获取微信联系人的技术尝试

一、预选方案

我做了三种尝试方案：

第一种：数据抓包

第二种：通过AccessibilityService进行获取

第三种：破解微信手机数据库

第一种方案：需要抓包微信数据，这个通过技术手段是可以实现的，有类似的例子：*Packet* Capture（类似于搭建VPN服务），但是发现微信的传输数据是经过加密的，目前还没有破解的方法，所以放弃次方案

第二种方案：通过AccessibilityService获取微信的数据，这个首先要展示出来而且要通过模拟点击以及滑动才能获取全部的联系人信息，而且仅仅展示的是用户昵称 无法获取更多的数据，所以也放弃了

第三种方案：破解微信数据库的方式，由于微信的数据库加密的Sqlite（也就是我们常用的的Sqlcipher库 ）微信将联系人以及聊天的内容都放在的本地的数据进行缓存，所以我们只要能破解他的数据库密码也就可以了。

二、破解微信

由于破解的过程比较繁琐复杂，详见“**微信数据库反编译密码的过程**”文档。经过一步一步破解分析，我们知道微信数据加密规则如下：

1.获取手机IMEI码

2.获取当前登录微信账号的uin(存储在sp里面)

3.拼接IMEI和uin

4.将拼接完的字符串进行md5加密

5.截取加完密的字符串的前七位（字母必须为小写）

因为我们要抓去微信的数据库和SP文件，而他们存放在微信的沙盒中，所以**我们必须要Root我们的手机**

一、App获取Root权限

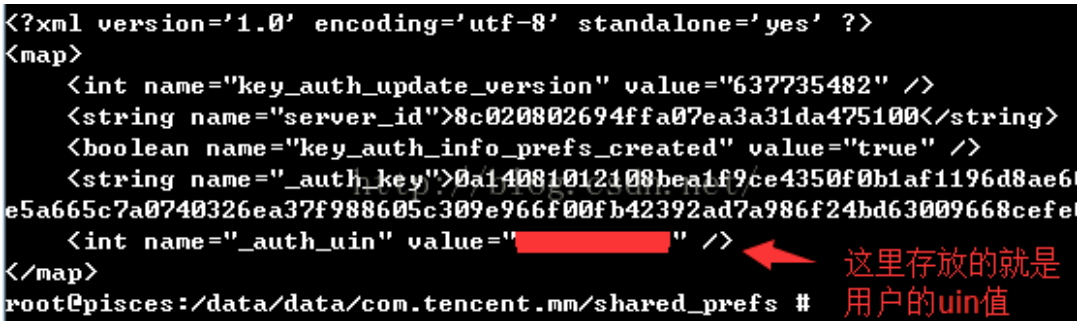
我们使用命令的方式 去获取Root全权限，这样才能打开微信的沙盒 。

二、获取密码

1、获取IMEI这个比较好获取直接通过getDeviceId就可以了。

2、获取当前微信账的uin：

这个我们首先要获取再哪个SP文件中，通过把微信的整个sp文件导出来（sp的路径：**/data/data/com.tencent.mm/shared_prefs**）。

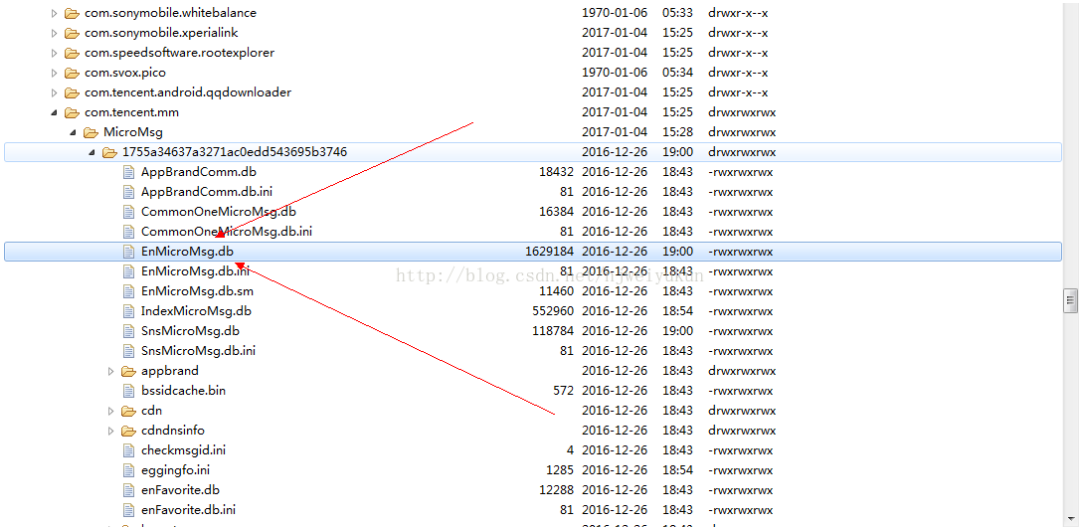


然后使用sublime工具打开所有的sp文件， 然后全局搜索uin这个字段，发现了这个字段在**auth_info_key_prefs.xml**文件中，通过解析XML数据的方式就可以获取到uin了。

3-5、我们获取到了所有的信息之后，，就可以拿到这个密码了。

三、获取数据库

微信聊天以及通讯录的数据库 都在**/data/data/com.tencent.mm/MicroMsg**这个路径下，这里有一个32位的md5加密的文件夹，这个应该是每个登陆过账户id加密之后文件夹。



不管这个文件夹名称是什么，我们最关键的是要找到叫**EnMicroMSg.db**的文件，这个就是存放所有的聊天以及通讯录的数据库了。所有我们要获取这个数

据，只要遍历文件夹找到名字叫**EnMicroMSg.db**的文件就可以了

四、在手机上破解数据库

我们既然找到了密码，也找到了数据库，那么我们就可以破解数据库了

之前我们是说过了，微信也是通过Sqlcipher这个加密的SQLITE数据库，但是有一点不同的是，微信使用的是Sqlcipher的2.x版本，而我们使用的是库一般是Sqlcipher的3.x版本。

不能像往常使用Sqlcipher数据库一样去打开数据，需要做一些兼容处理：

```
SQLiteDatabase.loadLibs(context);
 SQLiteDatabaseHook hook = new SQLiteDatabaseHook() {
 public void preKey(SQLiteDatabase database) {
 }
 public void postKey(SQLiteDatabase database) {
    database.rawExecSQL("PRAGMA cipher_migrate;"); //兼容2.0的数据库  这句话很关键
 }
};
```

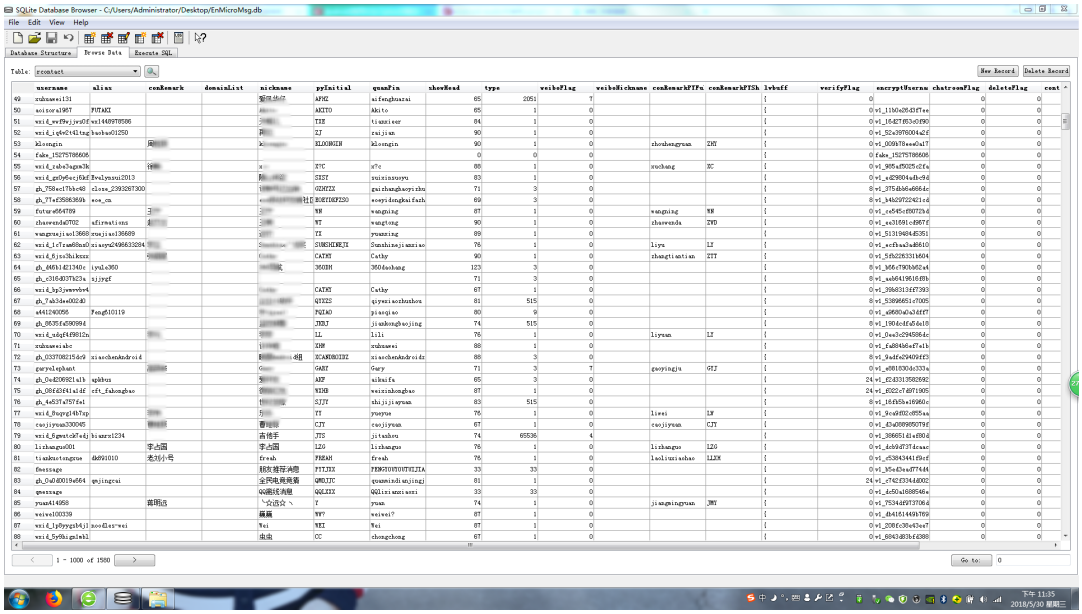
另外我们要拷贝出一份数据库到我们沙盒中，然后去连接打开数据库，不能直接使用微信沙盒中的数据库，因为微信的数据库已经建立连接了，我们不能再打开连接这个数据库，否则会出现连不上或者微信连不上（因为数据库只能连接一个）。

之后我们就可以正常的打开微信的数据库了

如果我们想获取聊天的信息 那么就查看message表，

如果我们想获取联系人的数据，那么久查看rcontact表。

如果我们想获会话列表的数据，那么久查看rconversation表。



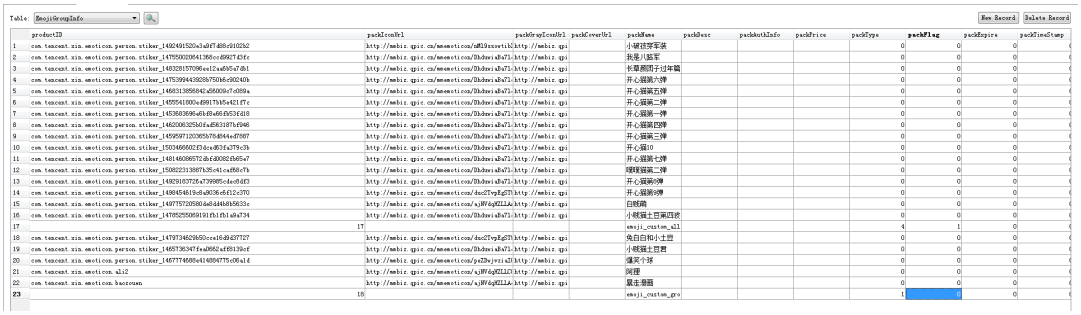
userinfo表 是记录微信的个人信息的表

Table: userinfo

	id	type	value
1	-2046825377	4	false
2	-2046825369	4	false
3	-2046825368	4	false
4	-2046825366	4	true
5	2	3	xuhuawei131
6	3	3	
7	4	3	爱凤华仔
8	5	3	1262751086@qq.co
9	6	3	13810864584
10	7	1	17006719
11	9	1	1262751086
12	14	1	637929266
13	15	1	1
14	16	1	0
15	17	1	2
16	18	1	1
17	19	3	
18	21	3	weixin
19	22	3	weixin
20	26	4	false
21	29	3	https://w.mail.q
22	30	4	false
23	34	1	17719378

24	40	1	195650
25	41	1	7
26	46	3	
27	52	1	0
28	54	4	false
29	59	4	true
30	60	4	true
31	62	4	true
32	64	1	0
33	72	3	
34	74	2	1527577392
35	79	3	<k25>22e57a8e980
36	89	1	1
37	256	4	false
38	8195	3	081e1208080110a1
39	8196	2	0
40	8197	3	

EnmojiGroupInfo这个表是 下载的动态表情管理



目前暂时知道的表是这些 其他的表以后可以通过代码详细的去分析 但是工作量比较巨大！根据具体需求在具体分析

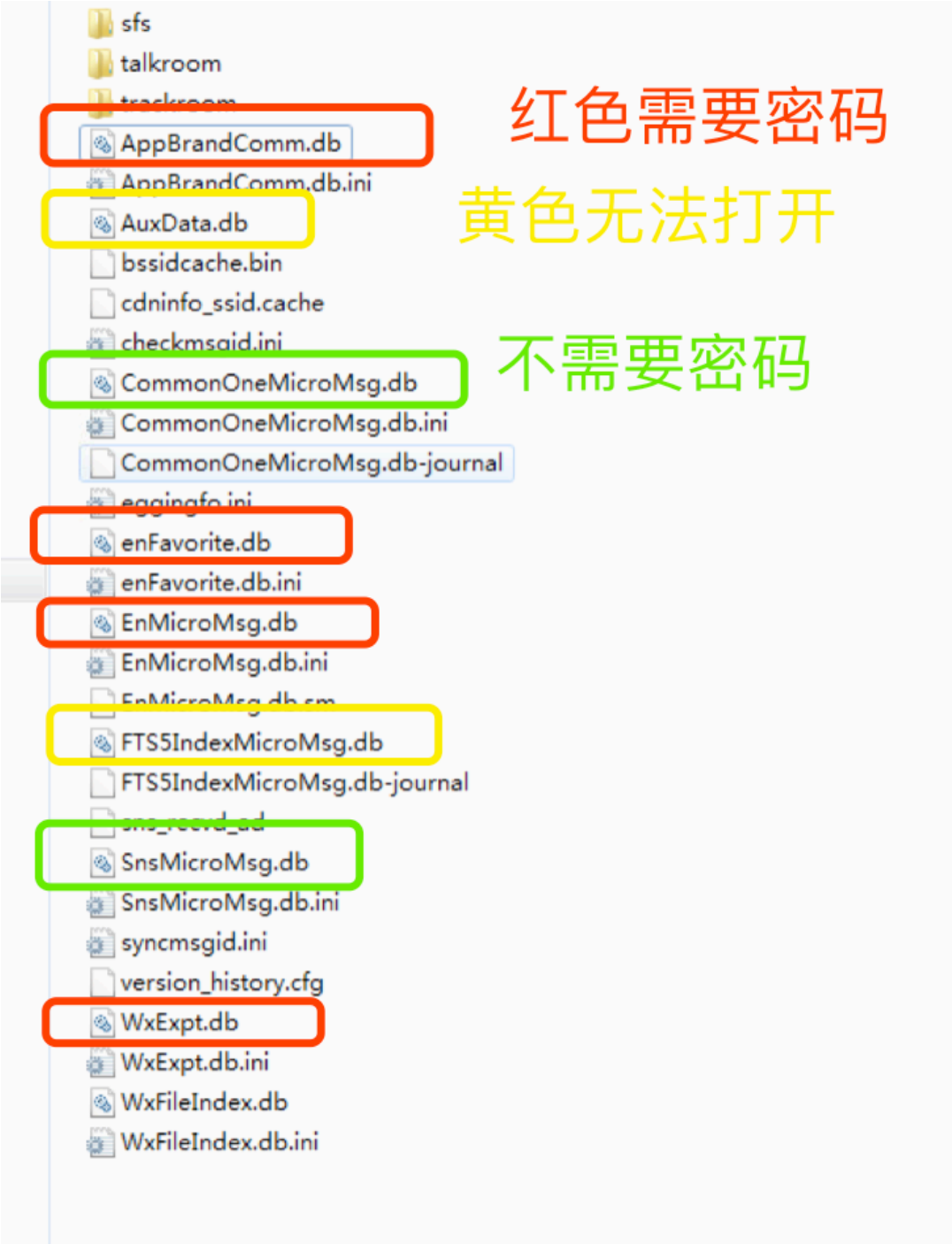
四、对于其他的数据库

我们这里对其他的数据库进行了一个简单的统计

红色圈起来的需要密码的，但是也是同一套密码，密码规则同上

绿色的是不需要密码的

黄色的数据库，打不开，猜测缺少ini文件！



这就是破解微信联系人的流程，具体细节可以查看项目源码。