

浣熊\_BUPT

移动互联网... 智能终端开发...

目录视图 摘要视图 RSS 订阅

个人资料



浣熊

访问： 514739次

积分： 4718

等级： **BLOG > 5**

排名： 第3655名

原创： 95篇 转载： 6篇

译文： 0篇 评论： 229条

文章搜索

文章分类

算法 (43)

软件使用 (2)

面试 (40)

文章存档

2014年12月 (1)

2014年11月 (2)

2014年08月 (3)

2014年07月 (2)

2014年06月 (20)

阅读排行

iOS开发：开发者账号申请 (86013)

Android ADT安装技巧 (48926)

直接利用Android手机破解 (30868)

Android开发——自动连挂 (28701)

高德地图 android api 实践 (28188)

## 直接利用Android手机破解微信加密数据库EnMicroMsg.db

标签： 微信数据库 EnMicroMsg Android

2014-12-04 11:16 30896人阅读 评论(56) 收藏 举报

版权声明：本文为博主原创文章，未经博主允许不得转载。

※首先，简单介绍一下微信加密数据库EnMicroMsg.db的破解方法：

要先批评一下微信，居然用开源的数据库加密方式，这不是一破解一个准吗...

如果你的模拟器或者真机已经获得了root权限，就可以直接将记录聊天记录的数据文件拷贝出来，数据库文件具体存放位置如下：

在/data/data/中：

com.tencent.mm	2014-11-21 10:14 drwxrwxrwx
MicroMsg	2014-11-21 10:15 drwx-----
47d58c79e692e212e...	2014-12-02 02:24 drwx-----
CommonOneMicroMsg.db	12288 2014-11-21 10:14 -rw-----
CommonOneMicroMsg.db.ini	80 2014-11-21 10:14 -rw-----
EnMicroMsg.db	894976 2014-12-02 02:24 -rw-----
EnMicroMsg.db.ini	80 2014-12-02 02:19 -rw-----
IndexMicroMsg.db	331776 2014-11-21 10:16 -rw-----
SnsMicroMsg.db	81920 2014-11-21 10:14 -rw-----
SnsMicroMsg.db-shm	32768 2014-12-02 02:19 -rw-----
SnsMicroMsg.db-wal	432632 2014-11-21 10:15 -rw-----
SnsMicroMsg.db.ini	80 2014-11-21 10:14 -rw-----
cdn	2014-11-21 10:14 drwx-----
cdnnsinfo	2014-11-21 10:14 drwx-----

（题外话：android原生的模拟器root起来很复杂，推荐一款第三方模拟器：genymotion，很方便）

※我们拿到EnMicroMsg.db后，用常用的数据库管理软件打开，发现EnMicroMsg.db被加密了，但是密码生成规则很简单，具体如下：

（手机IMEI + 微信uin）取MD5的前7位

手机的IMEI获取：手机拨号盘输入：\*#06#

微信uin获取：<http://blog.csdn.net/yuanboh/article/details/41280837>

但是即使算出来解密密码，我们仍发现用刚才使用的数据库管理软件是打不开的。因为其用的是SQLCipher开源库提供的加密解密算法，故在网上下载SQLCipher.exe这个软件，打开.db文件时，输入计算出来的密码后，就可以打开EnMicroMsg.db文件了：

SQLite Database Browser - C:\Users\del\Desktop\EnMicroMsg.db													
File Edit View Help													
Database Structure Browse Data Execute SQL													
Table: message													
	msgId	msgOrId	type	status	isSend	isShowTimer	createTime	talker	content	ingPath	reserved	lvbuffer	transContent
1	1	519662403	1	3	0	0	1416192831000	weixin	Welcome back			{	
2	2	6819148787			0	0	1416192972000	5153124648ch	To translate			{	
3	3				2	0	1416192973896	5153124648ch	You invited			{	
4	4	2565264290			1	0	1416193028203	5153124648ch	Test... just			{	
5	5	7078015971	10000	4	0	0	1416193068000	weid_739ee	To translate			{	
6	6	0267897946			0	0	1416193068001	weid_739ee	干嘛呢			{	
7	7	8204948261			0	0	1416198143000	5153124648ch	yanyn_hper: 32323221116144:52			{	

※上面提到了SQLCipher是一个提供数据库文件加密解密功能的第三方开源库，我们先来访问以下他们的官网看个究竟：

<https://www.zetetic.net/sqlcipher/open-source/>

我们惊喜的发现，现在SQLCipher提供了Android操作系统的开源库，源码在Github上可以下载获得，但是我尝试下载了Github上的工程，编译的时候遇到了很多问题，导致最终没有编译成功。所以建议大家下载如下图所示

- MySQL批量导入Excel、t  
(24855)
- iOS通过ASIHTTPRequest:  
(23245)
- iOS TableView didSelec  
(21932)
- 制作iOS Ad-Hoc测试应用  
(19616)
- android在Service中弹出  
(15440)

- 评论排行
- 直接利用Android手机破... (56)
- Android开发——自动连... (50)
- UC——成也专一，败也... (33)
- android AlarmManager的... (14)
- 制作iOS Ad-Hoc测试应用 (12)
- idoubs DevelopersGuid... (10)
- Android ADT安装技巧其... (8)
- 如何获取微信uin (8)
- 高德地图 android api 实... (8)
- iOS开发：开发者账号申... (7)

- 推荐文章
- \*搭建docker私有仓库
- \*Android杂谈之RadioGroup+ViewPager制作的底部导航栏
- \* Android几种常见的多渠道(批量)打包方式介绍
- \*Oculus Rift, HTC Vive, SONY PSVR的全面对比
- \*Android View的事件分发机制探索
- \*Redis源码解析：15Resis主从复制之从节点流程

- 最新评论
- Android开发——自动连接指定S...  
xiaovxiaoa: @hwliu51:为什么我连接没有密码的无线还是不行啊？，addNetwork()返回的是1，en...
- Android开发——自动连接指定S...  
aidonglei521: 如何解决连接中文ssid连接不上网的情况
- Android开发——自动连接指定S...  
aidonglei521: @yuyan19850204:是中文怎么办
- Android开发——自动连接指定S...  
Mr\_DongLi: 非常感谢！！
- 直接利用Android手机破解微信加...  
QQ14685162: 现在这样的骗子太多了！可恨至极！我也想查老公的记录，也被骗过，最后找了黑客（QQ）1468516...
- android AlarmManager的时间设...  
Big\_e: 是不是也可以用这个代替：  
c\_set.add(Calendar.DAY\_OF\_YEA
- android AlarmManager的时间设...  
Big\_e: 顶一个，遇到一样的问题，网上的关于alarmManager的教程都忽略的东西
- 直接利用Android手机破解微信加...  
npcwow: 楼主好，请问下必须是root拿到EnMicroMsg.db文件才行吗？root之后直接连接ddms就...
- 直接利用Android手机破解微信加...  
npcwow: @sa1510:您好，请问你新版本的微信能打开数据库吗？步骤算法跟楼主的一样就行了呀？必须要root...
- Android开发——自动连接指定S...  
qq\_30267841: 你好我想请问如

的开源库压缩包：

SQLCipher for Android

Source code for the Android packages are made available via git:

git clone https://github.com/sqlcipher/android-database-sqlcipher.git

http://blog.csdn.net/yuanboh

SQLCipher for Android Community Edition binaries are made available as a free service to the community here:

SQLCipher For Android ← 点此下载“SQLCipher for Android开源库”

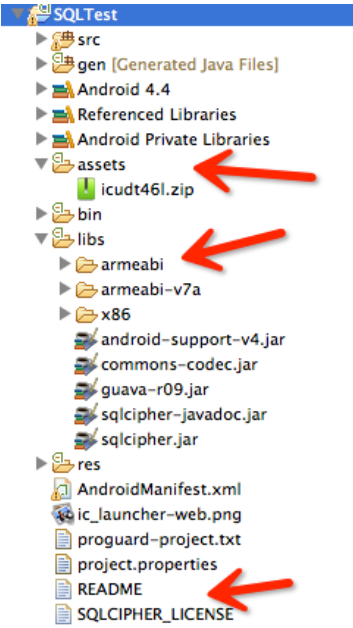
Note that private support for SQLCipher for Android is available through our Commercial Edition program.

解压下载的压缩包，其目录如下图所示：



※下面涉及到Android工程创建、导入SQLCipher开源库等工作：

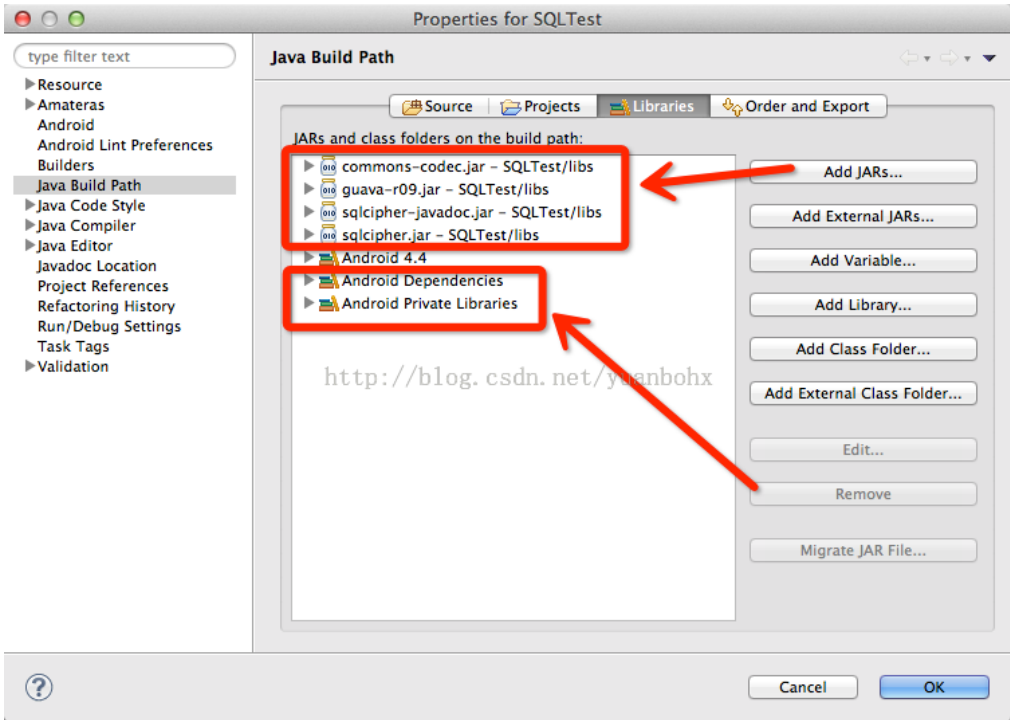
创建Android工程就不详细说了，创建完工程后，直接将sqlcipher-for-android-v3.2.0文件夹中的内容全部拷贝到android工程中即可：



接下来的步骤也很关键：

右键工程，Build Path → Configure Build Path，按照下图所示添加相应的jar包，删除android自有库：

果是类似麦当劳的那种免费WIFI，第一种擒敌康适用吗，我试过可以连到，但是无法跳转到登...



最后在程序中加入读取加密数据库的关键代码即可：

```
[java]
01. public void readWeChatDatabase() {
02.
03.     SQLiteDatabase.loadLibs(this);
04.     String password = "XXXXXXX";
05.     File databaseFile = getDatabasePath("/data/data/com.tencent.mm/MicroMsg/47d58c79e
06.     //File databaseFile = getDatabasePath("EnMicroMsg.db");
07.     eventsData = new myDataHelper(this);
08.
09.     SQLiteDatabaseHook hook = new SQLiteDatabaseHook() {
10.         public void preKey(SQLiteDatabase database) {
11.
12.         public void postKey(SQLiteDatabase database) {
13.             database.rawQuery("PRAGMA cipher_migrate;"); //最关键的一句!!!
14.         }
15.     };
16.
17.     try {
18.         SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(databaseFile, "XXXXXXX
19.         Cursor c = db.query("message", null, null, null, null, null, null);
20.         while (c.moveToNext()) {
21.             int _id = c.getInt(c.getColumnIndex("msgId"));
22.             String name = c.getString(c.getColumnIndex("content"));
23.             Log.i("db", "_id=>" + _id + ", content=>" + name);
24.         }
25.         c.close();
26.         db.close();
27.     } catch (Exception e) {}
28. }
```

程序很简答，password即为数据库的加密密码，databaseFile为数据库文件路径，database.rawQuery("PRAGMA cipher\_migrate")这句最为关键，原因如下：

现在SQLCipher for Android已经是3.X版本了，而微信居然还停留在2.X时代，所以这句话是为了能够用3.X的开源库兼容2.X的加密解密方法，如果不加这句话，是无法对数据库进行解密的。

（题外话：SQLCipher的功能确实相当强大，我这里介绍的只是冰山一角，更多的功能大家可以通过其官网或者Github中提供的工程代码进行探究）

最后展示一下程序运行效果，从Logcat信息可以看到，我们成功读取了微信的EnMicroMsg.db文件中的message数据表：

```
I 12-04 03:10:38.131 1775 1789 com.example.sqltest Database cipher.so 0xa69f7948
I 12-04 03:10:38.131 1775 1789 com.example.sqltest Database JNI_OnLoad called
I 12-04 03:10:39.011 1775 1789 com.example.sqltest db JNI_OnLoad register methods
I 12-04 03:10:39.011 1775 1789 com.example.sqltest db _id=>1, content=>Welcome back! Feel free to tell me if you have any
problems or suggestions for WeChat.
I 12-04 03:10:39.011 1775 1789 com.example.sqltest db _id=>2, content=>To translate a message into system's language, lon
g press the message and then select "Translate".
I 12-04 03:10:39.011 1775 1789 com.example.sqltest db _id=>3, content=>You invited [redacted] to the group chat
I 12-04 03:10:39.011 1775 1789 com.example.sqltest db _id=>4, content=>Test...just ignore this...
I 12-04 03:10:39.011 1775 1789 com.example.sqltest db _id=>5, content=>To translate a message into system's language, lon
g press the message and then select "Translate".
I 12-04 03:10:39.011 1775 1789 com.example.sqltest db _id=>6, content=>干啥呢
I 12-04 03:10:39.011 1775 1789 com.example.sqltest db _id=>7, content=>yanyu_hper:3352:1
```

当然，我所做的工作有着明显的不足，即需要先通过各种人工方式计算出数据库解密密码，然后再进行.db文件的解密。有兴趣的网友可以尝试直接在程序中取得IMEI与微信uin（这个应该是难点），然后MD5取前7位，最后用算出的解密码对数据库进行解密。

顶

8

踩

1

上一篇 如何获取微信uin

参考知识库



**Android知识库**  
11932 关注 | 1149 收录



**MySQL知识库**  
8359 关注 | 1396 收录




**微信开发知识库**  
6099 关注 | 500 收录

猜你在找

- 微信公众平台深度开发Java版 v2.0（第一季）完整版
- Android入门实战教程
- 嵌入式Linux C编程基础
- 深入浅出MySQL入门必备
- 微信公众平台开发入门
- android手机命令行下不能使用sqlite3命令查看db
- cocos2d-x-39.js对ccs的Listview的item的Button如
- android xmpp asmack提供类似微信陌陌的IM即时通
- android手机获取系统短信sqlite数据库并查看内容
- 从root的android手机中导出app的db文件

查看评论

32楼 QQ14685162 2016-03-31 19:47发表



现在这样的骗子太多了！可恨至极！我也想查老公的记录，也被骗过，

最后找了黑客（QQ）14685162帮我查好的

现在除了他，其他的还真没有能破译的

认准QQ: 14685162

认准QQ: 14685162

认准QQ: 14685162

认准QQ: 14685162

31楼 npcwow 2016-03-16 09:24发表



楼主好，请问下必须是root拿到EnMicroMsg.db文件才行吗？ root之后直接连接ddms就可以打开了吗？

30楼 sa1510 2016-02-25 17:10发表



感谢您的分享，通过查看手机文件发现，data/data/com.tencent.mm/shared\_prefs/auth\_info\_key\_prefs.xml文件中有个int类型的\_auth\_uin字段为uin值，微信6.3.13亲测可用

Re: [npcwow](#) 2016-03-16 09:16发表



回复[sa1510](#)：您好，请问你新版本的微信能打开数据库吗？步骤算法跟楼主的一样就行了呀？必须要root吗？谢谢！

29楼 [mjhksm](#) 2016-02-22 00:49发表



EnMicroMsg.db文件有，密码也有了，软件.SQLcipher也装了，把文件拖放到上面，根本就没有弹出输入密码的提示框啊！到底怎么弄，兄弟们帮帮我啊！我的邮箱mjhksm@163.com 谢谢了啊！

28楼 [jty123jty](#) 2016-01-14 14:41发表



请问下为什么我的uin 是10位数呢

27楼 [qq\\_33631820](#) 2016-01-05 11:33发表



手机监控 通话 短信 位置 QQ, 上传webservice, 手机查询  
手机需要root, webservice自己搭建,

26楼 [qq\\_33631820](#) 2016-01-05 11:29发表



手机端监控 通话 短信 位置 QQ 并上传webservice 另外有手机端查询 手机需要root并能安装程序

25楼 [ji40188](#) 2015-12-29 17:14发表



楼主 有没有试过PC版本的db解密？

24楼 [田埂上的梦想](#) 2015-12-17 09:07发表



这个是基于那个 微信版本上测试的呢？

23楼 [qq\\_32693691](#) 2015-11-10 10:43发表



大侠

22楼 [sinat\\_32010083](#) 2015-11-02 15:45发表



请问您还有没有sqlcipher-for-android-v3.2.0这个东西啊，这个版本网上找不到，最新的版本也没有下载的。另外，请教一下，myDataHelper这个类是怎么写的？可否赐教？

21楼 [sinat\\_32010083](#) 2015-11-02 15:44发表



请问您还有没有sqlcipher-for-android-v3.2.0这个东西啊，这个版本网上找不到，最新的版本也没有下载的。另外，请教一下，myDataHelper这个类是怎么写的？可否赐教？

20楼 [scj2cy](#) 2015-08-26 10:14发表



sqlite3\_open\_v2("/data/data/com.tencent.mm/MicroMsg/cdffdf33xxxxxxxxxxxxxxxxxxxx/EnMicroMsg.db", &handle, 6, NULL) failed 楼主，我在读取数据库的时候报这个错，java.io.FileNotFoundException:  
/data/data/com.tencent.mm/MicroMsg/cdffdf33xxxxxxxxxxxxxxxxxxxx/EnMicroMsg.db: open failed: EACCES (Permission denied) 但是我手机已经root且程序也获得了权限，为何还是会报无权限呢？

Re: [zheng\\_raul](#) 2015-09-24 19:47发表



回复[scj2cy](#)：遇到同样的问题，请问你解决了吗

19楼 [scj2cy](#) 2015-08-11 16:49发表



楼主你好，我测试了一下在程序里实现，但是不行，你可不可把你的代码发我一份。谢谢楼主了，scj2cy@163.com

18楼 [ljcmeng](#) 2015-08-09 22:45发表



苑神真是厉害！

17楼 [ayj2011](#) 2015-07-11 14:15发表



很不错，可以查看数据库聊天记录，用sqlcipher.exe打开数据库，输入（手机IMEI + 微信uin）的MD5 32位 加密的小写的前七位即可。

16楼 [sam\\_zhang1984](#) 2015-07-03 16:48发表



你好，看了你的直接利用Android手机破解微信加密数据库EnMicroMsg.db受益不少。有个问题请教一下，如果才能操作到微信的data/data文件夹，我试了好像读出的数据库文件大小等于0，应该就是没正确读取到了，能否给我一份DEMO代码学习一下，谢谢你了

15楼 [sam\\_zhang1984](#) 2015-07-03 16:48发表

你好，看了你的直接利用Android手机破解微信加密数据库EnMicroMsg.db受益不少。有个问题请教一下，如果才能操作到



微信的data/data文件夹，我试了好像读出的数据库文件大小等于0，应该就是没正确读取到了，能否给我一份DEMO代码学习一下，谢谢你了

14楼 5月18日 2015-06-28 09:04发表



大神您好，我是小白，能帮我恢复我的聊天记录吗？我把enmicromsg.db导出来了的

13楼 leo18945 2015-06-19 18:05发表



楼主，我取到的uin是10位不是9位啊，156xxxxxx, 所以MD5后取几位啊当密码啊？

12楼 aili2015 2015-05-19 18:02发表



“（手机IMEI + 微信uin）取MD5的前7位”  
md5加密套用时，是带括号、加号、空格的吗？为啥我16位，32位大小写都试着取前7位了，就是密码不正确呢，就只有一个EnMicroMsg文件名，但是复制到SD卡的时候文件名变成了EnMicroMsg-复制，这有影响吗？

Re: aili2015 2015-05-19 18:18发表



回复aili2015：我连括号，空格的全半角都试，还是不正确啊，我使用的是sqlcipher.exe，不过可能是2011年左右的版本，有影响吗？

11楼 tianyaofande 2015-04-22 19:44发表



你好 SnsMicroMsg.db 这个纪录 朋友圈内信息的数据库研究过没有？text字段是blob类型的，里面中文不可以正常显示，可否一起研究研究？

10楼 feixiangdeqianqiu 2015-03-10 17:14发表



大神，我求教一下，为啥我的手机root之后也看不到enmicromsg.db文件捏？用的360的文件管理工具。

Re: feixiangdeqianqiu 2015-03-10 17:26发表



回复feixiangdeqianqiu：我是小白，我的sony手机是用的root大师。对开发是外行，只知道一点点java和python。我是不是应该从头学习一下android操作系统？

9楼 mbclk1009 2015-03-03 05:21发表



楼主您, 好可否進一步說明一下MD5要怎麼生成呢？

Re: y788iiiiii 2015-03-04 17:48发表



回复mbclk1009：javaAPI里面有，调用即可

8楼 bitlik 2015-02-25 19:26发表



非常棒的文章，我刚刚成功提取出了全部微信消息。有几点提醒一下：  
\* 取MD5的前7位，字母用小写形式；  
\* 如果不打算编译sqlcipher，可以到<http://download.csdn.net/detail/wang382758656/7000933>下载编译好的windows版本。

Re: 浣熊 2015-02-25 22:14发表



回复bitlik：谢谢分享

7楼 u010857479 2015-01-29 18:51发表



特别想知道文件夹名 47d58c\*\*\*\*\* 是怎么生成的，博主知道么？

Re: y788iiiiii 2015-03-04 17:41发表



回复u010857479：MD5("mm"+uin)

6楼 sqtds 2015-01-26 20:05发表



楼主V5，经测试可用，就是图片显示不了，有没有办法让微信使用当前的加密数据库，微信如果崩溃了就会产生一个EnMicroMsg.dberr1422272608776，我想替换EnMicroMsg.db，微信也没读到，不知道哪里数据不对的原因

Re: 斯考尔雷欧海德 2015-03-04 16:42发表



回复sqtds：微信5.3.1的EnMicroMsg.db经常崩溃。一般不会坏。将改名的数据库EnMicroMsg.dberr1422272608776改回去就好。

5楼 简单的梦想 2015-01-21 15:45发表



请问你的那段代码是加在那个JAVA文件里的

4楼 简单的梦想 2015-01-21 14:12发表

请问你这是那个版本的微信，貌似现在的版本不行吧，我在手机上连com.Tencent.mm文件夹都找不到，很多人也找不到





3楼 [SYSTEMUI](#) 2015-01-13 16:37发表



楼主，能不能把Android工程创建的具体步骤说一下，我还是不太清楚，您是在WINDOWS下操作，还是在MAC下操作，您有QQ吗？可不可以加我一下！

2楼 [wangmingli61](#) 2014-12-11 21:54发表



您好。感谢您的分享！

首先我想说我不懂Android开发，也不太懂数据库。我想通过这个方法把我的聊天记录保存下来方便查看。

几个问题如下，希望您能帮我解答

1.SQLcipher是一个软件还是一个依托别的软件平台才能使用的数据库。如果是前者，那么在什么操作系统下运行？（我在网上找到了所谓的SQLcipher，发现无法在win7下打开，或者不会；虚拟了mac系统，也打不开）。如果是后者，那么用什么软件？怎么操作呢？

2.我是否可以这样理解。博文的第二部分，也就是导入数据库 创建安卓工程 再一堆代码的过程是为了解密的。前面的 手机IMEI + 微信uin 取MD5的前7位 就可以直接不解密而打开数据库 看到聊天内容。（MD5是啥意思？）那样是否也可以提取出聊天内容？

衷心地希望您能帮我解惑，不胜感激！

1楼 [wangmingli61](#) 2014-12-11 21:54发表



您好。感谢您的分享！

首先我想说我不懂Android开发，也不太懂数据库。我想通过这个方法把我的聊天记录保存下来方便查看。

几个问题如下，希望您能帮我解答

1.SQLcipher是一个软件还是一个依托别的软件平台才能使用的数据库。如果是前者，那么在什么操作系统下运行？（我在网上找到了所谓的SQLcipher，发现无法在win7下打开，或者不会；虚拟了mac系统，也打不开）。如果是后者，那么用什么软件？怎么操作呢？

2.我是否可以这样理解。博文的第二部分，也就是导入数据库 创建安卓工程 再一堆代码的过程是为了解密的。前面的 手机IMEI + 微信uin 取MD5的前7位 就可以直接不解密而打开数据库 看到聊天内容。（MD5是啥意思？）那样是否也可以提取出聊天内容？

衷心地希望您能帮我解惑，不胜感激！

您还没有登录,请[\[登录\]](#)或[\[注册\]](#)

\* 以上用户言论只代表其个人观点，不代表CSDN网站的观点或立场

核心技术类目

全部主题	Hadoop	AWS	移动游戏	Java	Android	iOS	Swift	智能硬件	Docker	OpenStack
VPN	Spark	ERP	IE10	Eclipse	CRM	JavaScript	数据库	Ubuntu	NFC	WAP
jQuery	BI	HTML5	Spring	Apache	.NET	API	HTML	SDK	IIS	Fedora
XML	LBS	Unity	Splashtop	UML	components	Windows Mobile	Rails	QEMU	KDE	Cassandra
CloudStack	FTC	coremail	OPhone	CouchBase	云计算	iOS6	Rackspace	Web App	SpringSide	
	Maemo	Compuware	大数据	apttech	Perl	Tornado	Ruby	Hibernate	ThinkPHP	HBase
	Pure	Solr	Angular	Cloud Foundry	Redis	Scala	Django	Bootstrap		

公司简介 | 招贤纳士 | 广告服务 | 银行汇款帐号 | 联系方式 | 版权声明 | 法律顾问 | 问题报告 | 合作伙伴 | 论坛反馈

网站客服 杂志客服 微博客服 webmaster@csdn.net 400-600-2320 | 北京创新乐知信息技术有限公司 版权所有 | 江苏乐知网络技术有限公司 提供商务支持  
京 ICP 证 09002463 号 | Copyright © 1999-2014, CSDN.NET, All Rights Reserved