# 电子取证

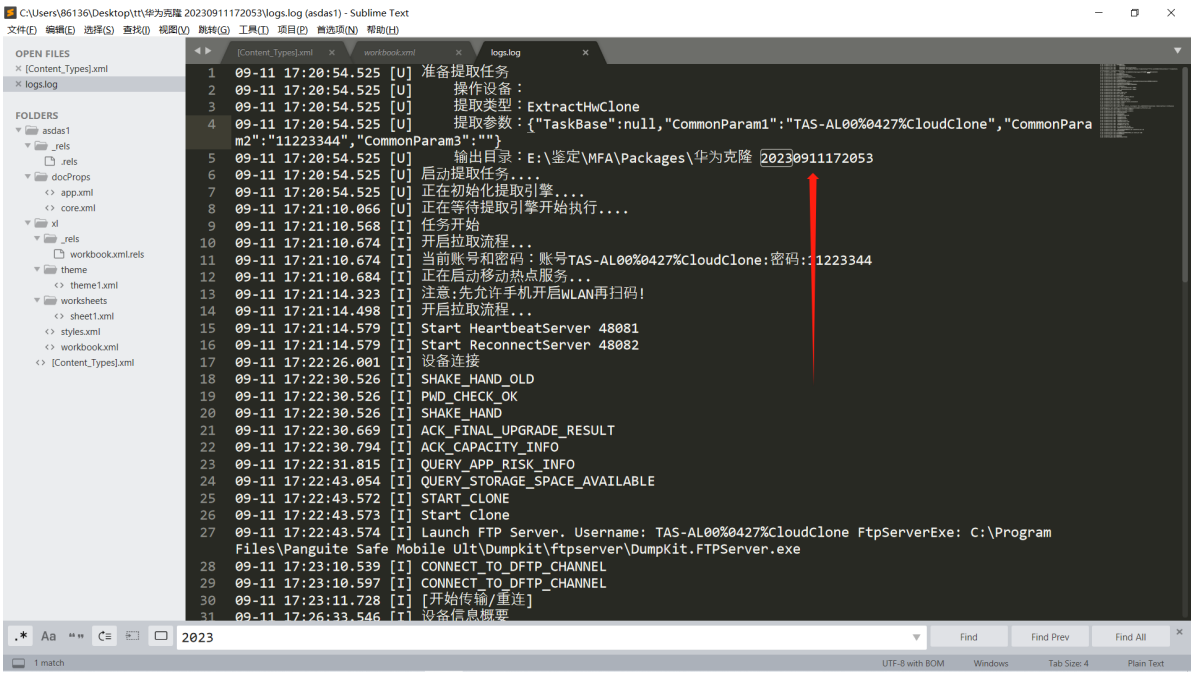
## 案例说明

> 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放到手机中。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）

```
09-11 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）

```
24.32
```


# 设备名称

嫌疑人手机设备名称是？（答案格式：adfer）

```
sailfish
```


# IMEI

嫌疑人手机IMEI是？（答案格式：3843487568726387）

```
352531082716257
```


# 通讯录数据库名

感觉

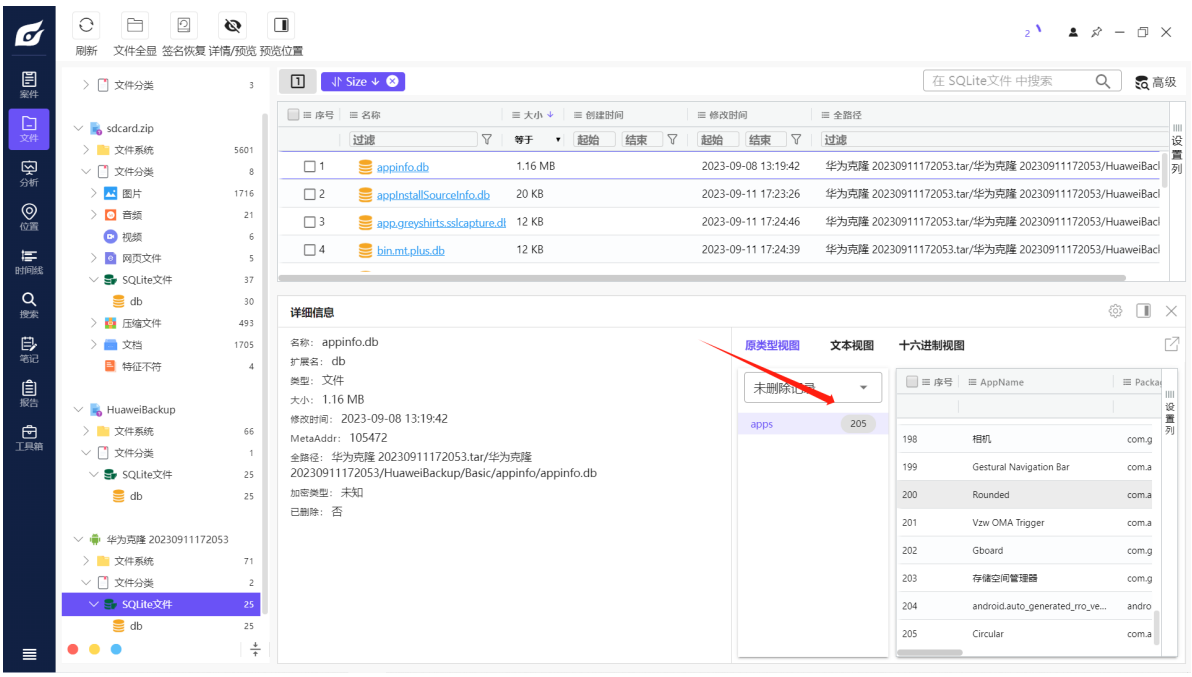
嫌疑人手机通讯录数据存放在那个数据库文件中？（答案格式：call.db）

```
contacts.db
```


# 应用数量

嫌疑人手机一共使用过多少个应用？（答案格式：22）

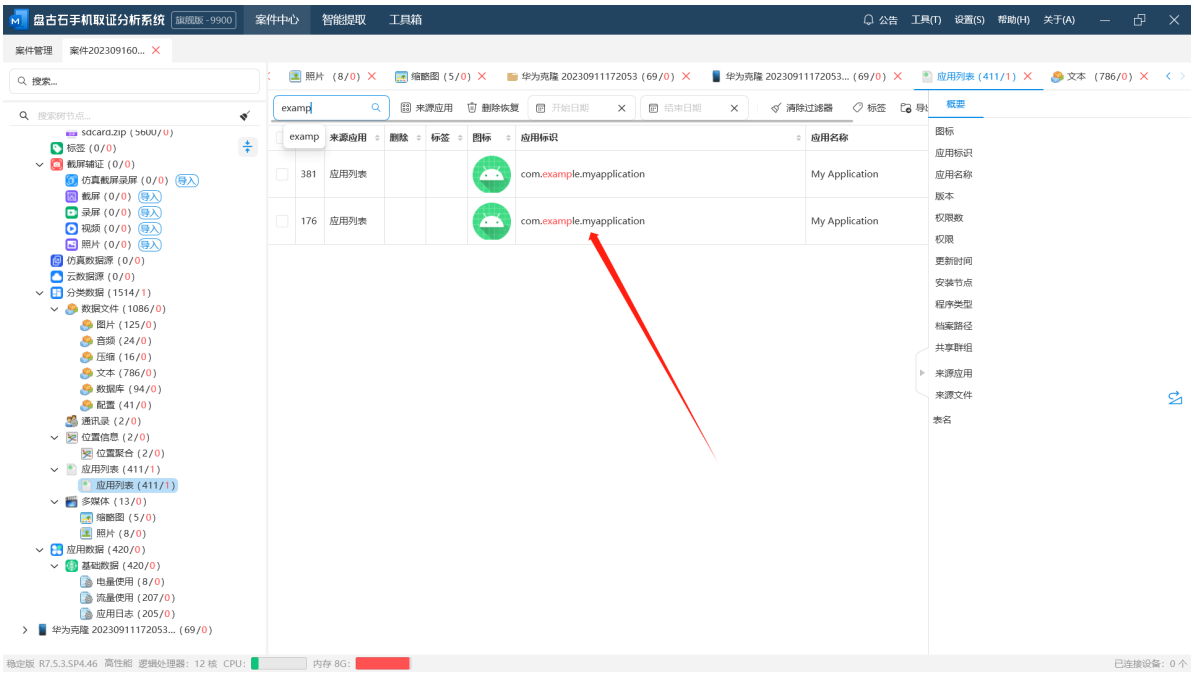
```
205
```




# 测试apk的包名

测试apk的包名是？（答案格式：con.tencent.com）

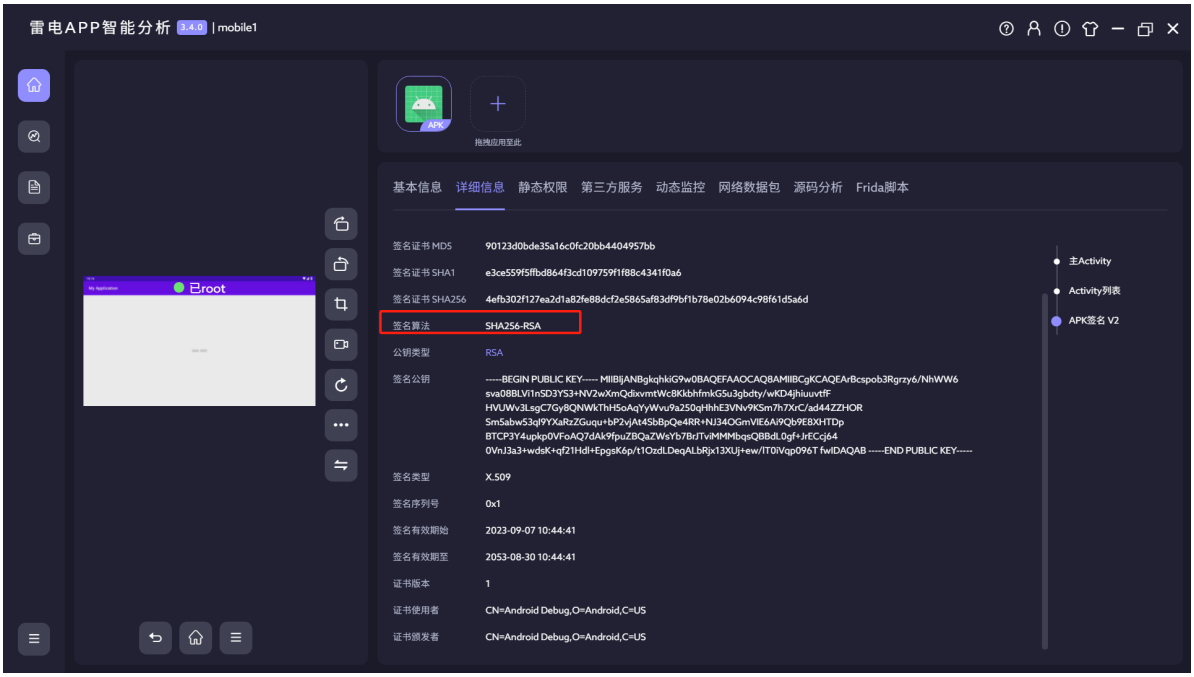
```
com.example.myapplication
```




# apk签名算法

测试apk的签名算法是？（答案格式:AES250）

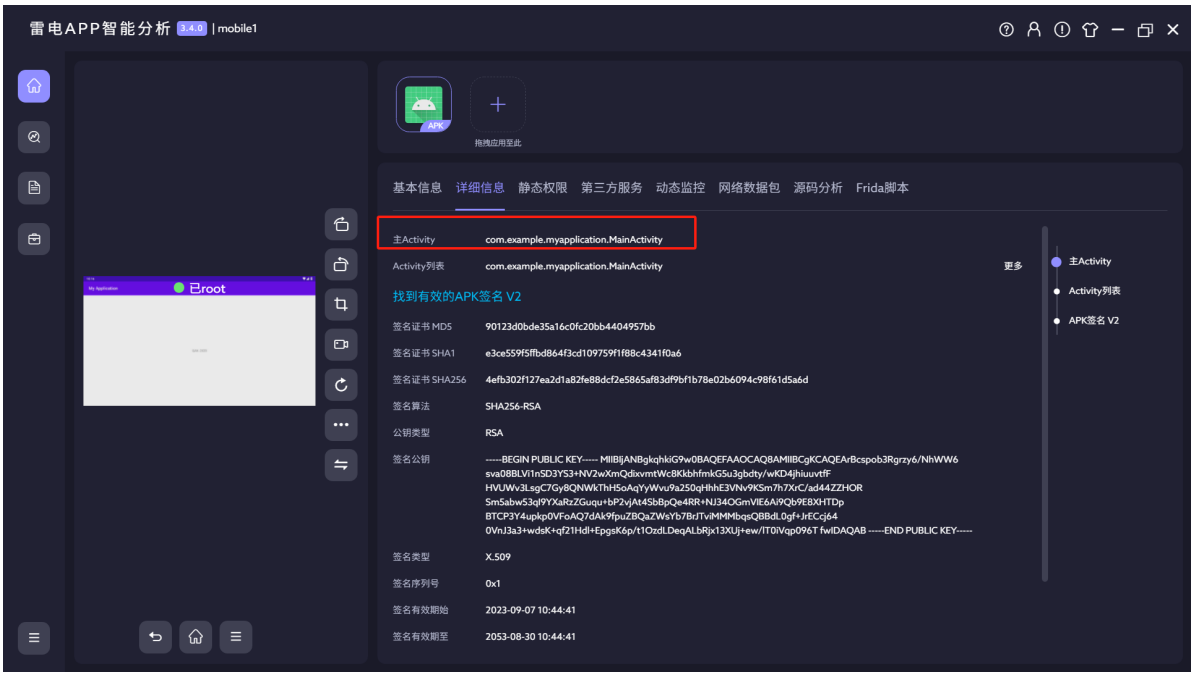
```
SHA256
```




# apk主入口

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

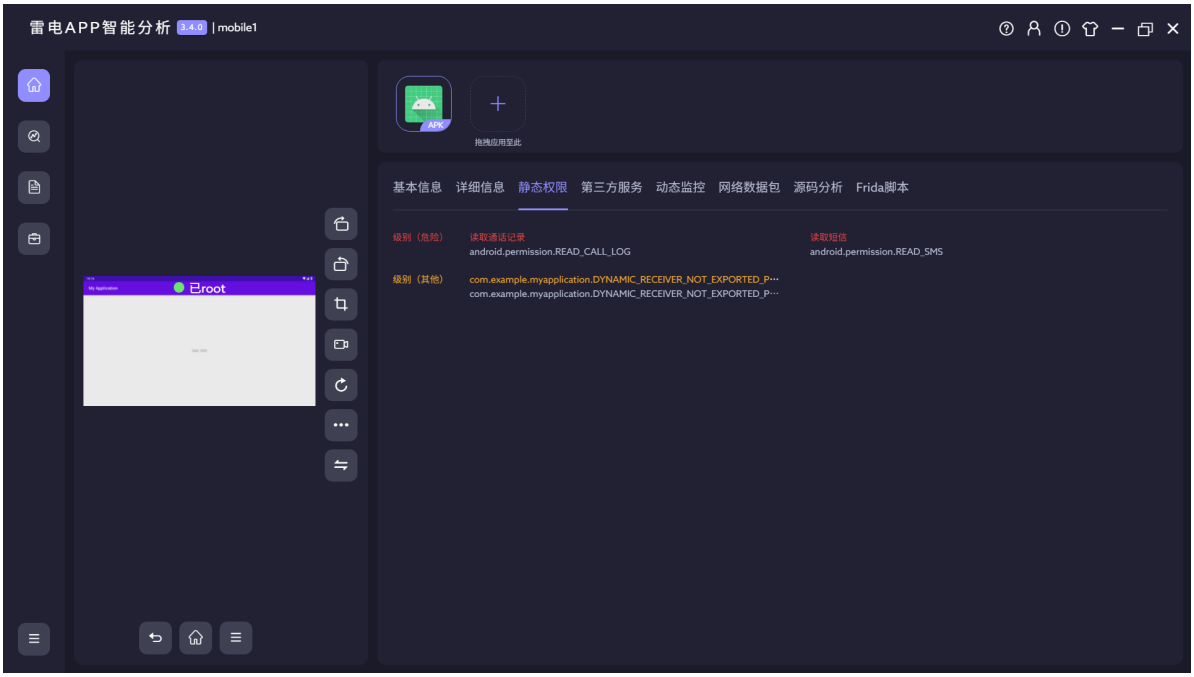
```
com.example.myapplication.MainActivity
```




# apk权限

测试apk一共申请了几个权限？（答案格式：7）

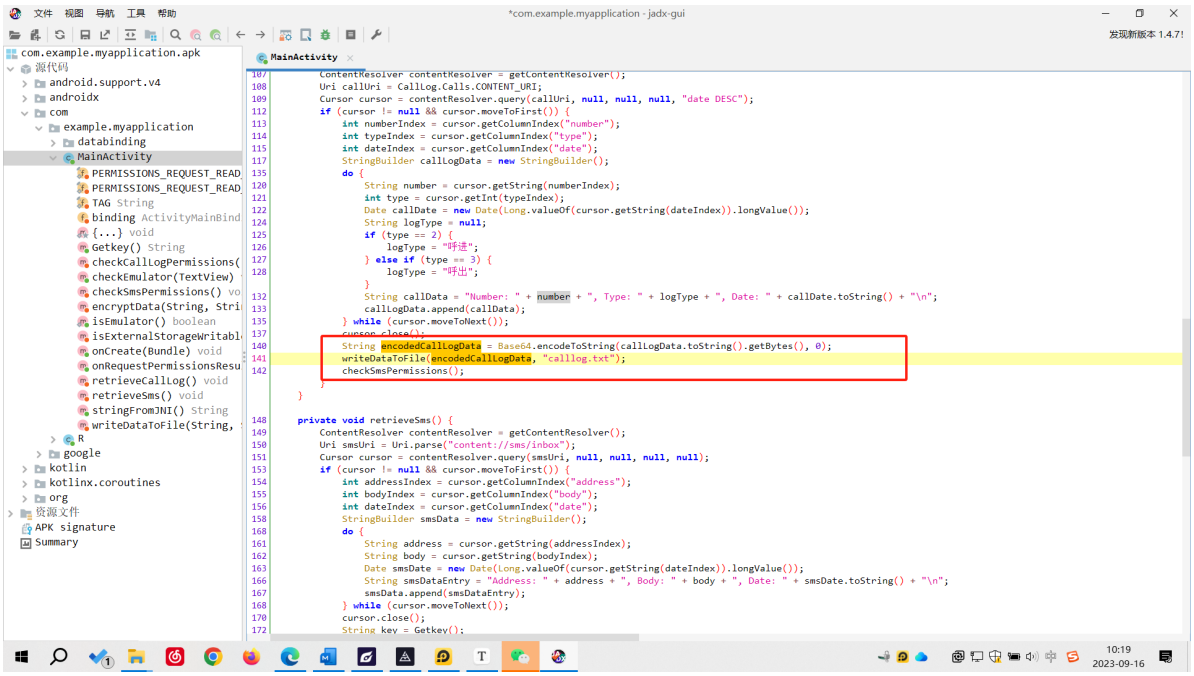
```
3
```




# 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）

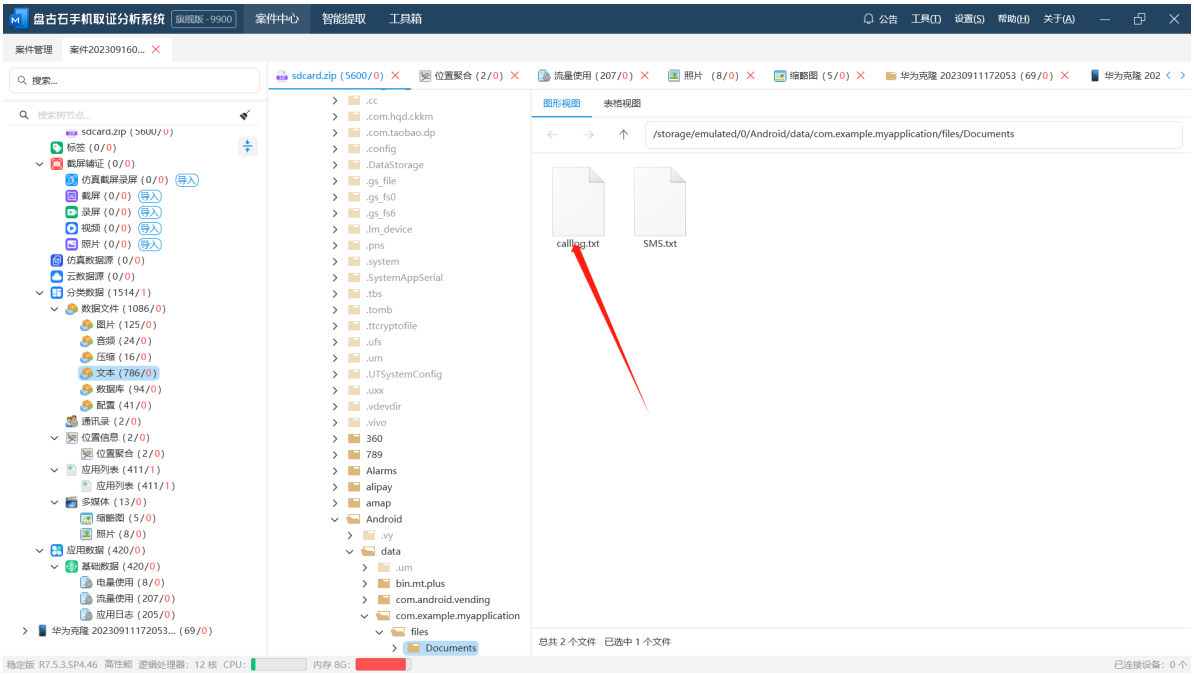
```
Base64
```




# 拨话记录

10086对嫌疑人拨打过几次电话？（答案格式：5）

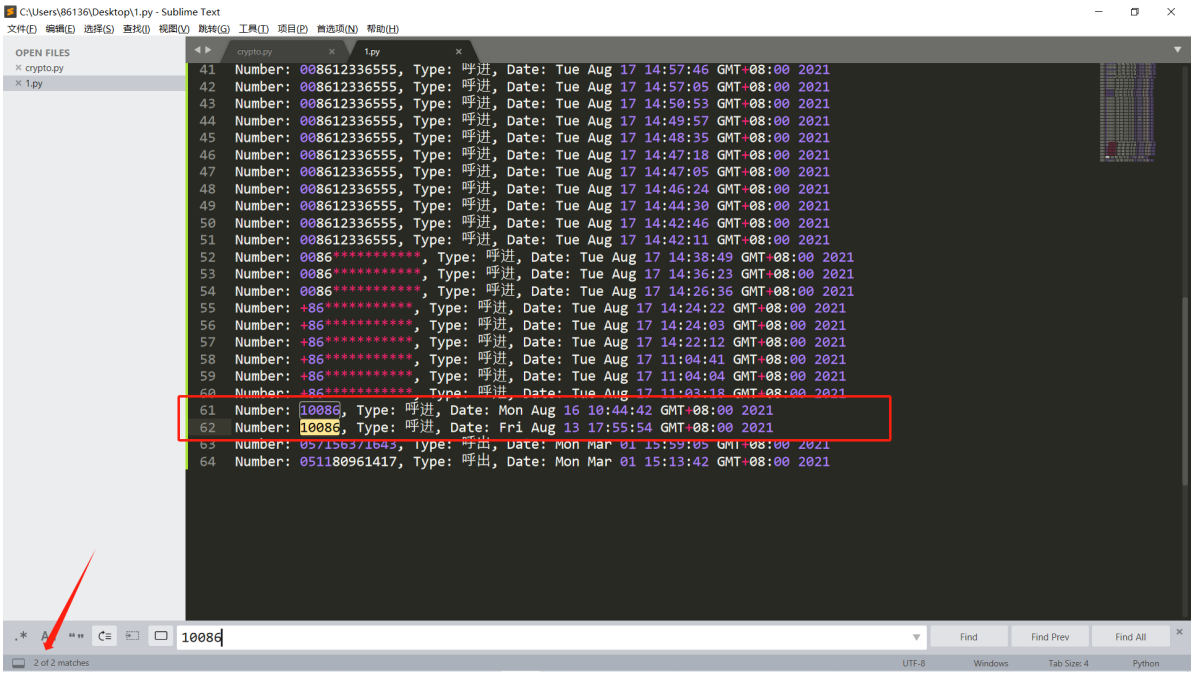
```
2
```




导出来，然后内容base64解密

```
Number: +8618181922867, Type: 呼进, Date: Thu Aug 19 17:41:48 GMT+08:00 2021
Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:48:45 GMT+08:00 2021
Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:45:46 GMT+08:00 2021
Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:45:24 GMT+08:00 2021
Number: +8618181922867, Type: 呼进, Date: Tue Aug 17 17:44:48 GMT+08:00 2021
Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:43:46 GMT+08:00 2021
Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:42:14 GMT+08:00 2021
Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:41:33 GMT+08:00 2021
Number: 18181922867, Type: 呼出, Date: Tue Aug 17 17:38:00 GMT+08:00 2021
Number: 008618181922867, Type: 呼进, Date: Tue Aug 17 17:36:16 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:35:20 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:33:02 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:32:50 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:32:14 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:31:48 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:31:31 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 17:30:35 GMT+08:00 2021
Number: +8612336555, Type: 呼进, Date: Tue Aug 17 17:30:30 GMT+08:00 2021
Number: +8612336555, Type: 呼进, Date: Tue Aug 17 17:29:38 GMT+08:00 2021
Number: +8612336555, Type: 呼进, Date: Tue Aug 17 15:57:49 GMT+08:00 2021
Number: +8612336555, Type: 呼进, Date: Tue Aug 17 15:49:12 GMT+08:00 2021
Number: +8612336555, Type: 呼进, Date: Tue Aug 17 15:48:50 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:43:58 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:34:21 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:33:53 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:33:11 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:32:52 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:31:58 GMT+08:00 2021
```

```
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:27:13 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:26:09 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:24:34 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:20:13 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:19:23 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:18:02 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:14:03 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:09:22 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:08:57 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:07:20 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:02:05 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 15:01:46 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:57:46 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:57:05 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:50:53 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:49:57 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:48:35 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:47:18 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:47:05 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:46:24 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:44:30 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:42:46 GMT+08:00 2021
Number: 008612336555, Type: 呼进, Date: Tue Aug 17 14:42:11 GMT+08:00 2021
Number: 0086**********, Type: 呼进, Date: Tue Aug 17 14:38:49 GMT+08:00
2021
Number: 0086**********, Type: 呼进, Date: Tue Aug 17 14:36:23 GMT+08:00
2021
Number: 0086**********, Type: 呼进, Date: Tue Aug 17 14:26:36 GMT+08:00
2021
Number: +86**********, Type: 呼进, Date: Tue Aug 17 14:24:22 GMT+08:00 2021
Number: +86**********, Type: 呼进, Date: Tue Aug 17 14:24:03 GMT+08:00 2021
Number: +86**********, Type: 呼进, Date: Tue Aug 17 14:22:12 GMT+08:00 2021
Number: +86**********, Type: 呼进, Date: Tue Aug 17 11:04:41 GMT+08:00 2021
Number: +86**********, Type: 呼进, Date: Tue Aug 17 11:04:04 GMT+08:00 2021
Number: +86**********, Type: 呼进, Date: Tue Aug 17 11:03:18 GMT+08:00 2021
Number: 10086, Type: 呼进, Date: Mon Aug 16 10:44:42 GMT+08:00 2021
Number: 10086, Type: 呼进, Date: Fri Aug 13 17:55:54 GMT+08:00 2021
Number: 057156371643, Type: 呼出, Date: Mon Mar 01 15:59:05 GMT+08:00 2021
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）

```
2
```

```
    }

    private void retrieveSms() {
        ContentResolver contentResolver = getContentResolver();
        Uri smsUri = Uri.parse("content://sms/inbox");
        Cursor cursor = contentResolver.query(smsUri, null, null, null, null);
        if (cursor != null && cursor.moveToFirst()) {
            int addressIndex = cursor.getColumnIndex("address");
            int bodyIndex = cursor.getColumnIndex("body");
            int dateIndex = cursor.getColumnIndex("date");
            StringBuilder smsData = new StringBuilder();
            do {
                String address = cursor.getString(addressIndex);
                String body = cursor.getString(bodyIndex);
                Date smsDate = new Date(Long.valueOf(cursor.getString(dateIndex)).longValue());
                String smsDataEntry = "Address: " + address + ", Body: " + body + ", Date: " + smsDate.toString() + "\n";
                smsData.append(smsDataEntry);
            } while (cursor.moveToNext());
            cursor.close();
            String key = Getkey();
            String encryptedSmsData = encryptData(smsData.toString(), key);
            writeDataToFile(encryptedSmsData, "SMS.txt");
        }
    }

    private String encryptData(String data, String key) {
        try {
            Cipher cipher = Cipher.getInstance("AES");
            Key aesKey = new SecretKeySpec(key.getBytes(), "AES");
            cipher.init(1, aesKey);
            byte[] encryptedData = cipher.doFinal(data.getBytes());
            return Base64.encodeToString(encryptedData, 0);
        } catch (Exception e) {
            Log.e(TAG, "Failed to encrypt data: " + e.getMessage());
            return null;
        }
    }

    private void writeDataToFile(String data, String fileName) {
        if (isExternalStorageWritable()) {
```

# 加密秘钥

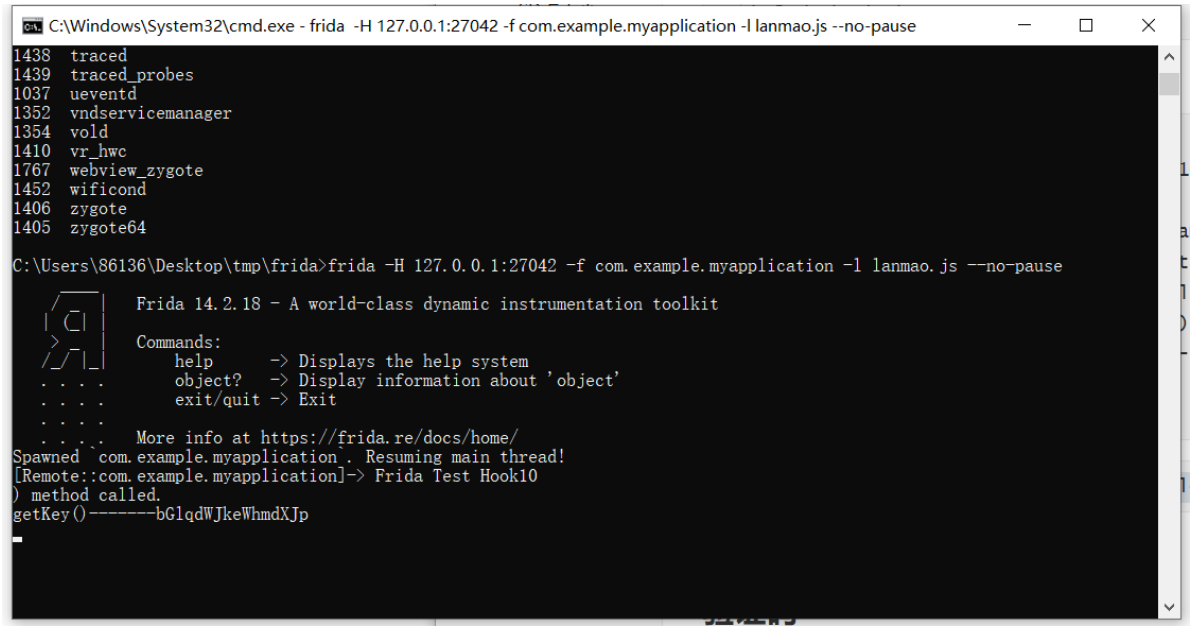
测试apk对短信记录进行加密的秘钥是？（答案格式：slkdjlfslskdnln）

```
bGlqdWJkeWhmdXJp
```

hook出来

```
Java.perform(function(){
        console.log("Frida Test Hook10");
        // 主动调用类静态方法
        var clszz = Java.use("com.example.myapplication.MainActivity");
        clszz.checkEmulator.implementation = function () {
            console.log(') method called.');
            const key = this.Getkey();
            console.log('getKey()-------'  + key);
    };
 });
```

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




## 验证码

嫌疑人在2021年登录支付宝的验证码是？（答案格式：3464）

```
9250
```

base加ase解密