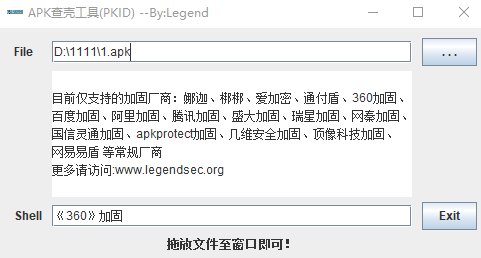
**hook星火im取sign加密方式**

1.通过黄鸟抓取http请求发现存在sign



2.发现改apk存在360加固



3.通过脚本hook脱壳

Frida配置 自行百度

项目地址:

<https://github.com/GuoQiang1993/Frida-Apk-Unpack>

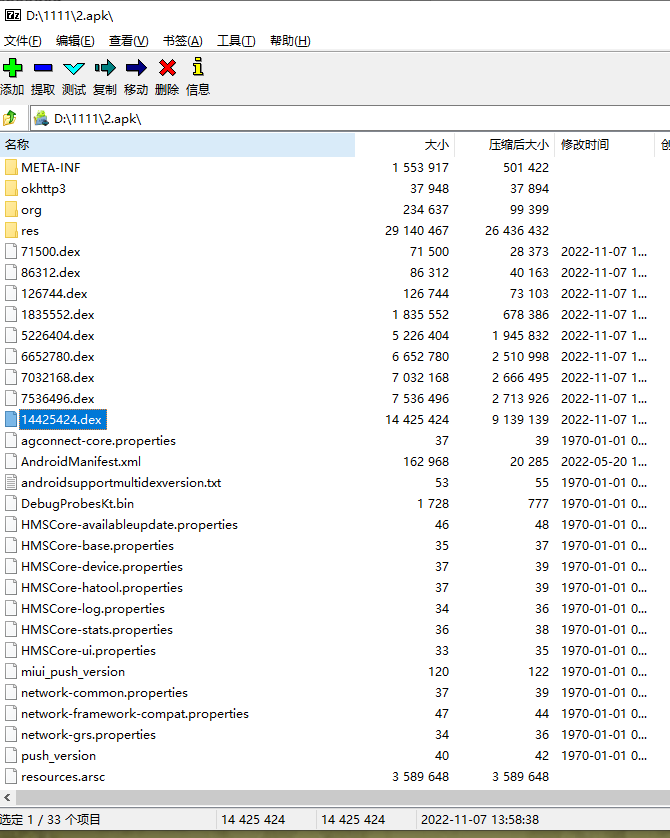
使用方法:

frida -U -f com.xxx.xxx -l dumpDex.js --no-pause

4.从Android设备push到本机并且解压到xxxx.apk包里

Adb push /xxxx/xxx.zip ./

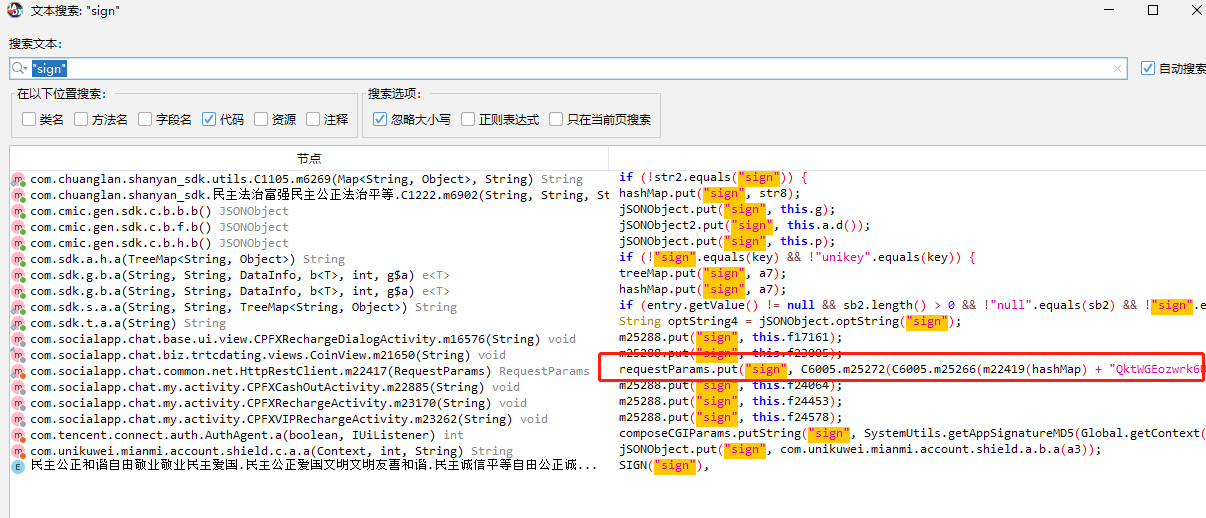




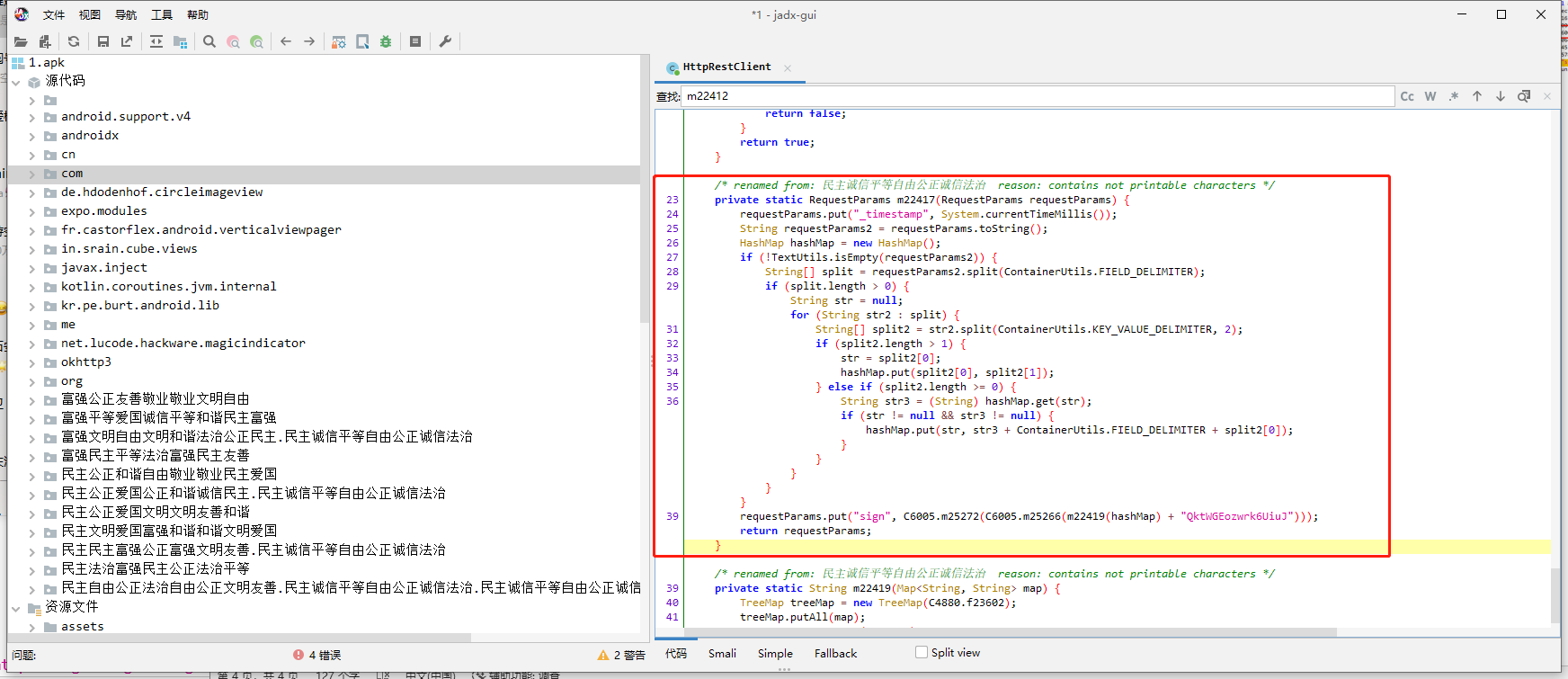
5.通过jadx反编译apk包

工具地址（注意下载-with-jre-win版本的）:

<https://github.com/skylot/jadx/>



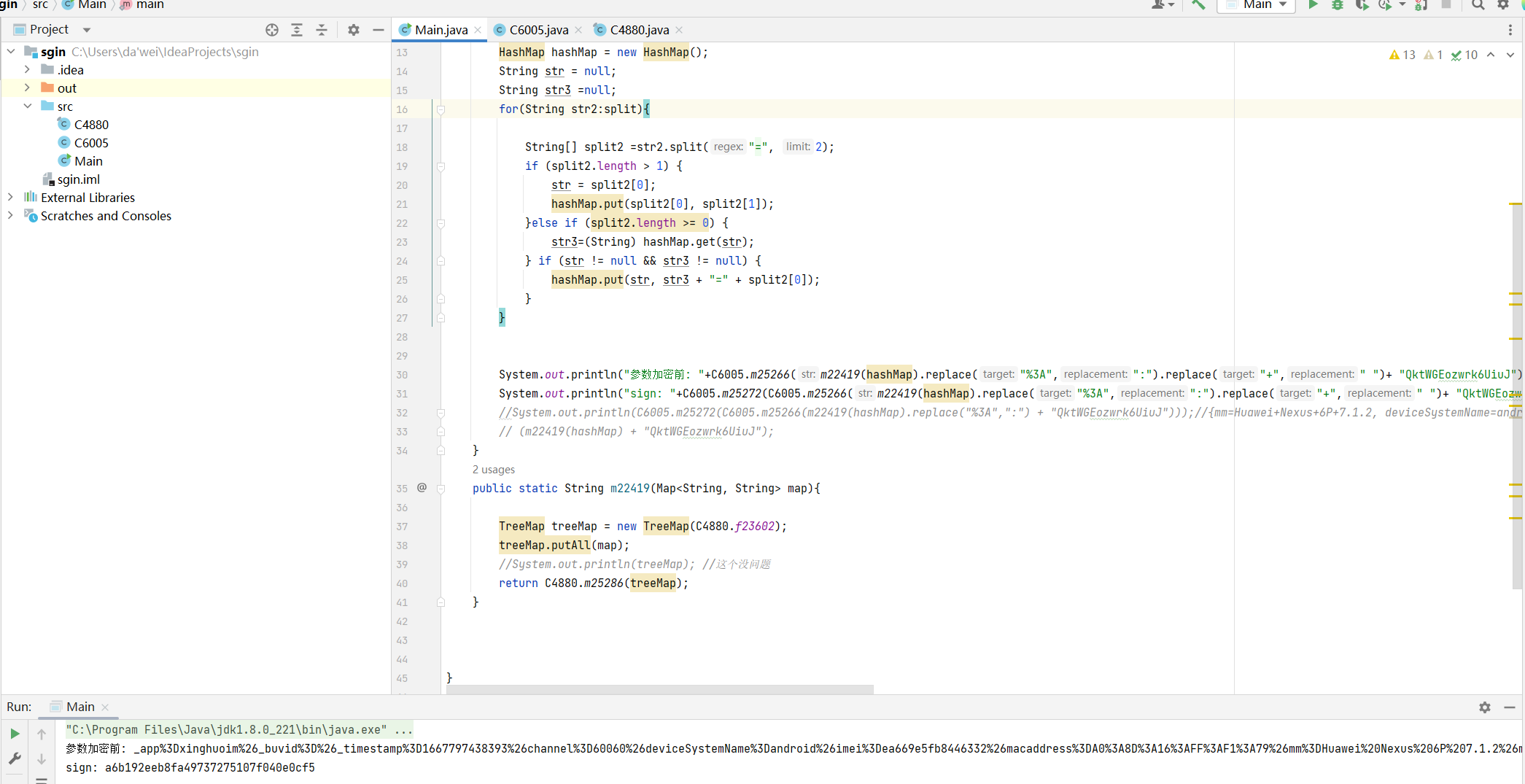
通过搜索关键字”sign”进行查询



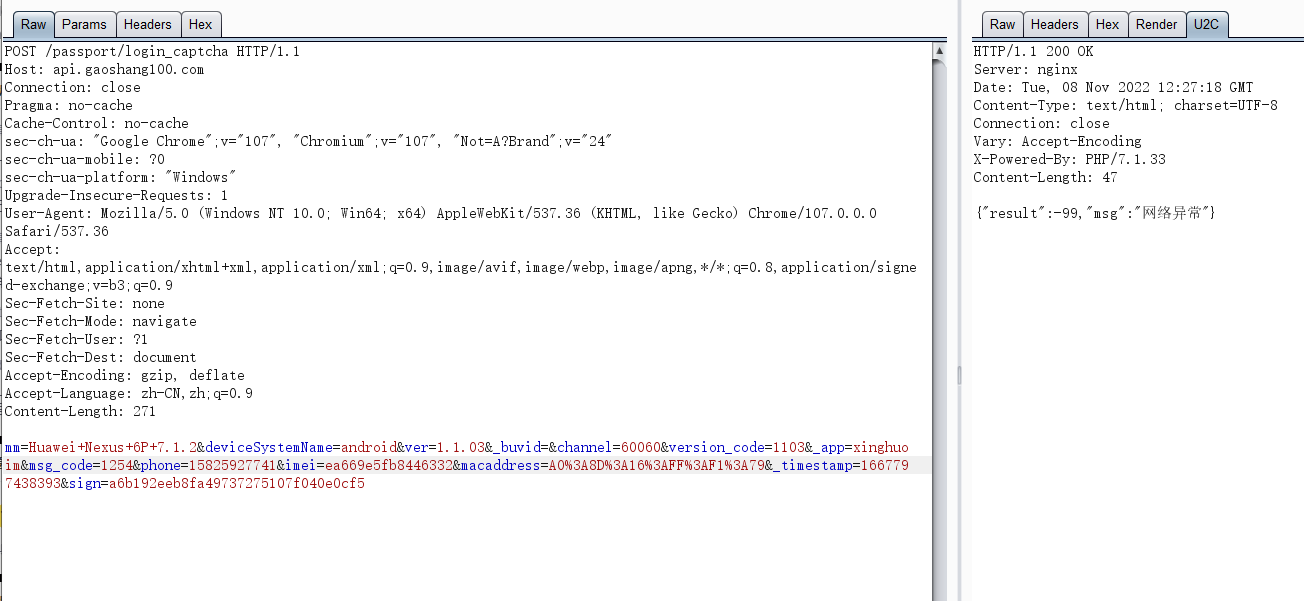
大概意思就是通过requestParams发包的时候把每个参数取出来然后进行cmd5加密最后赋值给sign上

我们可以通过代码进行重写然后达到二次解密的效果（分析过程就是一个函数一个函数的去重新出来 最好通过Android idea来写很多包可以直接使用这里使用的java重写的）

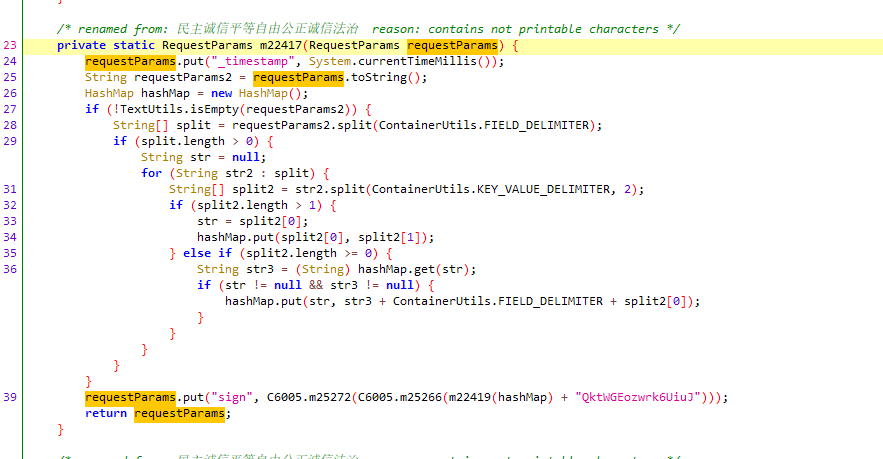
如下



然后我们就可以随便修改参数值了然后再生成新的sign



6.脚本写好后你会发现你加密的和app的不一样;为啥会这样就是因为我们不知道它Params是怎么传递如果直抓包那要就可以成功但是有很多小问题我们还是需要hook这个apk的函数来获取参数才能知道具体的





7. hook脚本和各种获取加密的办法

Frida官网指南:

<https://frida.re/docs/examples/android/>

Frida文章:

<https://www.bilibili.com/video/BV1C34y157M5/>

https://www.bilibili.com/video/BV12t4y1t7aj

<https://www.bilibili.com/video/av92571713/>

<https://github.com/smartdone/Frida-Scripts/tree/master/shell>

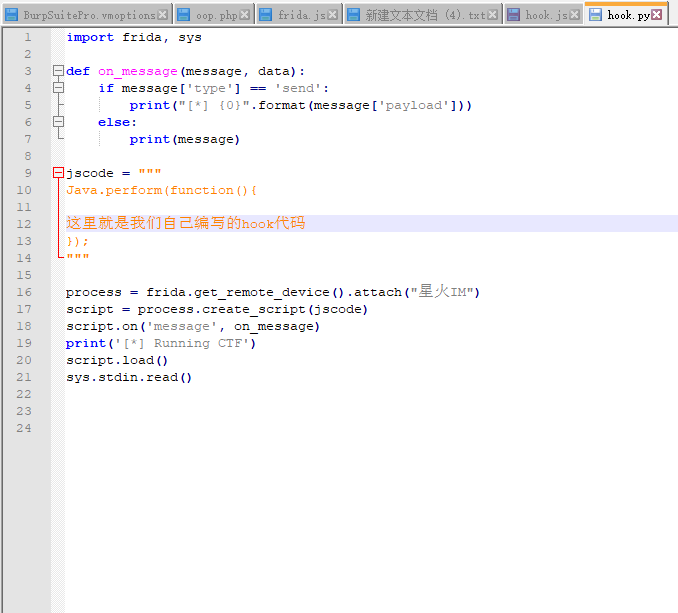
<https://blog.csdn.net/m0_54352040/article/details/115734161>

<https://xz.aliyun.com/t/8211>

<https://bbs.pediy.com/thread-249602.htm>

https://github.com/xiaokanghub/Android

copy一份他的默认代码



第一种自己分析代码编写hook：

手机打开你要抓的apk 然后通过cmd命令操作

adb shell(通过adb shell连接手机命令终端)

su (提为root权限)

cd /data/local/tmp/ (看你把frida-server放在那个目录)

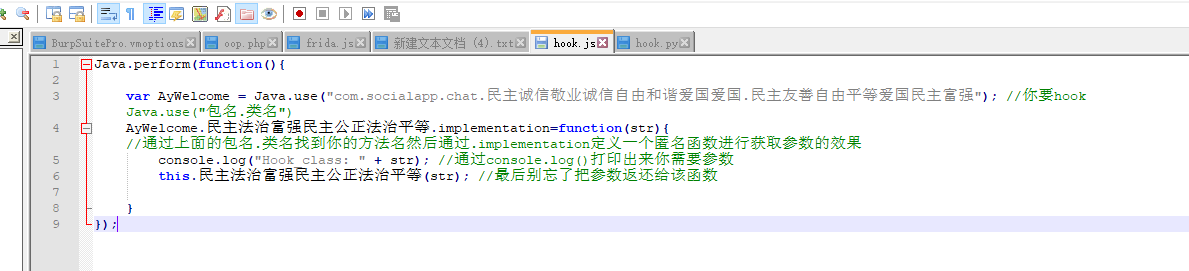
./frida-server(第一次记得chmod 777 加权限)

adb forward tcp:27042 tcp:27042(端口转发)

adb forward tcp:27043 tcp:27043(端口转发)

1. 把自己写好的hook代码放在js文件里面如下:

frida -R -f com.xinghuoim.app(包名) -l hook.js(hook文件名)



2.通过直接运行python脚本如下：

Python hook.py



Java.perform(function(){

var AyWelcome = Java.use("com.socialapp.chat.民主诚信敬业诚信自由和谐爱国爱国.民主友善自由平等爱国民主富强"); //你要hook Java.use("包名.类名")

AyWelcome.民主法治富强民主公正法治平等.implementation=function(str){ //通过上面的包名.类名找到你的方法名然后通过.implementation定义一个匿名函数进行获取参数的效果

console.log("Hook\_class: " + str); //通过console.log()打印出来你需要参数

this.民主法治富强民主公正法治平等(str); //最后别忘了把参数返还给该函数

}

});

注意注意注意:

package com.socialapp.chat.民主诚信敬业诚信自由和谐爱国爱国;

/\* compiled from: Utils.java \*/

/\* renamed from: com.socialapp.chat.民主诚信敬业诚信自由和谐爱国爱国.民主友善自由平等爱国民主富强 reason: contains not printable characters \*/

/\* loaded from: 7536496.dex \*/

public class C6005 {

}

假类名："C6005"

真类名："民主友善自由平等爱国民主富强"

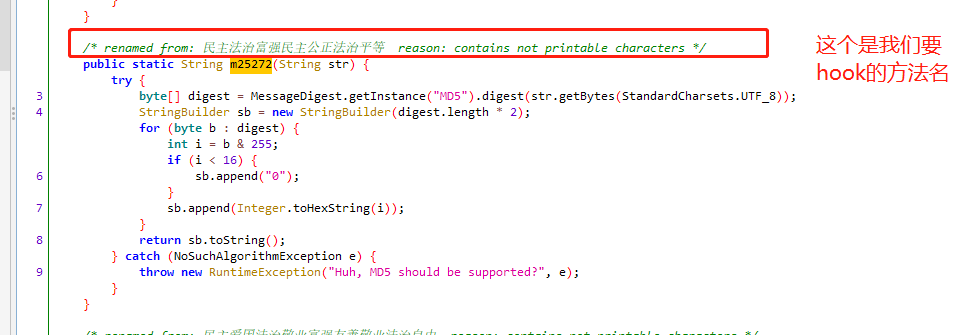
/\* renamed from: 民主法治富强民主公正法治平等 reason: contains not printable characters \*/

public static String m25272(String str) {

}

假函数名："m25272"

真函数名："民主法治富强民主公正法治平等"



第二种通过图形化通杀算法插件：

项目地址:

<https://github.com/dqzg12300/fridaUiTools>

手机打开你要抓的apk 然后通过cmd命令操作

adb shell(通过adb shell连接手机命令终端)

su (提为root权限)

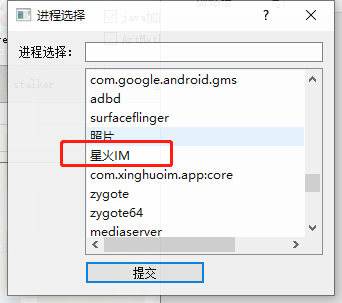
cd /data/local/tmp/ (看你把frida-server放在那个目录)

./frida-server(第一次记得chmod 777 加权限)

然后通过软件的目录应用信息 刷新查看是否连接成功如如下所示:

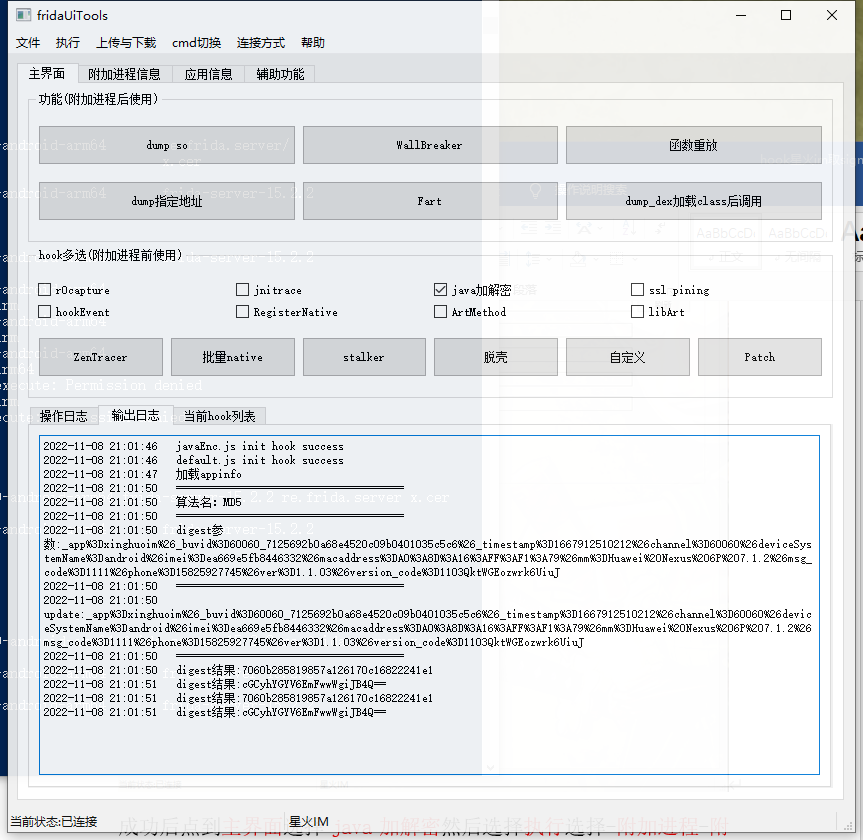


成功后回到主界面选择java加解密然后选择执行选择-附加进程-附加指定进程然后会弹出一个选择框选择你需要hook的apk包名如下:



就可以成功获取到

\_app%3Dxinghuoim%26\_buvid%3D60060\_7125692b0a68e4520c09b0401035c5c6%26\_timestamp%3D1667912522672%26deviceSystemName%3Dandroid%26imei%3Dea669e5fb8446332%26macaddress%3DA0%3A8D%3A16%3AFF%3AF1%3A79%26mm%3DHuawei%20Nexus%206P%207.1.2%26ver%3D1.1.03%26version\_code%3D1103QktWGEozwrk6UiuJ



3.第三种通过xposed+inspeckage(没有复现)傻瓜式

视频地址：

https://www.bilibili.com/video/BV1Kp4y1s7F1

工具地址：

Xposed(3.1.5)下载地址

<https://forum.xda-developers.com/attachments/xposedinstaller_3-1-5-apk.4393082/>

inspeckage

https://github.com/ac-pm/Inspeckage