

电子取证

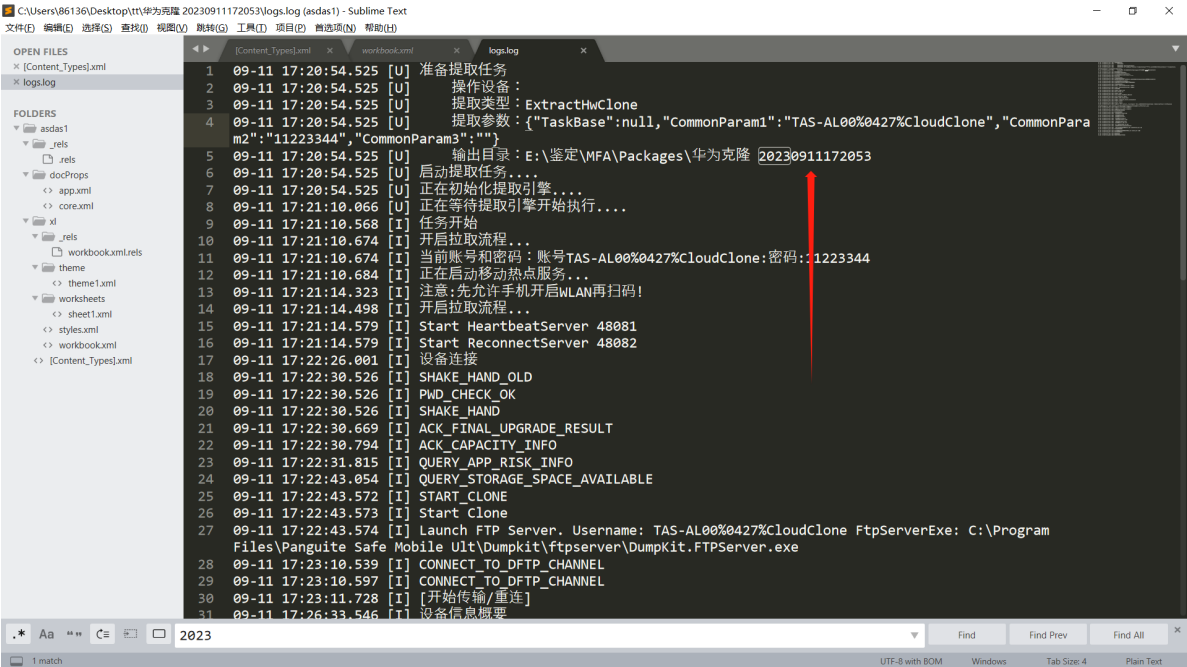
案例说明

- 1案情：2023年初，某地公安机关抓获一个网络诈骗技术嫌疑人，公安机关在扣押嫌疑人后，对嫌疑人手机进行数据提取，在提取完成分析发现嫌疑人将通话记录及短信记录进行了删除，根据嫌疑人交代，其在删除通话及短信记录前使用过同伙编写的测试软件，该安卓程序会读取通话及短信记录并存储到手机中。由于通话和短信记录对案件很重要，请参赛队员分析手机镜像及对应apk，完成取证题目

检材提取时间

检材数据开始提取是今年什么时候？（答案格式：04-12 13:26）

- 109-11 17:20



SD卡大小

嫌疑人手机SD卡存储空间一共多少GB？（答案格式：22.5）

- 124.32

盘古石手机取证分析系统

案卷中心

智能提取

工具箱

公告

工具(T)

设置(S)

帮助(H)

关于(A)

案件管理

案件202309160...

新建任务 20230916093705 (6697/1)

数据库 (94/0)

图片 (125/0)

音频 (24/0)

华为克隆 20230911172053 (69/0)

华为克隆 202309111720...

新建任务 20230916093705 (7783/1)

文件系统 (5849/0)

华为克隆 20230911172053 (69/0)

华为克隆 20230911172053... (70/0)

HuaweiBackup (110/0)

sdcard.zip (5600/0)

标签 (0/0)

截屏验证 (0/0)

仿真数据源 (0/0)

云数据源 (0/0)

分类数据 (1514/1)

数据文件 (1086/0)

图片 (125/0)

音频 (24/0)

压缩 (16/0)

文本 (786/0)

数据库 (94/0)

配置 (41/0)

通讯录 (2/0)

位置信息 (2/0)

位置聚合 (2/0)

应用列表 (411/1)

应用列表 (411/1)

多媒体 (13/0)

缩略图 (5/0)

照片 (8/0)

应用数据 (420/0)

基础数据 (420/0)

电量使用 (8/0)

流量使用 (207/0)

应用日志 (205/0)

华为克隆 20230911172053... (69/0)

稳定版 R7.5.3.5P4.46

高性能

逻辑处理: 12 核

CPU:

内存 8G:

已连接设备: 0 个

新建任务 20230916093705

导出给设备信息

编辑给设备信息

给设备信息

给设备名称: 新建任务 20230916093705

给设备编号: 2023/9/16 上午9:37:05

给设备平台: Android

给设备类型: 手机型号1

给设备型号: 手机型号2

给设备IMEI: IMEI1

给设备备注: IMEI2

路径信息

给设备路径: C:\MFA\Cases\案件20230916093705\新建任务 2...

数据路径: C:\Users\86136\Desktop\...\C:\Users\86136\Desktop\...\C:\Users\86136\Desktop\...\C:\Users\86136\Desktop\...

设备信息

品牌: Google

本地化代码: zh-Hans-CN

设备名称: sailfish

CPU架构: ["arm64-v8a","armeabi-v7a","armeabi"]

是否Root: 是

空闲的磁盘空间: 16.11 GB

基带版本: 16.11 GB

设备ID: sailfish

序列号: FGA680312283

内核版本: 3.18.137

ICCID2: 3.18.137

型号: Pixel

运营商: 运营商

手机号: 352531082716257

时区: Asia/Shanghai

日志文件系统: ext4

蓝牙物理地址: AC:37:43:8D:32:EB

硬件平台: sailfish

SDK版本: 29

WLANMac地址: AC:37:43:53:37:30

鸿蒙版本: 鸿蒙版本

Mtp序列号: FGA680312283

补丁时间: 2019-09-05

系统版本: 10.0.0

MEID: 35253108271625

总的磁盘空间: 24.32 GB

加密: FBE

Boardid: sailfish

IMSI: 460024082819284

安卓ID: 70ec24580a585a56

ICCID: 70ec24580a585a56

存储: /storage/emulated/0

设备名称

嫌疑人手机设备名称是？（答案格式：adfer）

1 | sailfish

盘古石手机取证分析系统

案卷中心

智能提取

工具箱

公告

工具(T)

设置(S)

帮助(H)

关于(A)

案件管理

案件202309160...

新建任务 20230916093705 (6697/1)

数据库 (94/0)

图片 (125/0)

音频 (24/0)

华为克隆 20230911172053 (69/0)

华为克隆 202309111720...

新建任务 20230916093705 (7783/1)

文件系统 (5849/0)

华为克隆 20230911172053 (69/0)

华为克隆 20230911172053... (70/0)

HuaweiBackup (110/0)

sdcard.zip (5600/0)

标签 (0/0)

截屏验证 (0/0)

仿真数据源 (0/0)

云数据源 (0/0)

分类数据 (1514/1)

数据文件 (1086/0)

图片 (125/0)

音频 (24/0)

压缩 (16/0)

文本 (786/0)

数据库 (94/0)

配置 (41/0)

通讯录 (2/0)

位置信息 (2/0)

位置聚合 (2/0)

应用列表 (411/1)

应用列表 (411/1)

多媒体 (13/0)

缩略图 (5/0)

照片 (8/0)

应用数据 (420/0)

基础数据 (420/0)

电量使用 (8/0)

流量使用 (207/0)

应用日志 (205/0)

华为克隆 20230911172053... (69/0)

稳定版 R7.5.3.5P4.46

高性能

逻辑处理: 12 核

CPU:

内存 8G:

已连接设备: 0 个

新建任务 20230916093705

导出给设备信息

编辑给设备信息

给设备信息

给设备名称: 新建任务 20230916093705

给设备编号: 2023/9/16 上午9:37:05

给设备平台: Android

给设备类型: 手机型号1

给设备型号: 手机型号2

给设备IMEI: IMEI1

给设备备注: IMEI2

路径信息

给设备路径: C:\MFA\Cases\案件20230916093705\新建任务 2...

数据路径: C:\Users\86136\Desktop\...\C:\Users\86136\Desktop\...\C:\Users\86136\Desktop\...\C:\Users\86136\Desktop\...

设备信息

品牌: Google

本地化代码: zh-Hans-CN

设备名称: sailfish

CPU架构: ["arm64-v8a","armeabi-v7a","armeabi"]

是否Root: 是

空闲的磁盘空间: 16.11 GB

基带版本: 16.11 GB

设备ID: sailfish

序列号: FGA680312283

内核版本: 3.18.137

ICCID2: 3.18.137

型号: Pixel

运营商: 运营商

手机号: 352531082716257

时区: Asia/Shanghai

日志文件系统: ext4

蓝牙物理地址: AC:37:43:8D:32:EB

硬件平台: sailfish

SDK版本: 29

WLANMac地址: AC:37:43:53:37:30

鸿蒙版本: 鸿蒙版本

Mtp序列号: FGA680312283

补丁时间: 2019-09-05

系统版本: 10.0.0

MEID: 35253108271625

总的磁盘空间: 24.32 GB

加密: FBE

Boardid: sailfish

IMSI: 460024082819284

安卓ID: 70ec24580a585a56

ICCID: 70ec24580a585a56

存储: /storage/emulated/0

IMEI

嫌疑人手机IMEI是？（答案格式：3843487568726387）

1 | 352531082716257

盘古石手机取证分析系统

版本: 9900

案件中心

智能提取

工具箱

公告

工具(T)

设置(S)

帮助(H)

关于(A)

案件管理

案件202309160...

搜索...

搜索树节点...

案件20230916093619 (7852/1)

新建任务 20230916093705 (7783/1)

文件系统 (5849/0)

华为克隆 20230911172053 (69/0)

华为克隆 20230911172053... (70/0)

HuaweiBackup (110/0)

sdcard.zip (5600/0)

标签 (0/0)

数据文件 (1086/0)

通讯录 (2/0)

位置信息 (2/0)

应用列表 (411/1)

多媒体 (13/0)

应用数据 (420/0)

基础数据 (420/0)

电量使用 (8/0)

流量使用 (207/0)

应用日志 (205/0)

华为克隆 20230911172053... (69/0)

文件系统 (69/0)

华为克隆 20230911172053 (69/0)

标签 (0/0)

数据文件 (1086/0)

通讯录 (2/0)

位置信息 (2/0)

应用列表 (411/1)

多媒体 (13/0)

应用数据 (420/0)

基础数据 (420/0)

电量使用 (8/0)

流量使用 (207/0)

应用日志 (205/0)

新建任务 20230916093705

导出检材设备信息

编辑检材

检材信息

路径信息

数据路径

设备信息

品牌: Google

本地化代码: zh-Hans-CN

设备名称: sailfish

CPU架构: ['arm64-v8a', 'armeabi-v7a', 'armeabi']

是否Root: 是

空闲的磁盘空间: 16.11 GB

基带版本:

设备ID: sailfish

序列号: FAGA80312283

内核版本: 3.18.137

ICCID2:

型号: Pixel

运营商:

手机号:

IMEI: 352531082716257

时区: Asia/Shanghai

日志文件系统: ext4

蓝牙物理地址: AC:37:43:8D:32:EB

硬件平台: sailfish

sdk版本: 29

WLANMac地址: AC:37:43:53:37:30

鸿蒙版本:

检材编号:

提取时间: 2023/9/16 上午9:37:05

机主姓名:

设备性质:

IMEI2:

备注:

检材平台: Android

手机号码1:

证件类型:

手机型号:

MEID:

Mtp序列号: FAGA80312283

补丁时间: 2019-09-05

系统版本: 10.0.0

MEID: 35253108271625

总的磁盘空间: 24.32 GB

加密: FBE

BoardId: sailfish

IMSI: 460024082819284

安卓ID: 70ec24580a585a56

ICCID:

存储: /storage/emulated/0

稳定版 R7.5.3.SP4.46

高性能

逻辑处理器: 12 核

CPU:

内存 8G:

已连接设备: 0 个

通讯录数据库名

感觉

嫌疑人手机通讯录数据存放在那个数据库文件中？（答案格式：call.db）

1 | contacts.db

盘古石手机取证分析系统

版本: 9900

案件中心

智能提取

工具箱

公告

工具(T)

设置(S)

帮助(H)

关于(A)

案件管理

案件202309160...

搜索...

搜索树节点...

案件20230916093619 (7852/1)

新建任务 20230916093705 (7783/1)

文件系统 (5849/0)

华为克隆 20230911172053 (69/0)

华为克隆 20230911172053... (70/0)

HuaweiBackup (110/0)

sdcard.zip (5600/0)

标签 (0/0)

数据文件 (1086/0)

通讯录 (2/0)

位置信息 (2/0)

应用列表 (411/1)

多媒体 (13/0)

应用数据 (420/0)

基础数据 (420/0)

电量使用 (8/0)

流量使用 (207/0)

应用日志 (205/0)

华为克隆 20230911172053... (69/0)

文件系统 (69/0)

华为克隆 20230911172053 (69/0)

标签 (0/0)

数据文件 (1086/0)

通讯录 (2/0)

位置信息 (2/0)

应用列表 (411/1)

多媒体 (13/0)

应用数据 (420/0)

基础数据 (420/0)

电量使用 (8/0)

流量使用 (207/0)

应用日志 (205/0)

数据库 (94/0)

图片 (125/0)

音频 (24/0)

配置 (41/0)

应用日志 (205/0)

sdcard.zip (5600/0)

位置聚合 (2/0)

流量 (0/0)

contacts

来源应用

删除恢复

清除过滤器

标签

导出

重新载入

概要

#

来源应用

删除

标签

文件预览

路径

文件预览

30

数据文件

20230911172053/HuaweiBackup/Basic/contacts/contacts.db

20230911172053/H

路径

HuaweiBackup/Basic/contacts/contacts.db

93

数据文件

Root/Basic/contacts/contacts.db

Root/Basic/contacts/contacts

路径

HuaweiBackup/Basic/contacts/contacts.db

5

数据文件

HuaweiBackup/Basic/contacts/contacts.db

HuaweiBackup/Basic/contacts

路径

HuaweiBackup/Basic/contacts/contacts.db

文件预览

文件类型

文件大小

来源应用

来源文件

数据库

8 KB

数据文件

HuaweiBackup/Basic/contacts/contacts.db

稳定版 R7.5.3.SP4.46

高性能

逻辑处理器: 12 核

CPU:

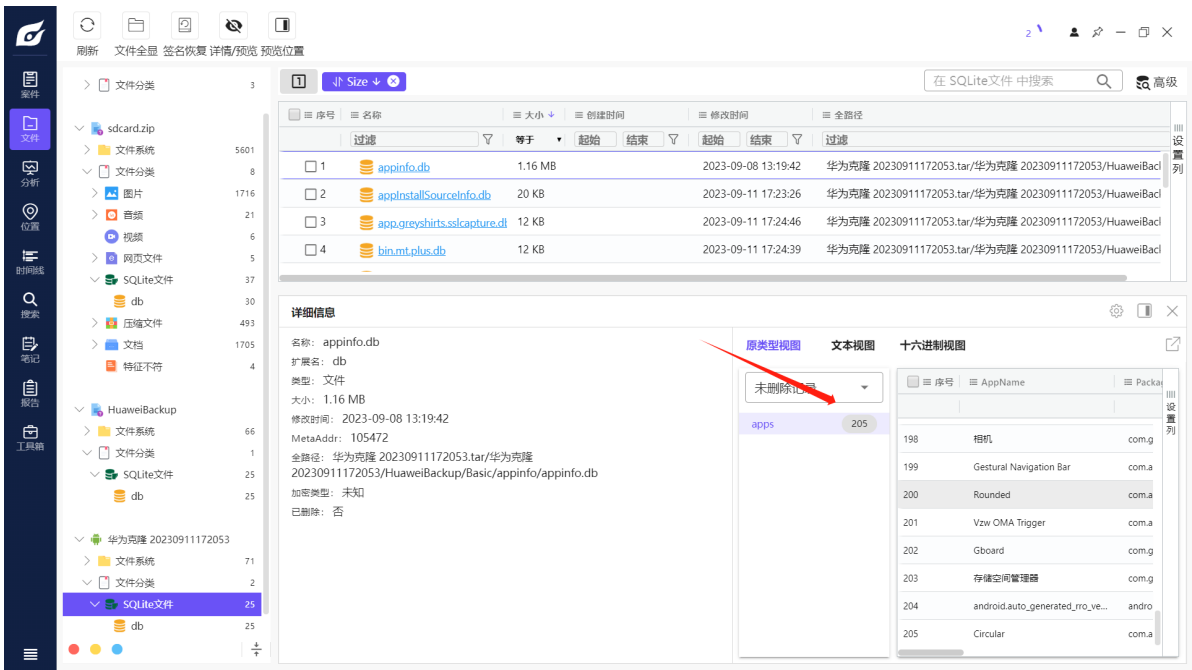
内存 8G:

已连接设备: 0 个

应用数量

嫌疑人手机一共使用过多少个应用？（答案格式：22）

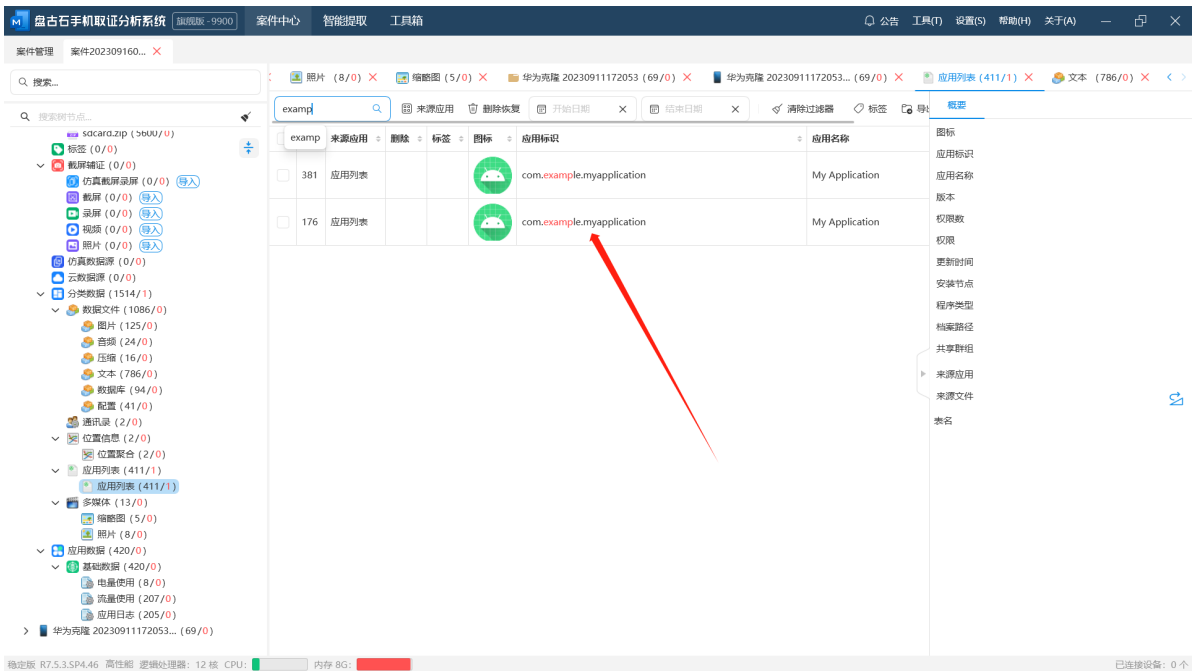
1 | 205



测试apk的包名

测试apk的包名是？（答案格式：con.tencent.com）

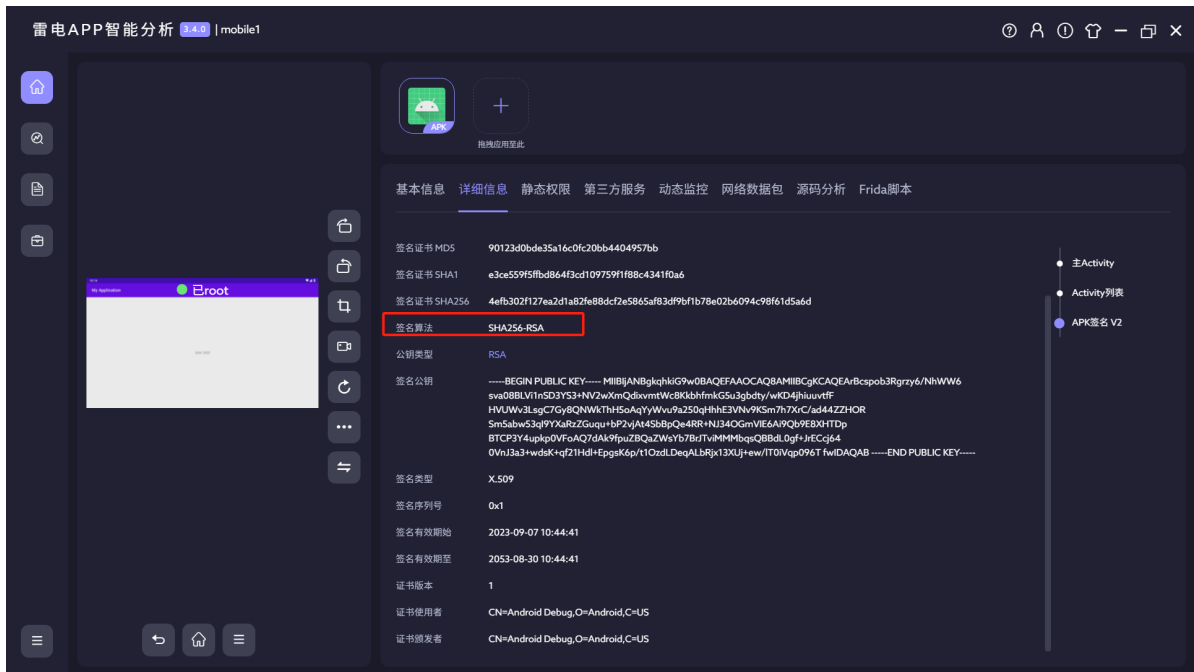
1 | com.example.myapplication



apk签名算法

测试apk的签名算法是？（答案格式:AES250）

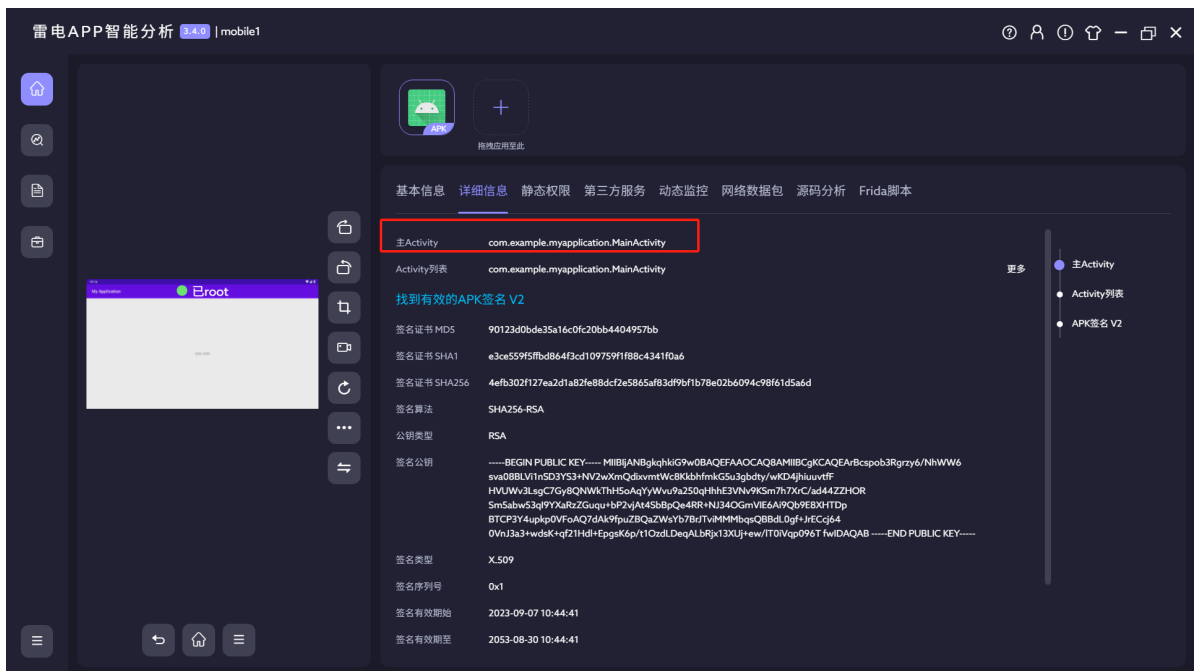
1 | SHA256



apk主入口

测试apk的主入口是？（答案格式：com.tmp.mainactivity）

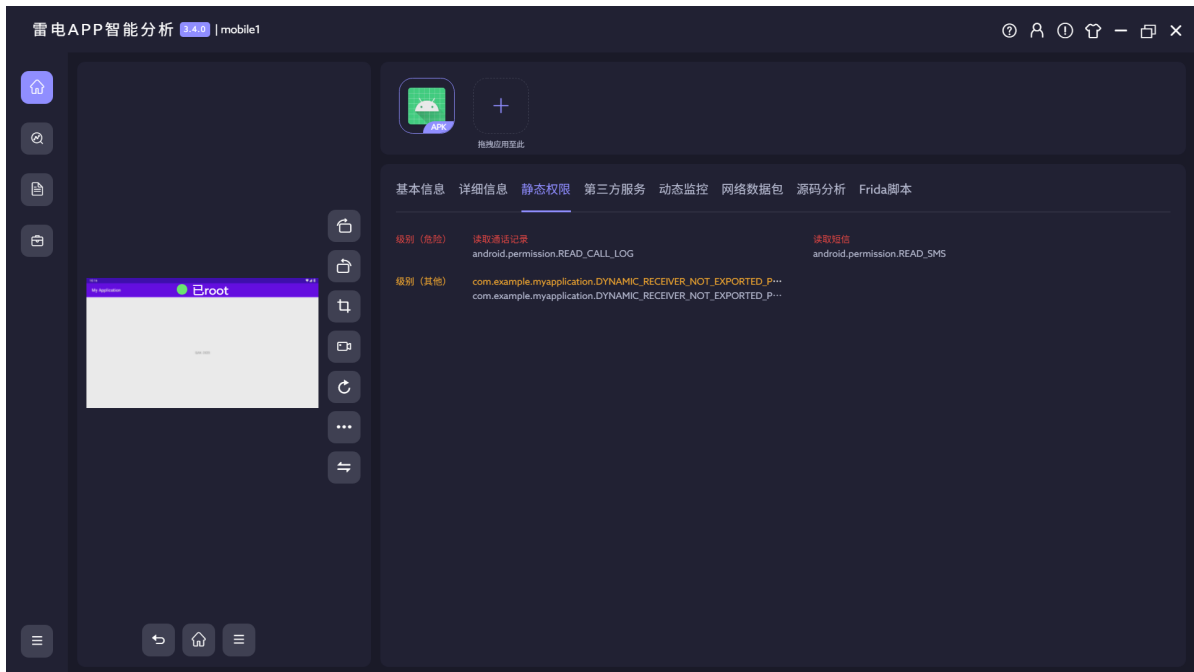
1 | com.example.myapplication.MainActivity



apk权限

测试apk一共申请了几个权限？（答案格式：7）

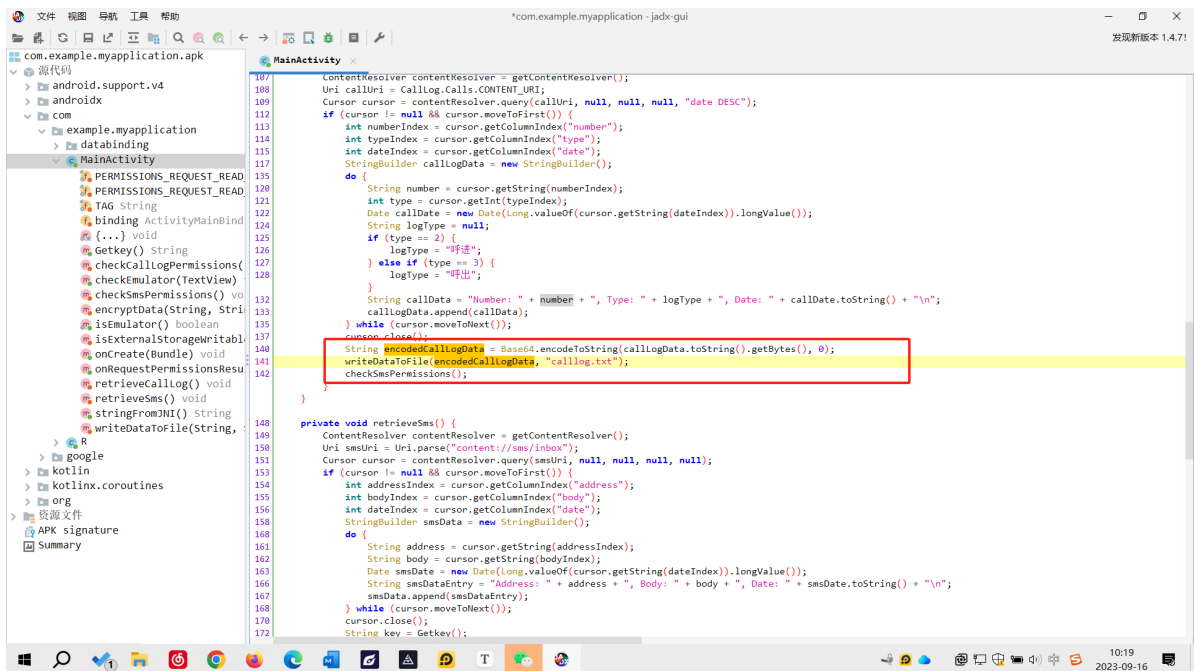
1 | 3



Calllog.txt加密

测试apk对Calllog.txt文件内的数据进行了什么加密？（答案格式：DES）

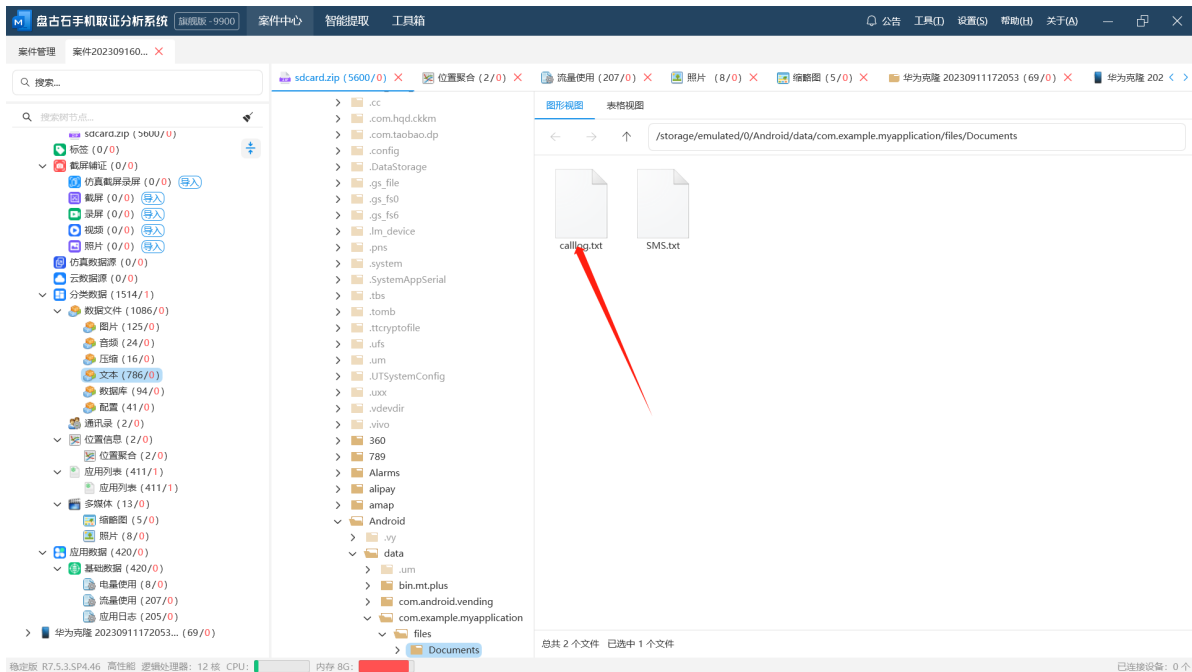
1 | Base64



拨话记录

10086对嫌疑人拨打过几次电话？（答案格式：5）

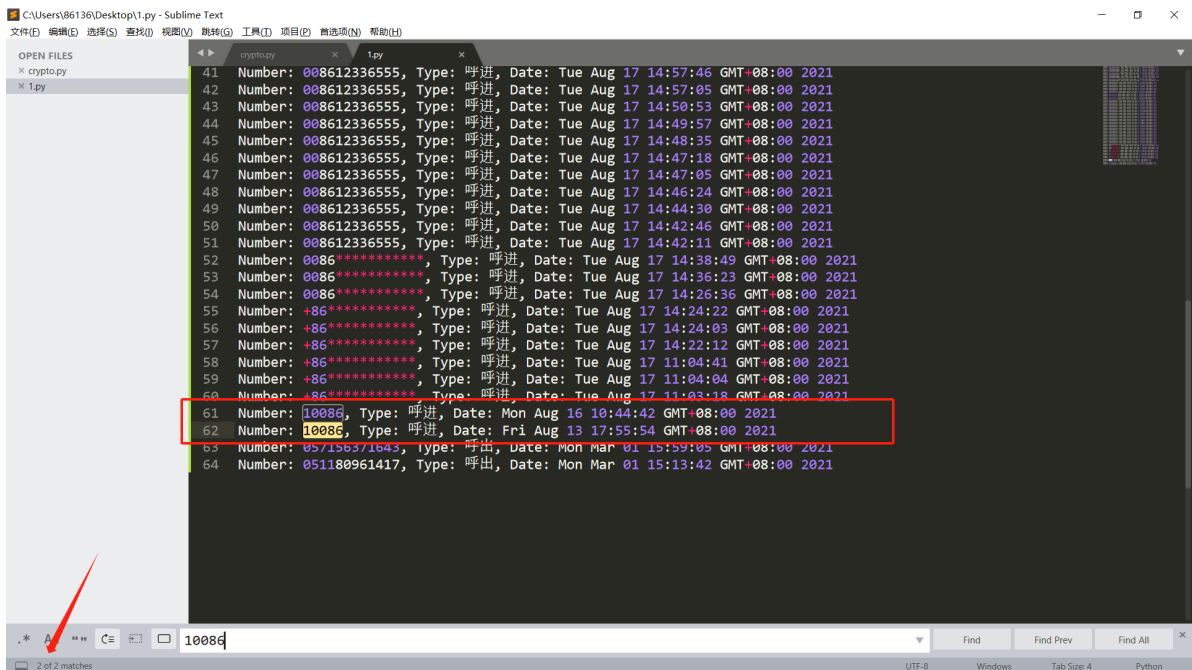
1 | 2



导出来，然后内容base64解密

```
1 Number: +8618181922867, Type: 呼进, Date: Thu Aug 19 17:41:48 GMT+08:00 2021
2 Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:48:45 GMT+08:00 2021
3 Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:45:46 GMT+08:00 2021
4 Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:45:24 GMT+08:00 2021
5 Number: +8618181922867, Type: 呼进, Date: Tue Aug 17 17:44:48 GMT+08:00 2021
6 Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:43:46 GMT+08:00 2021
7 Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:42:14 GMT+08:00 2021
8 Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:41:33 GMT+08:00 2021
9 Number: 18181922867, Type: 呼出, Date: Tue Aug 17 17:38:00 GMT+08:00 2021
10 Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:36:16 GMT+08:00 2021
11 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:35:20 GMT+08:00 2021
12 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:33:02 GMT+08:00 2021
13 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:32:50 GMT+08:00 2021
14 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:32:14 GMT+08:00 2021
15 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:31:48 GMT+08:00 2021
16 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:31:31 GMT+08:00 2021
17 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:30:35 GMT+08:00 2021
18 Number: +8612336555, Type: 呼进, Date: Tue Aug 17 17:30:30 GMT+08:00 2021
19 Number: +8612336555, Type: 呼进, Date: Tue Aug 17 17:29:38 GMT+08:00 2021
20 Number: +8612336555, Type: 呼进, Date: Tue Aug 17 15:57:49 GMT+08:00 2021
21 Number: +8612336555, Type: 呼进, Date: Tue Aug 17 15:49:12 GMT+08:00 2021
22 Number: +8612336555, Type: 呼进, Date: Tue Aug 17 15:48:50 GMT+08:00 2021
23 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:43:58 GMT+08:00 2021
24 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:34:21 GMT+08:00 2021
25 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:33:53 GMT+08:00 2021
26 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:33:11 GMT+08:00 2021
27 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:32:52 GMT+08:00 2021
28 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:31:58 GMT+08:00 2021
```

29 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:27:13 GMT+08:00 2021
30 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:26:09 GMT+08:00 2021
31 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:24:34 GMT+08:00 2021
32 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:20:13 GMT+08:00 2021
33 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:19:23 GMT+08:00 2021
34 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:18:02 GMT+08:00 2021
35 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:14:03 GMT+08:00 2021
36 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:09:22 GMT+08:00 2021
37 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:08:57 GMT+08:00 2021
38 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:07:20 GMT+08:00 2021
39 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:02:05 GMT+08:00 2021
40 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:01:46 GMT+08:00 2021
41 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:57:46 GMT+08:00 2021
42 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:57:05 GMT+08:00 2021
43 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:50:53 GMT+08:00 2021
44 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:49:57 GMT+08:00 2021
45 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:48:35 GMT+08:00 2021
46 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:47:18 GMT+08:00 2021
47 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:47:05 GMT+08:00 2021
48 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:46:24 GMT+08:00 2021
49 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:44:30 GMT+08:00 2021
50 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:42:46 GMT+08:00 2021
51 Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:42:11 GMT+08:00 2021
52 Number: 0086*****, Type: 呼进, Date: Tue Aug 17 14:38:49 GMT+08:00
2021
53 Number: 0086*****, Type: 呼进, Date: Tue Aug 17 14:36:23 GMT+08:00
2021
54 Number: 0086*****, Type: 呼进, Date: Tue Aug 17 14:26:36 GMT+08:00
2021
55 Number: +86*****, Type: 呼进, Date: Tue Aug 17 14:24:22 GMT+08:00 2021
56 Number: +86*****, Type: 呼进, Date: Tue Aug 17 14:24:03 GMT+08:00 2021
57 Number: +86*****, Type: 呼进, Date: Tue Aug 17 14:22:12 GMT+08:00 2021
58 Number: +86*****, Type: 呼进, Date: Tue Aug 17 11:04:41 GMT+08:00 2021
59 Number: +86*****, Type: 呼进, Date: Tue Aug 17 11:04:04 GMT+08:00 2021
60 Number: +86*****, Type: 呼进, Date: Tue Aug 17 11:03:18 GMT+08:00 2021
61 Number: 10086, Type: 呼进, Date: Mon Aug 16 10:44:42 GMT+08:00 2021
62 Number: 10086, Type: 呼进, Date: Fri Aug 13 17:55:54 GMT+08:00 2021
63 Number: 057156371643, Type: 呼出, Date: Mon Mar 01 15:59:05 GMT+08:00 2021
64 Number: 051180961417, Type: 呼出, Date: Mon Mar 01 15:13:42 GMT+08:00 2021



短信几次加密

测试apk对短信记录进行了几次加密？（答案格式：5）

1 | 2



加密密钥

测试apk对短信记录进行加密的密钥是？（答案格式：slkdjflslskdnln）

1 | bG1qdWJkewhmdXJp

hook出来

```

1  Java.perform(function(){
2      console.log("Frida Test Hook10");
3      // 主动调用类静态方法
4      var clszz = Java.use("com.example.myapplication.MainActivity");
5      clszz.checkEmulator.implementation = function () {
6          console.log('method called. ');
7          const key = this.GetKey();
8          console.log('getKey()-----' + key);
9      };
10 });

```

```
1 | frida -H 127.0.0.1:27042 -f com.example.myapplication -l lanmao.js --no-pause
```

```

C:\Windows\System32\cmd.exe - frida -H 127.0.0.1:27042 -f com.example.myapplication -l lanmao.js --no-pause
1438 traced
1439 traced_probes
1037 ueventd
1352 vndservicemanager
1354 vold
1410 vr_hwc
1767 webview_zygote
1452 wificond
1406 zygote
1405 zygote64

C:\Users\S6136\Desktop\tmp\frida>frida -H 127.0.0.1:27042 -f com.example.myapplication -l lanmao.js --no-pause

Frida 14.2.18 - A world-class dynamic instrumentation toolkit

Commands:
  help      -> Displays the help system
  object?   -> Display information about 'object'
  ...
  exit/quit -> Exit

More info at https://frida.re/docs/home/
Spawned com.example.myapplication. Resuming main thread!
[Remote::com.example.myapplication]-> Frida Test Hook10
method called.
getKey()-----bGlqdWJkeWhmdXJp

```

验证码

嫌疑人在2021年登录支付宝的验证码是？（答案格式：3464）

```
1 | 9250
```

base加ase解密

```

C:\Users\15715\Desktop>python exp.py
Address: 1069076034938581, Body: 【探探应用】碧波，有人追你！她20岁，离你553米，建议匹配后和她聊聊成都
app.com/app 回T退订， Date: Tue Aug 17 17:51:02 GMT+08:00 2021
106931164284, Body: 【百合网】有人多次给你留言没有得到你的回复呢，点击查看 http://j.qiuai.com/21VCHMdST
te: Tue Aug 17 17:31:23 GMT+08:00 2021
10658678, Body: 四川手机报：你和妻子/丈夫最难沟通的事是什么？“3.8国际妇女节”到来之际，四川手机报发起话
日常生活中哪种情形让你觉得和丈夫很难沟通？作为丈夫，妻子的哪些话让你不明所以？跟帖留言 mala.cn/t/16104
te: Mon Mar 01 09:50:52 GMT+08:00 2021
106948500153, Body: 【借呗】你支付宝120***@qq.com借呗今天将从余额、储蓄卡或余额宝自动还款1021.68元。如
ate: Mon Mar 01 09:26:44 GMT+08:00 2021
10086, Body: 【缴费提醒】尊敬的客户，您好！您于2021年03月01日09时10分，使用统一支付充值服务为本机充值10
为124.21元。为避免影响您上网功能的正常使用，请进行关开机或关开飞行模式操作，谢谢。如需查看更多业务使用情
多动掌上营业厅】，点击下载体验http://dx.10086.cn/schfcd。百分努力，只为您10分满意！【中国移动】， Date:
49 GMT+08:00 2021
106980095188, Body: 【支付宝】你正在登录支付宝，验证码9250，泄露验证码会影响资金安全。唯一热线：95188，
09:08:43 GMT+08:00 2021

```

