydFS2J6/ZOvV84C8sE1bq//Zh3JKu74bOayGDzKjSr8u
NbDZ5sP4DMFg/ZXqnkUOnSJJVlP/DUlMfdZA+kzN8Iad/5SDEDyjmPb2yIag0uEJVjQt0qz6FeoT2h7m
MVLwBCMyl2WK+OtTXL2xEpA63Y7MfxyMj8R2DeaX6WRz96IoTlOGr8+11TsavI6EHHanMJdY94Es+s+x
OOyvJnRybbNnlqvqu4FcE+l6EeDiojoqbaczZOYS6zkPCYIDrLMIbdXjCdxq1ZCw9FQXXNVrEKfOk9PE
DmHJQ8y2hJTTyqaSVqU7imgbOPRlGBV4Eu2/r1euLftwRImZc6cfRqre9YOGaZGsNHyYh6oKl35Z1bsX
uNaGOgR/ow32s5xUaq6O26hdxdFVbWn7j3OyVJ3OrHEOGArj95DFnx2IURvMgRYrmUgwdCvmiNTLqZXf
sbfmB2kUWGKp2mWa5RWrzDGKjQQ9wTuV2ZLI3qDmKN4RkLT5z6lZ8n9rLFCv8YpgBS6KHhljwVwTr7ah
OCChIlaa/9y53XuoB9cDrqBmO8rj+4VFbyxkFMcHy6RhoY23OklYstQxXvdf5FjzNdbHCenVMkz8ThJU
uSP3VOuVrUHAZssuyiqocQhr8gxPsC6k4XDZohrp+Yfzq5YbLTOnv4+FmTIJ8JWZy5axUG2oACiL8LNy
pQlqmTCBixpjFM5iQKPSVdkCOTmZ8bOT+UQLa2YOXn5Thr0ktaTTN3GkeWq2DlmFktOFCQCbjIaWxY75
RtUitKcooctFQ3xUNH7s/ROyb/sXlV+8ebi6L59L3x2PCvqOEXnQ9gSirr24loYXitrxXsE1zaaVrU9Y
ZcB+a49A6O2Nrywn81dRPb5tO2mUQRp/Kg1IJPSr5tcc36yGVYwmVcnOUqmMrgeNQT5QUBH7LEmQWDnI
S+Djqn9pbhb8wroyxOFF8aEhwulo2hsgW91RwZ9umAFjEC4sSt8sc1ELaqaqWKnooKg7seVLq25b6toF
ARWgdd8yTXH7OjPniFuF+UEl43yK912LWXfM/squU/UZP97RqbWuPu+bv2bYe3hiqBkJ5xv5IOxgS6H3F
uIlpP2zyGwHGrXWOaqZ+4/npkuJ7ILAV7y1g8SOZWfc86hPyRIrV2LNa3gr0bNnUOCsfpcRwdkmBlyhn
lbGqojOiUrBkjUbYPQ4G8jzoqUJmQ5xNyH6OAQBOu7LdEDiCOHSUSI3SKzo1uESNSeE3qfV+UF87kZti
eLj+RaqhAGN9nxstGn9F3yIUb76Jl3STbwwdEUzB7X8mhij9gQVLNFBR2tgrY=\",\"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/jOIIwJeExOYHDCJIqU/1pEPsXYbOlBhwD5mq34cORiRxlji+g+D4rFRO/Xr
efRJSeB3W1djvOAMkXoygp+813ZM6mzPd36zjbUIaJfzkC5LOeITUcC6Db98XiN/hNmvciWtiO1Sm9FE
U1ip1fFb9NZO4vb2Z6Xt/ti/rUVzWyshZClqqVq4s9W4iGPqfTnBsxttiooRUproe2LtB+J73kKTgJJH
6OpnOljqd+FaMsL/sddY6lggM+w4ePTe4HF+/dV2ZZp+w+8AtAgMBAAGjUDBOMB0GA1UdDgQWBBS83RQ
ZA5/ORAVrhWrYFlnyreX4FjAfBgNVHSMEGDAWgBS83RQZA5/ORAVrhWrYFlnyreX4FjAMBgNVHRMEBTA
DAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCAayqoRv2uOwKT3mrkkZO6fn+mH124C8Djm15jCRjYqOISpgk
gsReEX2FOOsxYqBuRPidycdsRNyQG44/i4PQrBwc9T/wLSOyHICaKbXXPhfWl4PLRNROLtgmCLoIveDy
jzTn3BEf57tZCYSmpHMUIOeJeV9o3yhluURv3Vbiqh+0ca2MqL9m7N49DkkgeZO4FAWUp9yG+p1jf5tA
1wa6t1vvH1T8TKvWjGtBH3jVYenKBk+W+DWzZnDepgOl+8BXozOOJP5U1u68Sqf+cke0BwlRfsTFU4yA
oEBsIIZ/Stx7Q82K8M4XucAFV8PTT8i3OQoGcSduEj4zape1vNn7f";
        String str5 = "dU56APPxOpvUizMTZXVP";
        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;)Ljavax/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
6db9000cd5ca68fd5b81fad0623950a24b42e39df031849e8130d33a26e0db637ff5fe7f14f3b527f
7b2dd3f2fc8f2fdbadad2ca2d0327f0e10bfb7144e8b7bc40d7c5820c993fa17c139995946b2f140
2e529ce7b4803f78f6026cb780f9a052a0ddd571a1ac13b06b27b4ad1432ce99efb93366dee4a67d
ccf302a612f902a03e06ebe1ba6eb8e84479cda22d6ad92834c4db0b6aa0ccea8a5fd0fc466fe595
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);
    }

}
```

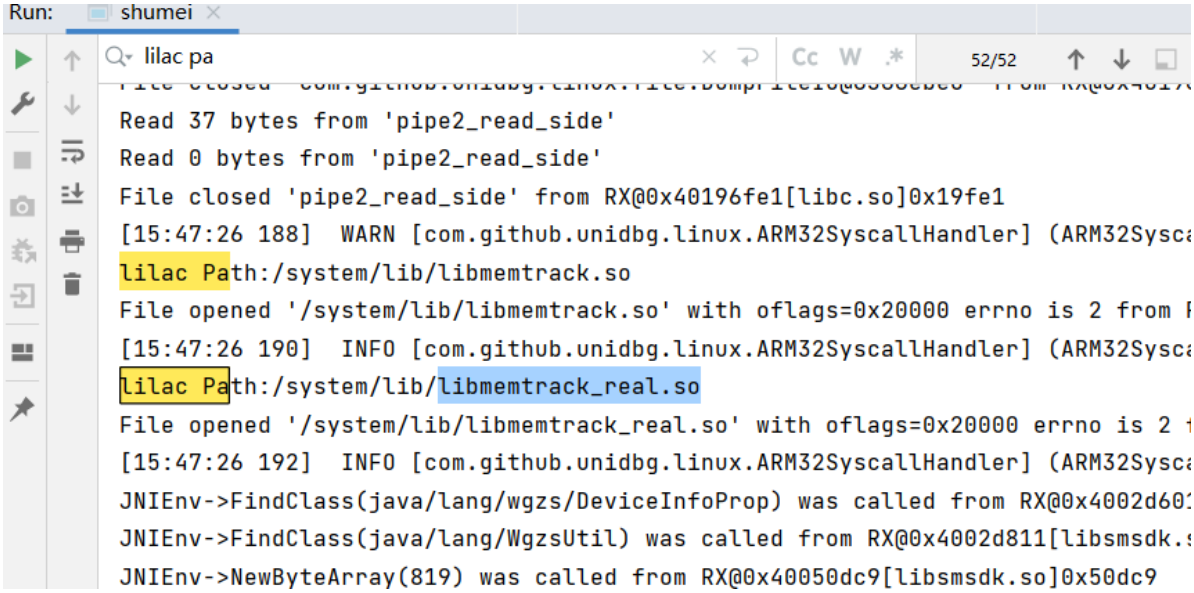
出结果了，但这里我们不验证它的对错，学习和研究Unidbg才是我们的重心。

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，我们还是塞给它空气，顺便给了他一个"你饱了"的信号，大概就是这回事儿。

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，那可以这么去做，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



这两个文件是Riru的特征文件，Riru是啥?