

第十五届CCFC计算机取证技术峰会暨展会

THE 15TH CHINA COMPUTER FORENSIC CONFERENCE & EXHIBITION

■ 电子数据取证技术最新发展与应用 ■

2019.11.5 -11.7

武汉市·荷田大酒店



手机取证案例深度分析

苏州龙信信息科技有限公司

王海啸

手机取证案例

- 支付宝数据提取及恢复
- 手机地图APP取证
- VIVO手机互传备份解密
- 微信7.0.6版本附件取证

支付宝数据提取及恢复

实验准备

1、以安卓支付宝10.1.78为例，测试支付

宝联系人与聊天记录的可恢复性

2、安卓手机（华为MATE20）



支付宝数据提取及恢复

聊天记录

名称

alsn20170807.db-journal

AnnaChatHistory

AnnaChatHistory-journal

aomp_favorite.db

aomp_favorite.db-journal

apm_local

apm_local-journal

birdnest.db

birdnest.db-journal

chat_message.db

chat_message.db-journal

chatmsgdb2088802017344773.db

chatmsgdb2088802017344773.db-encrypt

chatmsgdb2088802017344773.db-shm

com.eg.android.AlipayGphone_PushEvents.db

com.eg.android.AlipayGphone_PushEvents.db-shm

com.eg.android.AlipayGphone_PushEvents.db-wal

contactsdb2088802017344773.db

contactsdb2088802017344773.db-encrypt

contactsdb2088802017344773.db-shm

contactsdb2088802017344773.db-wal

coupon.db

coupon.db-journal

dafile.db

dafile.db-journal

chatmsgdb2088802017344773.db

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	B3	A7	BF	86	82	A9	1E	76	06	1B	77	1D	36	B7	51	BF
00000010	0F	44	8A	BA	63	EF	72	3C	8C	9E	13	60	B3	1F	D0	41
00000020	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000030	9F	F1	48	20	6A	7C	15	BC	4F	71	99	C3	CA	D7	9A	A0
00000040	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000050	57	25	A5	DB	AA	3F	F7	D5	70	AF	A4	CC	6F	0A	50	5E
00000060	95	1F	78	B4	71	59	AB	76	D4	E8	39	E9	00	0B	BC	55
00000070	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000080	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000090	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000000A0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000000B0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000000C0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000000D0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000000E0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000000F0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000100	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000110	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000120	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000130	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000140	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000150	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000160	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000170	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000180	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
00000190	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000001A0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000001B0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000001C0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000001D0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000001E0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48
000001F0	27	34	DF	91	7C	C6	BB	5C	31	EB	58	13	64	F0	4C	48

chatmsgdb.db

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	53	51	4C	69	74	65	20	66	6F	72	6D	61	74	20	33	00
00000010	04	00	02	02	00	40	20	20	8B	0F	81	19	00	00	00	01
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	8B	0F	81
00000060	00	2E	01	5A	0D	00	00	00	00	00	04	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

数据加密方式是对整个数据库文件进行加密的，因此需要对相关数据文件进行解密才能进行分析与恢复

支付宝数据提取及恢复

联系人

ali_account记录了通讯录的联系人

chatgroup_info记录了通讯录的群

contactsdb

ali_account

android_metadata

chat_relation

chatgroup_info

contact_ext_info

contact_relation

gpannounce_relation

ignore_stranger

new_friend

person_recommend

personal_wall_relation

recent_session

recent_session_tip

recommendation_friend

user_label

DatabaseExtensionsSchemaSQL BuilderSQLDataDesignDDLScripting

Refresh

RecNo	_id	name	headImageUrl	account	nickName	remarkName	gender	signature	userGrade	source
1	2088802017344773	通	http://tfs.alipayobjects.com/images/partner/T1g7XeKpfXXXXX_160X160	18151782	/Alipay	(null)	m	(null)	黄金会员	
2	2088702799555995	傅	http://tfs.alipayobjects.com/images/partner/T1FOFXeVaXXXXX_160X160	158*****90	的前的鱼妈	(null)	f	(null)	大众会员	通过好
3	2088702977494283		http://tfs.alipayobjects.com/images/partner/T1gbNvXhNaXXXXX_160X160	812***@qq.com			m	(null)	铂金会员	通过扫
4	2088302308720683	何	http://tfs.alipayobjects.com/images/partner/T1TORdXn0lXXXXX_160X160	180*****62		(null)	m	(null)	黄金会员	通过扫
5	2088102551463890		http://tfs.alipayobjects.com/images/partner/TB1dWq6XnP891l_ugXXXWkVXa_160X160	mai***@rebiekong.com		(null)	m	(null)	铂金会员	通过好
6	2088702475269673		http://tfs.alipayobjects.com/images/partner/TB1BfNJXw1JDunXXX3KFXa_160X160	152*****80		kity	f		大众会员	通过手
7	2088102952333279		http://tfs.alipayobjects.com/images/partner/T1FotvXfBfXXXXX_60X160	113***@qq.com		佑	m	(null)	黄金会员	通过好
8	2088512437949312	(nu	http://tfs.alipayobjects.com/images/partner/TB1jP_aRhDDUNXXc7pXa_160X160	139***1725		(ni	m	(null)	(null)	(null)
9	2088002962420128		http://tfs.alipayobjects.com/images/partner/T1qu0mXhVgXX_160X160	111***@qq.com	小小虫要做超人		f	用钱砸死我吧。	黄金会员	通过好
10	2088002712579348	王	http://tfs.alipayobjects.com/images/partner/T1sEJeXdVcXXX_160X160	wan***@163.com		海	m	(null)	铂金会员	通过好
11	2088702160052711	王	http://tfs.alipayobjects.com/images/partner/T1ijRdXlRjXXXXX_60X160	186*****57		(nu	m	(null)	黄金会员	通过好
12	2088802593487673	(nu	http://tfs.alipayobjects.com/images/partner/T1CoXjXn4XXXXX_160X160	130***3102		(null)	f	(null)	(null)	(null)
13	2088612807332703		http://tfs.alipayobjects.com/images/partner/TB1rrtX.qHDunXXPwXXa_160X160	150*****21		(null)	m	(null)	大众会员	(null)
14	2088412242417180	(null)	http://tfs.alipayobjects.com/images/partner/TB1VLKWbgSJLXqXXbesFXa_160X160	137***2654		(null)	m	(null)	(null)	(null)
15	2088632147671580	(null)	http://tfs.alipayobjects.com/images/partner/TB1t4AxbRCDuTXXbOEpXa_160X160	134***2866	的小号	(null)	f	(null)	(null)	(null)

<Filter is Empty>

Customize...

支付宝数据提取及恢复

聊天记录

Group_chat_xxxxxxxxxxxx记录了一个群的聊天记录

Peronal_chat_yyyyyyyyyyyy记录了一个人的聊天记录

contactsdb

chatmsgdb

android_metadata

group_chat_018790000020190717104518775

group_chat_0260310000020190520100637778

group_chat_0927060000520190625093230770

personal_chat_2088002962420128

personal_chat_2088102952333279

personal_chat_2088802017344773

resource_chat

uploading_msg

DatabaseExtensionsSchemaSQL BuilderSQLDataDesignDDLScripting

Refresh

RecNo	localId	clientMsgId	createTime	bizType	bizMemo	bizIcon	templateCode	ter
1	1572681084534	2088802017344773@1157268127329275	1572681273292	CHAT	你好	(null)	11	['n
2	1572681084535	st_191102155433778566	1572681273716	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	['n 好; hr e= &s
3	1572681084536	2088802017344773@2157268131867046	1572681318670	CHAT	测试支付宝	(null)	11	['n
4	1572681084537	st_191102155519770919	1572681319057	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	['n 好; hr e= &s
5	1572681084538	2088802017344773@3157268132450013	1572681324499	CHAT	[图片]	(null)	14	['h . '
6	1572681084539	st_191102155526770407	1572681326148	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	['n 好; hr e= &s
7	1572681084541	st_191102155550772961	1572681350677	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	['n 好; hr e= &s
8	1572681084542	2088802017344773@4157268134800325	1572681354906	CHAT	[小视频]	(null)	19	['h . ' Pi F
9	1572681084543	st_191102155555772975	1572681355299	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	['n 好; hr e= &s
10	1572682899725	2088802017344773@1157268294148855	1572682941488		[小程序]支日历	(null)	1102	['a . ' ' //e

<Filter is Empty>

Customize...

支付宝数据提取及恢复

删除方式与数据痕迹

逻辑删除

原理上是执行了update或replace的sql操作，以支付宝通讯录为例，删除“2088002962420128”这个人实际上是更新了好友状态，如下为删除好友的前后变化



删除的数据

支付宝数据提取及恢复

对比发现是记录的friendStatus由2变为0

Database: contactsdb Table: main.ali_account File: C:\Users\Tony\Desktop\支付宝(old)\contactsdb.db SQLite Library: [internal] version 3.8.5

RecNo	_id	name	headImageUrl	account	nickName	friendStatus	remarkName	gender	signature
1	2088802017344773		http://fs.alipayobjects.com/images/partner/T1g7XkXep0000X_160X160	<11>01	T...pay	1 (null)	m	(null)	
2	2088702799555995		http://fs.alipayobjects.com/images/partner/T1FOFkXkXa0000X_160X160	158****90	大...的渔码	1 (null)	f	(null)	
3	2088702977494283		http://fs.alipayobjects.com/images/partner/T1g0NkXa0000X_160X160	812***@qq.com	信	2	m	(null)	
4	2088302308720683		http://fs.alipayobjects.com/images/partner/T1TORkXkXa0000X_160X160	180****62	信	1 (null)	m	(null)	
5	2089102551463890		http://fs.alipayobjects.com/images/partner/T1dWqkXkXa0000X_160X160	mai***@rebiekong.com		1 (null)	m	(null)	
6	2088702475269673		http://fs.alipayobjects.com/images/partner/T1B1BNkXkXa0000X_160X160	152****80	1 kty	f	(null)	(null)	
7	2089102952332729		http://fs.alipayobjects.com/images/partner/T1F0hXkXa0000X_160X160	1113***@qq.com		1	m	(null)	
8	2088512437949312	(null)	http://fs.alipayobjects.com/images/partner/T1B1P2kXkXa0000X_160X160	EIX 139****1725		0 (null)	m	(null)	
9	208800296240128		http://fs.alipayobjects.com/images/partner/T1qu0mXkXa0000X_160X160	111***@qq.com	小小主要做运人	2	f	月亮是死吧	
10	2088002712579348		http://fs.alipayobjects.com/images/partner/T1k6LkXkXa0000X_160X160	XXXXXXX wan***@163.com		1	m	(null)	
11	2088702160052711	王	http://fs.alipayobjects.com/images/partner/T1jkdXkXa0000X_160X160	XXXXXXX 1 186****57		1 (null)	m	(null)	
12	2088802593487673	(n	http://fs.alipayobjects.com/images/partner/T1CoXXXXXXX 130****3102			0 (null)	f	(null)	
13	2088612807332703		http://fs.alipayobjects.com/images/partner/T1B1mXXXXX 150****21			0 (null)	m	(null)	
14	2088412242417180	(n	http://fs.alipayobjects.com/images/partner/T1B1VXXXXX 137****2654			0 (null)	m	(null)	
15	2088632147671580	(null)	http://fs.alipayobjects.com/images/partner/T1B14XXXXX 134****2866			0 (null)	f	(null)	

Database: contactsdb Table: main.ali_account File: C:\Users\Tony\Desktop\支付宝(new)\contactsdb.db SQLite Library: [internal] version 3.8.5

RecNo	_id	name	headImageUrl	account	nickName	friendStatus	remarkName	gender	signature
1	2088802017344773		http://fs.alipayobjects.com/images/partner/T1g7XkXep0000X_160X160	<181>1301	Tc...pay	1 (null)	m	(null)	
2	2088702799555995		http://fs.alipayobjects.com/images/partner/T1FOFkXkXa0000X_160X160	158****90	大...的渔码	1 (null)	f	(null)	
3	2088702977494283		http://fs.alipayobjects.com/images/partner/T1g0NkXa0000X_160X160	812***@qq.com	信	2	m	(null)	
4	2088302308720683		http://fs.alipayobjects.com/images/partner/T1TORkXkXa0000X_160X160	180****62	信	1 (null)	m	(null)	
5	2089102551463890		http://fs.alipayobjects.com/images/partner/T1dWqkXkXa0000X_160X160	mai***@rebiekong.com		1 (null)	m	(null)	
6	2088702475269673		http://fs.alipayobjects.com/images/partner/T1B1BNkXkXa0000X_160X160	152****80	1 kty	f	(null)	(null)	
7	2089102952332729		http://fs.alipayobjects.com/images/partner/T1F0hXkXa0000X_160X160	1113***@qq.com		1	m	(null)	
8	2088512437949312		http://fs.alipayobjects.com/images/partner/T1B1P2kXkXa0000X_160X160	EIX 139****1725		0 (null)	m	(null)	
9	208800296240128		http://fs.alipayobjects.com/images/partner/T1qu0mXkXa0000X_160X160	111***@qq.com	小小主要做运人	0	f	月亮是死吧	
10	2088002712579348		http://fs.alipayobjects.com/images/partner/T1k6LkXkXa0000X_160X160	XXXXXXX wan***@163.com		1	m	(null)	
11	2088702160052711	王	http://fs.alipayobjects.com/images/partner/T1jkdXkXa0000X_160X160	XXXXXXX 1 186****57		1 (null)	m	(null)	
12	2088802593487673	(n	http://fs.alipayobjects.com/images/partner/T1CoXXXXXXX 130****3102			0 (null)	f	(null)	
13	2088612807332703		http://fs.alipayobjects.com/images/partner/T1B1mXXXXX 150****21			0 (null)	m	(null)	
14	2088412242417180	(n	http://fs.alipayobjects.com/images/partner/T1B1VXXXXX 137****2654			0 (null)	m	(null)	
15	2088632147671580	(null)	http://fs.alipayobjects.com/images/partner/T1B14XXXXX 134****2866			0 (null)	f	(null)	

支付宝数据提取及恢复

物理删除

原理上是执行了delete或drop的sql语句，以支付宝聊天记录为例，当解除了“2088002962420128”好友关系后，原本的聊天记录被清空，如下为删除前后的情况如下图所示

Database: chatmsgdb Table: main.personal_chat_2088002962420128 File: C:\Users\Tony\Desktop\支付宝\old\chatmsgdb.db SQLite Library: [internal] version 3.8.6

RecNo	localId	clientMsgId	createTime	bizType	bizMemo	bizIcon	templateCode	templateData
1	1572681084534	2088802017344773@1157268127329275	1572681273292	CHAT	你好	(null)	11	["m": "你好"]
2	1572681084535	st_191102155433778566	1572681273716	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	["m": "小小虫", "type": "friend_verification_request", "href": "\alipay", "e": "addfriend", "source": "by"]
3	1572681084536	2088802017344773@2157268131867046	1572681318670	CHAT	测试支付宝	(null)	11	["m": "测试支付"]
4	1572681084537	st_191102155519770919	1572681319057	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	["m": "小小虫", "type": "friend_verification_request", "href": "\alipay", "e": "addfriend", "source": "by"]
5	1572681084538	2088802017344773@3157268132450013	1572681324499	CHAT	[图片]	(null)	14	["h": 1920, "i": " ", "w": 1080]
6	1572681084539	st_191102155526770407	1572681326148	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	["m": "小小虫", "type": "friend_verification_request", "href": "\alipay", "e": "addfriend", "source": "by"]
7	1572681084541	st_191102155550772961	1572681350677	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	["m": "小小虫", "type": "friend_verification_request", "href": "\alipay", "e": "addfriend", "source": "by"]
8	1572681084542	2088802017344773@4157268134800325	1572681354906	CHAT	[小视频]	(null)	19	["h": 640, "size": "time": 500, "PiRroXKwAu"]
9	1572681084543	st_191102155555772975	1572681355299	SYSTEM	小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。	(null)	8003	["m": "小小虫", "type": "friend_verification_request", "href": "\alipay", "e": "addfriend", "source": "by"]
10	1572682899725	2088802017344773@1157268294148855	1572682941488		[小程序]支日历	(null)	1102	["appDesc": " ", "image": "A", "appstoreis"]

支付宝数据提取及恢复

删除后的数据

Database: chatmsgdb Table: main.personal_chat_2088002962420128 File: C:\Users\Tony\Desktop\支付宝\new\chatmsgdb.db SQLite Library: [internal] version 3.8.6

chatmsgdb

- android_metadata
- group_chat_0187900000020190717104518775
- group_chat_0260310000020190520100637778
- group_chat_0927060000520190625093230770
- personal_chat_2088002962420128
- personal_chat_2088102952333279
- personal_chat_2088802017344773
- resource_chat_
- uploading_msg

Database Extensions Schema SQL Builder SQL Data Design DDL Scripting

Refresh

RecNo	localId	clientMsgId	createTime	bizType	bizMemo	bizIcon	templateCode	templateData
Click here to define a filter								
<No data to display>								

<Filter is Empty>Customize...

支付宝数据提取及恢复

以“你好”这条消息为例来检查数据痕迹，将数据转为utf8编码格式即“E4 BD A0 E5 A5 BD”，16进制的方式搜索删除后的数据库文件，情况如下

chatmsgdb.db

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000022B0	31	31	2A	2A	2A	40	71	71	2E	63	6F	6D	26	73	6F	75	11***@qq.com&sou
000022C0	72	63	65	3D	62	79	5F	66	5F	76	26	61	6C	65	72	74	rce=by_f_v&alert
000022D0	3D	74	72	75	65	5C	22	3E	E5	8F	91	E9	80	81	E5	A5	=true\">ã. 'éÉ.ã¥
000022E0	BD	E5	8F	8B	E9	AA	8C	E8	AF	81	3C	2F	61	3E	22	7D	%ã.<é*Gè-."}
000022F0	02	A6	EE	65	DA	71	11	FF	53	59	53	54	45	4D	7B	7D	..!ieŮq.ÿSYSTEM{}
00002300	7B	22	65	78	70	72	65	73	73	69	6F	6E	53	74	61	74	{"expressionStat
00002310	65	22	3A	30	2C	22	61	75	64	69	6F	53	74	61	74	65	e":0,"audioState
00002320	22	3A	30	2C	22	67	61	6D	65	53	74	61	74	65	22	3A	":0,"gameState":
00002330	30	7D	04	30	63	37	33	64	63	31	34	37	30	33	62	64	0}.0c73dcl4703bd
00002340	36	34	65	63	37	63	33	66	61	32	37	34	32	62	36	30	64ec7c3fa2742b60
00002350	37	39	34	5F	31	39	31	31	30	32	31	35	35	34	33	33	794_191102155433
00002360	37	37	35	36	31	35	81	17	01	1D	05	4F	05	15	19	00	775615.....O....
00002370	11	29	09	00	00	08	00	00	71	08	00	01	08	09	08	00	.).....q.....
00002380	08	08	00	09	08	00	01	6E	2B	18	EE	76	32	30	38	38	n+.iv2088
00002390	38	30	32	30	31	37	33	34	34	37	37	33	40	31	31	35	802017344773@115
000023A0	37	32	36	38	31	32	37	33	32	39	32	37	35	01	6E	2B	72681273429275.n+
000023B0	1B	CF	CC	43	48	41	54	E4	BD	A0	E5	A5	BD	31	31	7B	.!iCHATA%ã¥%ll{
000023C0	22	6D	22	3A	22	E4	BD	A0	E5	A5	BD	22	7D	7B	22	65	"m": "%ã¥ã¥"}{"e
000023D0	78	70	72	65	73	73	69	6F	6E	53	74	61	74	65	22	3A	xpressionState":
000023E0	30	2C	00	00	00	3D	0B	00	00	00	25	0A	00	00	00	24	0,...=%....\$
000023F0	09	00	00	00	22	07	00	00	00	20	05	00	00	00	1F	03	".....
00002400	0A	00	00	00	00	04	00	00	03	DB	02	C1	03	9B	03	5B	Ů.Á.>.[
00002410	03	1B	03	C1	03	81	03	41	03	01	02	E7	02	A7	00	00	...Á...A...ç.\$..
00002420	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00002430	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00002440	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00002450	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00002460	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00002470	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00002480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00002490	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000024A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

偏移: 23C5 块: 23C5-23CA 长度: 6 只读 覆盖

说明安卓支付宝的聊天记录删除方式并不是完全的清0，还是有痕迹残留

支付宝数据提取及恢复

需要结合sqlite文件结构与聊天记录的表结构进行分析恢复即可还原相关记录，在用取证工具对微信数据进行解析：

显示全部对话

搜索当前对话内容

搜索

序号	数据状态	名称(ID)	消息总数
1	已删除	佑宝(2088102952333279)	49\3
2	已删除	小小虫要做超人 (2088002962420128)	3\0
3	存在	TonyAlipay(2088802017344...	0\4

显示全部消息

搜索当前消息内容

搜索

小小虫要做超人开启了好友验证,你还不是他(她)好友。请先发送好友验证请求,对方验证通过后,才能聊天。[发送好友验证](#)

2019-11-02 15:54:33

已删除 TonyAlipay(2088802017344773)

你好

2019-11-02 15:54:33

已删除 TonyAlipay(2088802017344773)

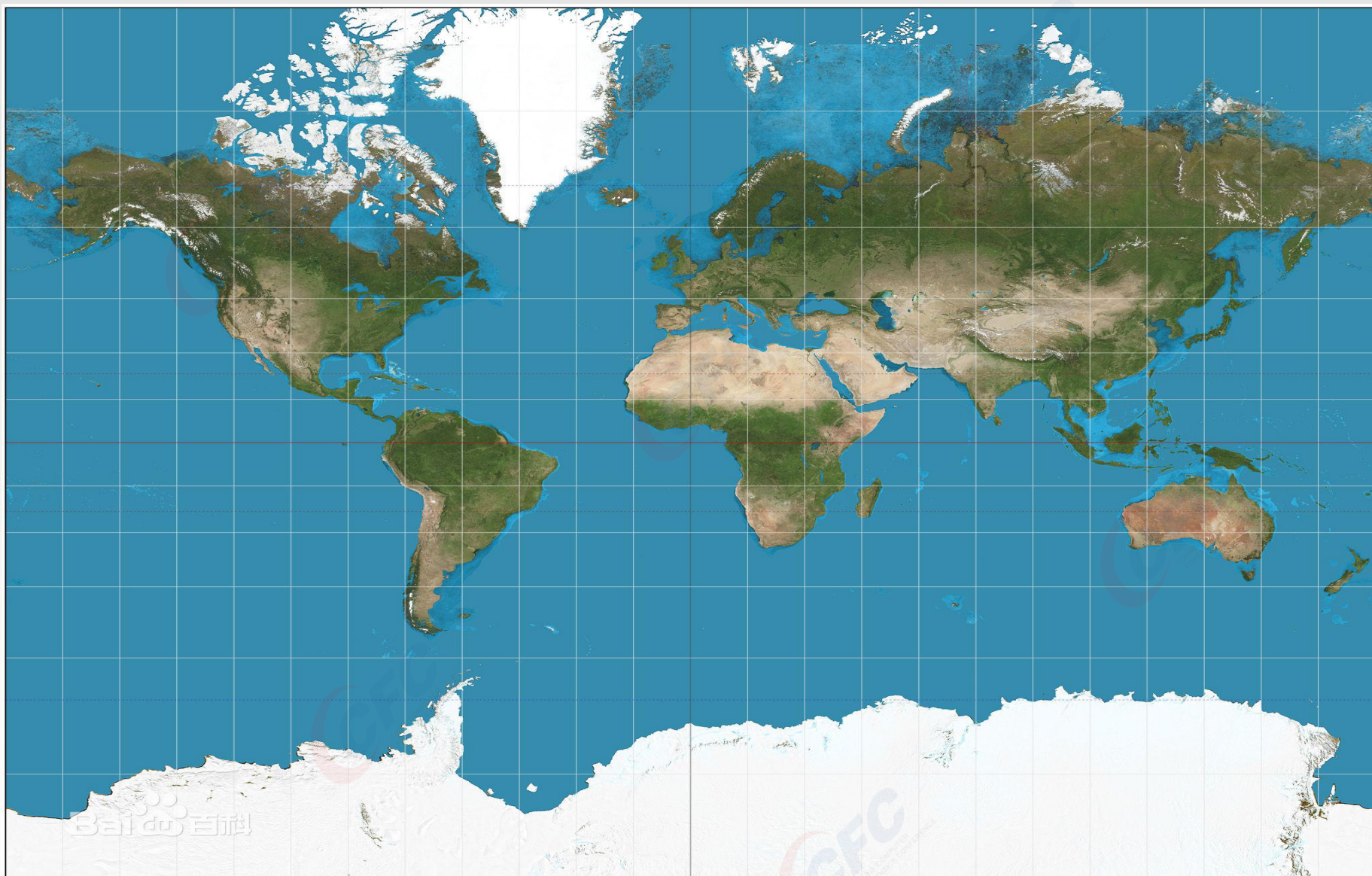
测试支付宝

2019-11-02 15:55:18

手机取证案例

- 支付宝数据提取及恢复
- 手机地图APP取证
- VIVO手机互传备份解密
- 微信7.0.6版本附件取证

手机地图APP取证



手机地图APP取证

实验准备

- 1、百度地图：10.20.0.950
- 2、安卓手机一部



手机地图APP取证

足迹点

足迹记录了一个人某段时间的轨迹，它支持上传到云端，也支持从云端同步到本地。



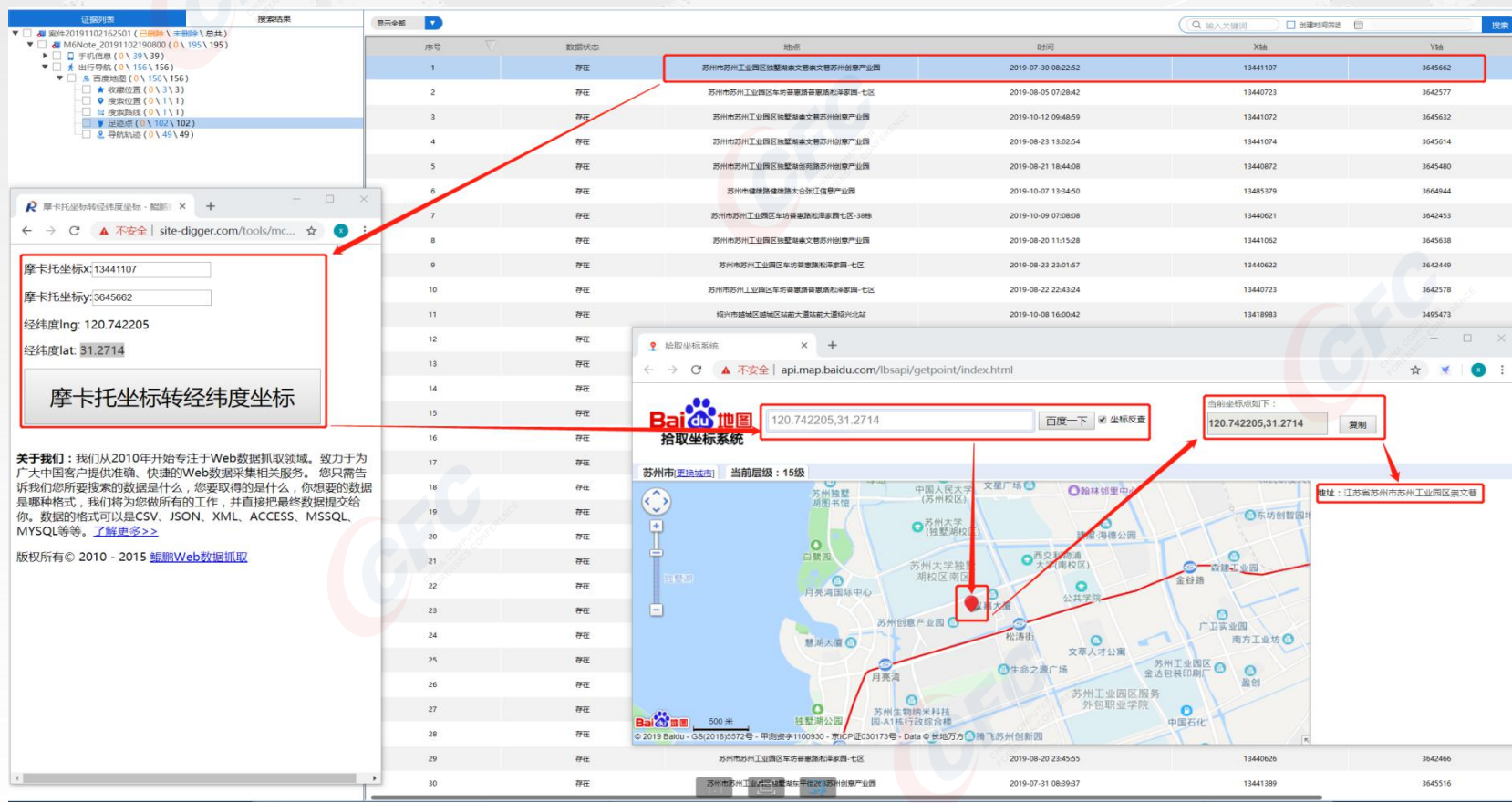
手机地图APP取证

RecNo	guid	type	lng	lat	city_name	district	business	street	street_num	poi_name	tags	image_list	last_time	poi_id	poi_type	data_from	detail
Click here to define a filter																	
1	22af0be4-da25-4c64-b35f-2c64ca272087	loc	13441061	3645645	苏州市	苏州工业园区	独墅湖	康文巷	康文巷	苏州创意产业园				b83c68af5d685942c9e33cf7	公司企业园区	mapinit	
2	d9d06dfd-3f4d-4db1-9c9b-f92d6f62a880	loc	13440732	3642583	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区				78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
3	e0e07fa9-47af-48b9-8988-ba03436dacb1	loc	13440425	3643837	苏州市	苏州工业园区	独墅湖	星湖街	星湖街	北高				b703e96b9ca399fa8f1a891d	行政地标;村庄	mapinit	
4	2a0d7f0f-4be5-4431-8f9b-328e26ac5a59	loc	13439704	3644134	苏州市	苏州工业园区	独墅湖	若水路	若水路	独墅湖邻里中心(地铁站)				044dd93534c0232ab54f54d9		mapinit	
5	262d8a26-f973-4c0c-82f8-048b73aca0dc	loc	13428495	3650750	姑苏区	南门	人民路	1135号	姑苏公安分局交警大队					510b5f09eb6a31c49968b43c	政府机构	mapinit	
6	a0e89e4f-28cb-4f77-903b-95662d9def10	loc	13441347	3645470	苏州市	苏州工业园区	独墅湖	东平街	东平街	苏州创意产业园				b83c68af5d685942c9e33cf7	公司企业园区	mapinit	
7	0CB48AE4-D2A6-4F97-8EC4-8A9FE28FC73F	loc	13441062	3645638	苏州市	苏州工业园区	独墅湖	康文巷		苏州创意产业园			[1566301541]		公司企业园区	mapinit	
8	6D3876DE-EF66-4AF5-9044-6D41ED0DFD10	loc	13441065	3645639	苏州市	苏州工业园区	独墅湖	康文巷		苏州创意产业园			[1566384020]		公司企业园区	mapinit	
9	4290310D-DD13-4AD3-8E0F-0DD84E8159EE	loc	13441069	3645642	苏州市	苏州工业园区	独墅湖	康文巷		苏州创意产业园			[1566478577]		公司企业园区	mapinit	
10	0A4C5AA2-3B5F-4FCB-AD20-210F6429038	loc	13441074	3645614	苏州市	苏州工业园区	独墅湖	康文巷		苏州创意产业园			[1566559517]		公司企业园区	mapinit	
11	15BBDFEA-6097-47EC-B99C-ACC086FDA8E9	loc	13440620	3642459	苏州市	苏州工业园区	车坊	普惠路		松泽家园-七区					房地产;住宅区	mapinit	
12	4F8A4F46-1DFE-41F9-8E26-3F62F90AC1EA	loc	13441075	3645623	苏州市	苏州工业园区	独墅湖	康文巷		苏州创意产业园					公司企业园区	mapinit	
13	3272DA77-FB9F-4AC3-8DC9-EDCB8F017AD	loc	13440626	3642466	苏州市	苏州工业园区	车坊	普惠路		松泽家园-七区					房地产;住宅区	mapinit	
14	0AC6F268-2AD2-42A7-9846-3515180818FF	loc	13440872	3645480	苏州市	苏州工业园区	独墅湖	创苑路		苏州创意产业园					公司企业园区	navidest	
15	94ED19CA-4382-46A3-B246-C5576C17DC8F	loc	13440259	3645067	苏州市	苏州工业园区	独墅湖	创苑路		月亮湾(地铁站)						navidest	
16	98DC7578-944C-458B-838E-2117E2B9EE54	loc	13440223	3644875	苏州市	苏州工业园区	独墅湖	星湖街		生物堡					房地产;住宅区	navidest	
17	26C344B3-96F3-48DC-9FBC-78308A19F0B7	loc	13440339	3643973	苏州市	苏州工业园区	独墅湖	星湖街		北高					行政地标;村庄	navidest	
18	F33DFC6A-EA81-4C50-AE2C-9AF3343DBA54	loc	13440200	3643687	苏州市	苏州工业园区	独墅湖	启月街	1号	北高					行政地标;村庄	navidest	
19	9ADD4D77-5A12-4B3E-A049-E6DB8906363D	loc	13440622	3643318	苏州市	苏州工业园区	车坊	星湖街		松泽家园八区					房地产;住宅区	navidest	
20	EFE8B4C3-4881-410F-B445-48FEA4D7B1DC	loc	13440716	3642787	苏州市	苏州工业园区	车坊	普惠路		松泽家园八区					房地产;住宅区	navidest	
21	C886B02E-D490-4FBF-BBCA-0B75C2135061	loc	13440648	3642479	苏州市	苏州工业园区	车坊	普惠路		松泽家园-七区					房地产;住宅区	navidest	
22	7677B070-8EC9-4C3E-81AC-B032D67C8854	loc	13440454	3643828	苏州市	苏州工业园区	独墅湖	星湖街		同程大厦					房地产;写字楼	navidest	
23	D14C5CD3-C392-4C84-9C08-660515A9EADE	loc	13440604	3642475	苏州市	苏州工业园区	车坊	普惠路		松泽家园-七区					房地产;住宅区	mapinit	
24	0DAC97E5-3522-4BD4-8CD3-ED3B145B4DB8	loc	13440622	3642449	苏州市	苏州工业园区	车坊	普惠路		松泽家园-七区					房地产;住宅区	mapinit	
25	B827F539-540B-48A0-98A1-FF998DABFE83	loc	13440638	3642544	苏州市	苏州工业园区	车坊	普惠路		松泽家园-七区					房地产;住宅区	mapinit	
26	4513241c-abfa-4ff7-a537-da0d2f201205	loc	13441387	3645516	苏州市	苏州工业园区	独墅湖	东平街	268	苏州创意产业园			[1564370602]	b83c68af5d685942c9e33cf7	公司企业园区	mapinit	
27	00f226e1-fd88-4b1a-adf8-0a2ac99f4024	loc	13441107	3645662	苏州市	苏州工业园区	独墅湖	康文巷	康文巷	苏州创意产业园			[1564451362]	b83c68af5d685942c9e33cf7	公司企业园区	mapinit	
28	3f7740cf-fd53-466e-b238-c5b8cdd2dbee	loc	13440711	3642912	苏州市	苏州工业园区	车坊	星湖街	星湖街	松泽家园八区				9ee7cc7835bff00d16c9057e	房地产;住宅区	mapinit	
29	3aafdd5f-6cc9-42de-91b1-974b704a753a	loc	13441389	3645516	苏州市	苏州工业园区	独墅湖	东平街	268	苏州创意产业园			[1564533659]	b83c68af5d685942c9e33cf7	公司企业园区	mapinit	
30	9f6a7289-ec24-4dd3-bb36-bd74e0738e75	loc	13440711	3642912	苏州市	苏州工业园区	车坊	星湖街	星湖街	松泽家园八区				9ee7cc7835bff00d16c9057e	房地产;住宅区	mapinit	
31	62412562-a22c-4d1f-92d7-97a8698482f0	loc	13440722	3642577	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区			[1564670764]	78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
32	763816b9-9764-475f-9c8e-6c29bbf8506a	loc	13440723	3642577	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区				78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
33	8c9f9e6a-4707-451a-ab3d-56fcfe667a8	loc	13440723	3642577	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区				78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
34	5f2fb485-23d8-481e-b239-e598647fe63b	loc	13440723	3642577	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区			[1564895753]	78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
35	dd4c1dd2-7614-4733-ad9d-e046387cce8b	loc	13441341	3643010	苏州市	苏州工业园区	车坊	惠松街	惠松街	车坊农贸市场				480dc1f09caa284ef13cbaaa	购物;购物中心	navidest	
36	054b01a5-b4dd-443f-b2ba-c9ff3e692c42	loc	13440723	3642577	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区				78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
37	b3cce7f1-e36b-4a01-9414-c90281b3a96f	loc	13440645	3642868	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园八区				9ee7cc7835bff00d16c9057e	房地产;住宅区	mapinit	
38	2edaeb7-df8f-4a3a-8479-5d7f68b2db59	loc	13440723	3642577	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区			[1565047773]	78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
39	fa580f05-af52-4f05-bec8-2b7d44ef6bdd	loc	13440646	3642422	苏州市	苏州工业园区	车坊	苏州工业园区		松泽家园-七区				78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
40	212c54cc-9194-4d53-a589-101f7456ded5	loc	13440722	3642578	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区				78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
41	7f34ed14-153a-49ee-97c5-b6f2b5170f5b	loc	13441307	3645543	苏州市	苏州工业园区	独墅湖	葫芦浜巷	葫芦浜巷	苏州创意产业园			[1565247584]	b83c68af5d685942c9e33cf7	公司企业园区	mapinit	
42	e04ea473-6844-4506-bfb9-49341c43e174	loc	13440723	3642578	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区				78bd50f76c27172631870a7e	房地产;住宅区	mapinit	
43	dee22703-76a1-4fc2-b9d9-c0f629740c91	loc	13440269	3642582	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园(八区西三期)				20a21fda211f8dd60782c2be	房地产;住宅区	mapinit	
44	6100-2b0-0-2-17-0-103-0704-07-2-1	loc	13440764	3642530	苏州市	苏州工业园区	车坊	普惠路	普惠路	松泽家园-七区				78bd50f76c27172631870a7e	房地产;住宅区	mapinit	

<Filter is Empty>

Customize...

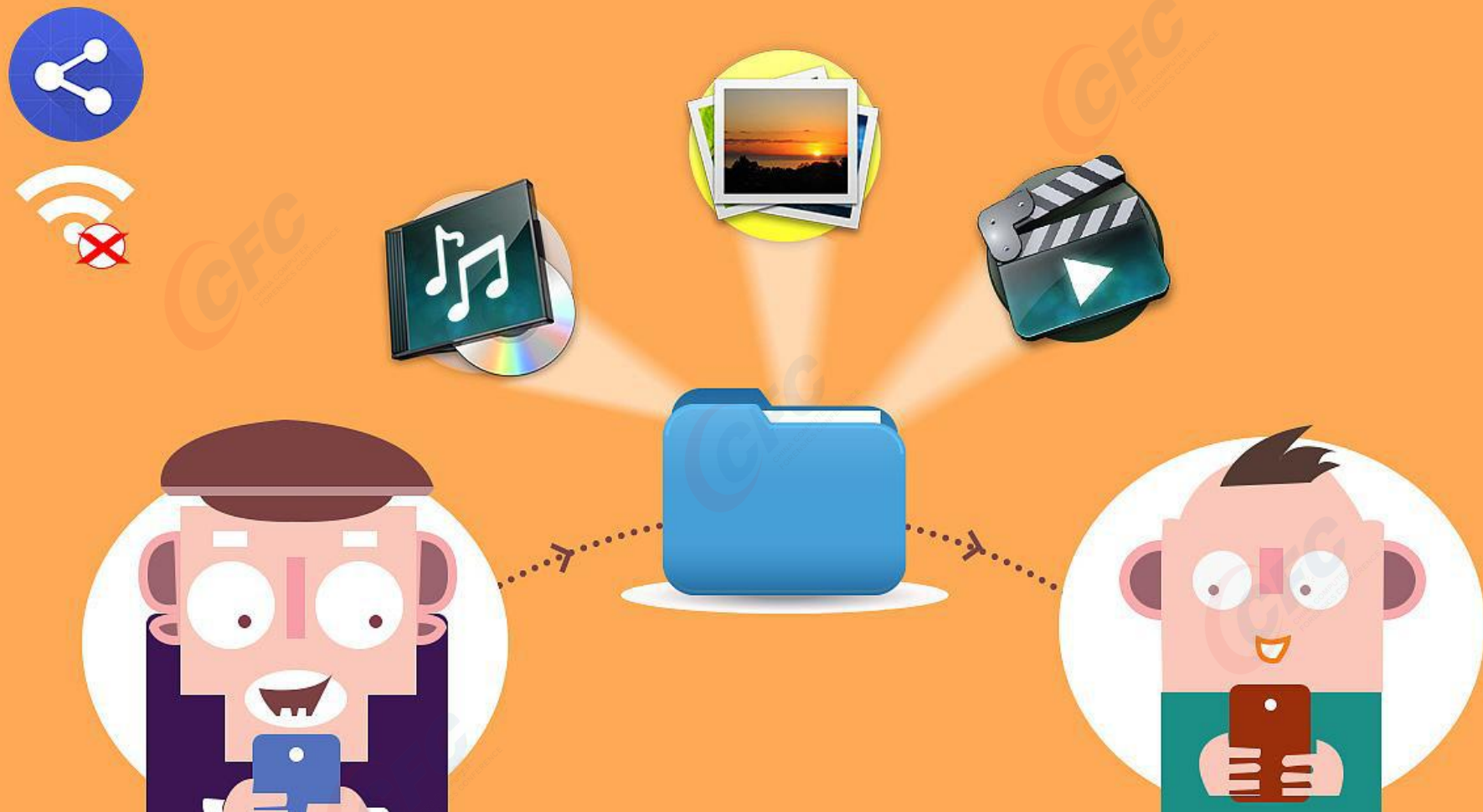
墨卡托(Mercator)投影，又名“等角正轴圆柱投影”，荷兰地图学家墨卡托(Mercator)在1569年拟定，假设地球被围在一个中空圆柱里，其赤道与圆柱相接触，然后再假想地球中心有一盏灯，把球面上的图形投影到圆柱体上，再把圆柱体展开，这就是一幅标准纬线为零度(即赤道)的“墨卡托投影”绘制出的世界地图。



手机取证案例

- 支持宝数据提取及恢复
- 手机地图APP取证
- **VIVO手机互传备份解密**
- 微信7.0.6版本附件取证

VIVO手机互传备份解密



VIVO手机互传备份解密



目前VIVO手机取证主要提取方式有以下5种方式：

(1) 互传获取：一种适用于两个vivo手机或vivo手机与电脑间的数据传输；

(2) 应用降级备份获取：通过对应用程序的版本降级，将数据库数据进行备份提取，主要代表有QQ、微信、支付宝等；

(3) vivo手机助手备份：官方早期提供的手机助手来备份，主适用于早期安卓版本6以下的vivo手机；

(4) 镜像获取：通过手机的芯片（高通或MTK）进行回读来完成整个手机数据的获取；

(5) 提权获取（ROOT），通过系统漏洞刷入第三方固件来获取root权限。

VIVO手机互传备份解密



通过“互传”方式是目前各大厂商手机取证选定的提取方式（因安卓系统高版本目前很难提权或镜像）

那么问题来了！

- （1）如果“互传”工具官方升级，取证工具提取端未及时更新。
- （2）使用者将手机数据备份到电脑端（加密）。

面对以上2个问题，我们该如何解决了？

本次交流就重点围绕互传（PC端）提取、备份解析、应用数据识别、数据解密、取证分析进行一次完整地介绍。

VIVO手机互传备份解密

工具准备：

1、互传Windows版（系统版本：2.0.5.0）

功能简介：

电脑安装互传，手机与备份助手连接。

通过备份助手可以备份手机上几乎所有数据。

具体数据如：应用数据（微信、浏览器等）

2、Vivo Z3手机（系统版本：安卓8.1）



VIVO手机互传备份解密

备份步骤：

Step1：安装互传并连接手机

安装好互传软件并打开，连接手机打开设置允许usb调试模式，保证软件正常识别手机。



VIVO手机互传备份解密

Step2: 设置备份路径

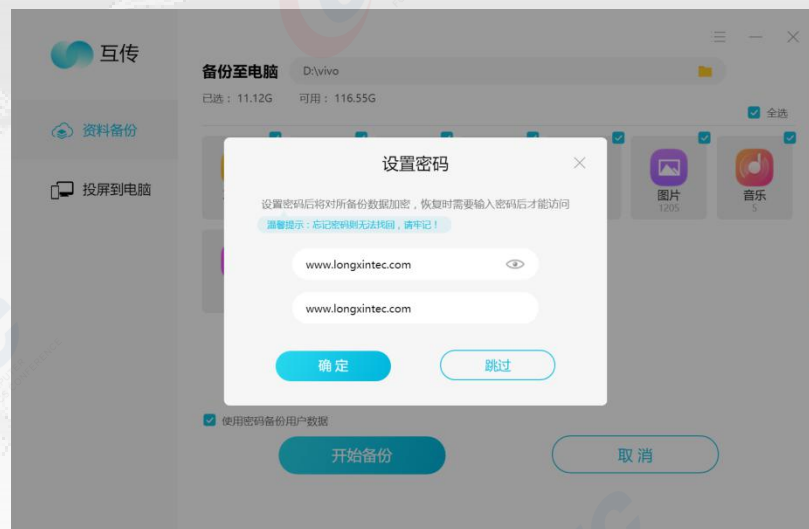
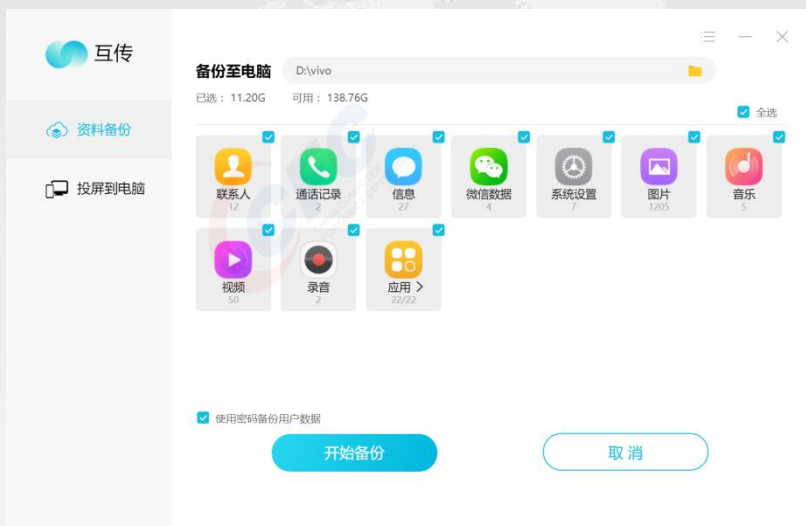
选择一个容量足够的磁盘作为备份目录，防止空间不足。



VIVO手机互传备份解密

Step3: 新建加密备份

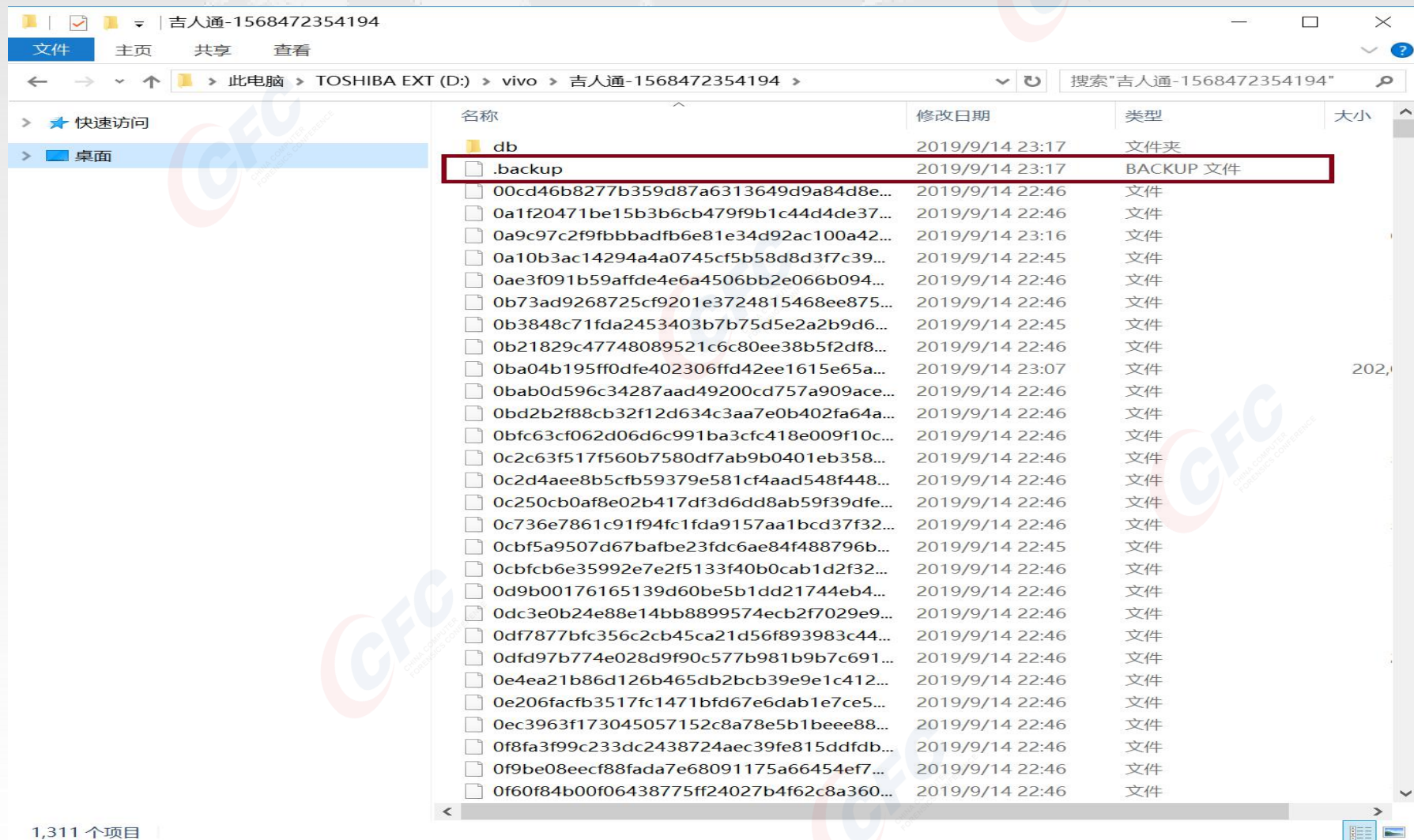
筛选好数据并设置密码，备份微信数据。



VIVO手机互传备份解密

加密状态识别

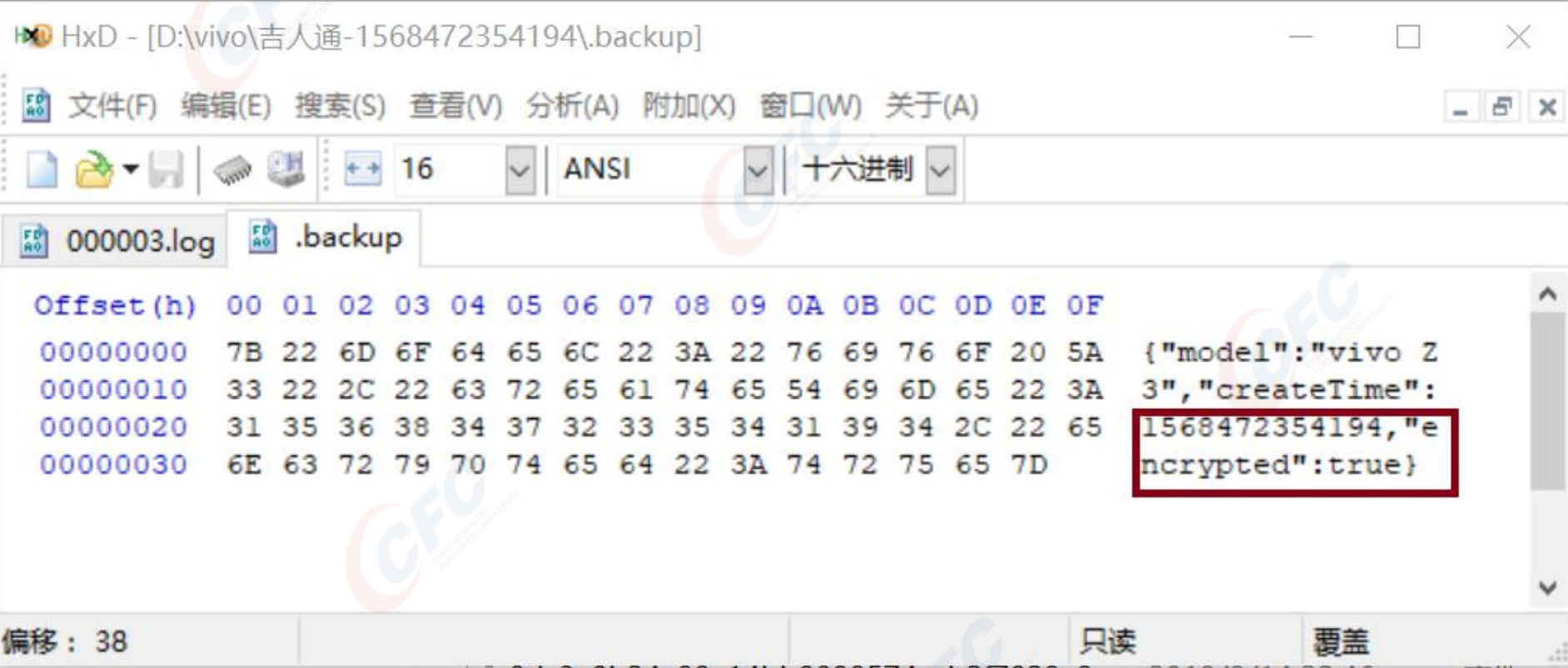
在生成的备份文件夹中找到“.backup”文件，如下图所示：



VIVO手机互传备份解密

然后将该文件用HxD工具打开，进行十六制分析，内容为json格式内容，发现“encrypted”字段为“true”表示备份为加密状态，如图7所示。（true: 加密，false: 未加密）

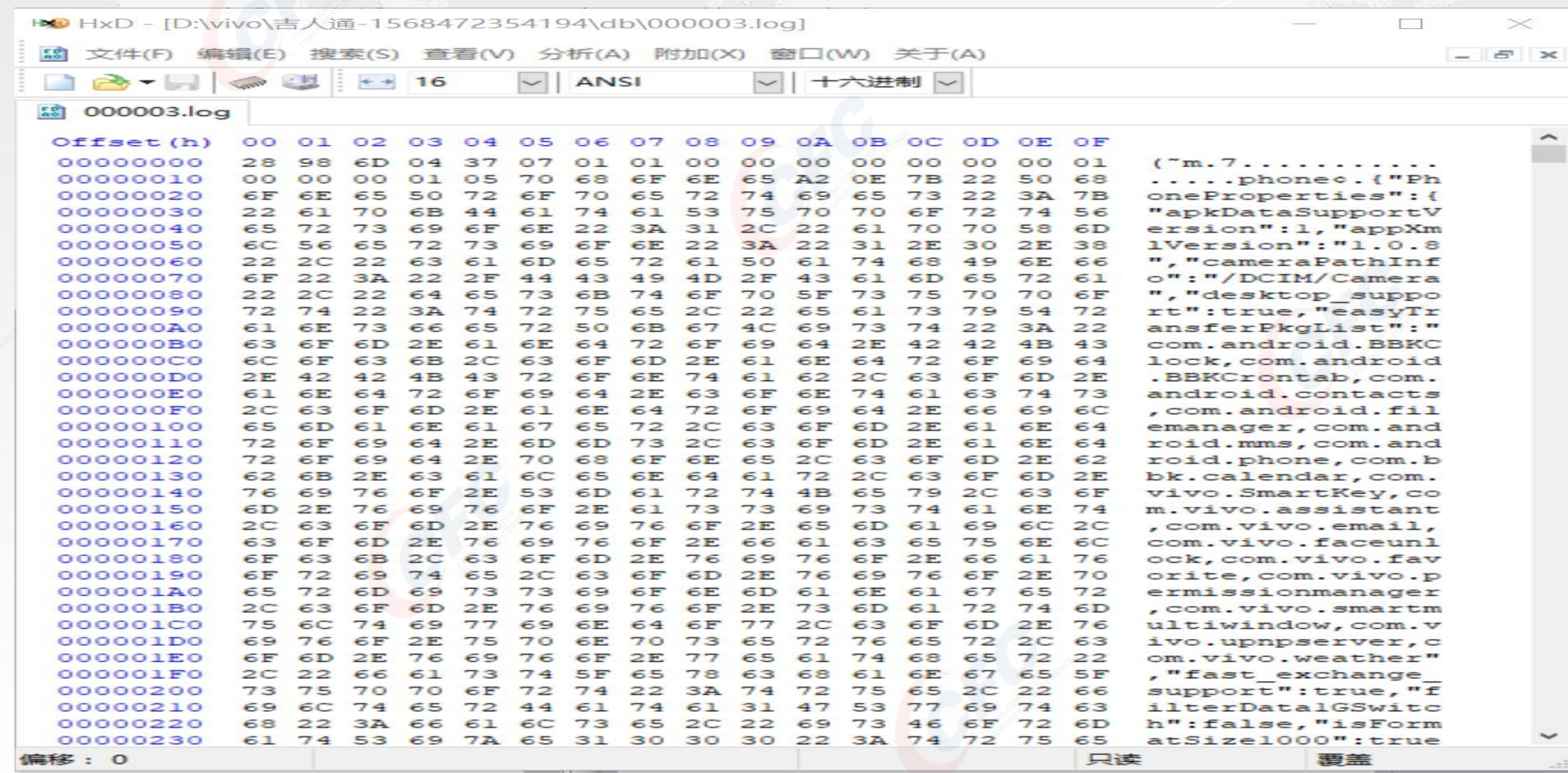
注：JSON是一个标记符的序列。这套标记符包含六个构造字符、字符串、数字和三个字面名，如：{"name": "John Doe", "age": 18, "address": {"country": "china", "zip-code": "10000"}}



VIVO手机互传备份解密

备份信息解密

我们在备份文件夹中看到的文件都是加密状态，要对文件进行解密，需要分析备份信息的数据，那么备份信息是存储在log文件中，打开备份文件夹中“DB”文件夹的“000003.log”文件，如下图所示，对备份文件中的文件进行解密。



```
HxD - [D:\Vivo\吉人通-1568472354194\db\000003.log]
文件(F) 编辑(E) 搜索(S) 查看(V) 分析(A) 附加(X) 窗口(W) 关于(A)
16 ANSI 十六进制
000003.log
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 28 98 6D 04 37 07 01 01 00 00 00 00 00 00 00 01 (~m.7.....
00000010 00 00 00 01 05 70 68 6F 6E 65 A2 0E 7B 22 50 68 .....phonec.{"Ph
00000020 6F 6E 65 50 72 6F 70 65 72 74 69 65 73 22 3A 7B oneProperties":{
00000030 22 61 70 6B 44 61 74 61 53 75 70 70 6F 72 74 56 "apkDataSupportV
00000040 65 72 73 69 6F 6E 22 3A 31 2C 22 61 70 70 58 6D ersion":1,"appXm
00000050 6C 56 65 72 73 69 6F 6E 22 3A 22 31 2E 30 2E 38 lVersion":"1.0.8
00000060 22 2C 22 63 61 6D 65 72 61 50 61 74 68 49 6E 66 ", "cameraPathInf
00000070 6F 22 3A 22 2F 44 43 49 4D 2F 43 61 6D 65 72 61 o":"/DCIM/Camera
00000080 22 2C 22 64 65 73 6B 74 6F 70 5F 73 75 70 70 6F ", "desktop_suppo
00000090 72 74 22 3A 74 72 75 65 2C 22 65 61 73 79 54 72 rt":true,"easyTr
000000A0 61 6E 73 66 65 72 50 6B 67 4C 69 73 74 22 3A 22 ansferPkgList":
000000B0 63 6F 6D 2E 61 6E 64 72 6F 69 64 2E 42 42 4B 43 com.android.BBKC
000000C0 6C 6F 63 6B 2C 63 6F 6D 2E 61 6E 64 72 6F 69 64 lock,com.android
000000D0 2E 42 42 4B 43 72 6F 6E 74 61 62 2C 63 6F 6D 2E .BBKCrontab,com.
000000E0 61 6E 64 72 6F 69 64 2E 63 6F 6E 74 61 63 74 73 android.contacts
000000F0 2C 63 6F 6D 2E 61 6E 64 72 6F 69 64 2E 66 69 6C ,com.android.fil
00000100 65 6D 61 6E 61 67 65 72 2C 63 6F 6D 2E 61 6E 64 emanager,com.and
00000110 72 6F 69 64 2E 6D 6D 73 2C 63 6F 6D 2E 61 6E 64 roid.mms,com.and
00000120 72 6F 69 64 2E 70 68 6F 6E 65 2C 63 6F 6D 2E 62 roid.phone,com.b
00000130 62 6B 2E 63 61 6C 65 6E 64 61 72 2C 63 6F 6D 2E bk.calendar,com.
00000140 76 69 76 6F 2E 53 6D 61 72 74 4B 65 79 2C 63 6F vivo.SmartKey,co
00000150 6D 2E 76 69 76 6F 2E 61 73 73 69 73 74 61 6E 74 m.vivo.assistant
00000160 2C 63 6F 6D 2E 76 69 76 6F 2E 65 6D 61 69 6C 2C ,com.vivo.email,
00000170 63 6F 6D 2E 76 69 76 6F 2E 66 61 63 65 75 6E 6C com.vivo.faceunl
00000180 6F 63 6B 2C 63 6F 6D 2E 76 69 76 6F 2E 66 61 76 ock,com.vivo.fav
00000190 6F 72 69 74 65 2C 63 6F 6D 2E 76 69 76 6F 2E 70 orite,com.vivo.p
000001A0 65 72 6D 69 73 73 69 6F 6E 6D 61 6E 61 67 65 72 ermissionmanager
000001B0 2C 63 6F 6D 2E 76 69 76 6F 2E 73 6D 61 72 74 6D ,com.vivo.smartm
000001C0 75 6C 74 69 77 69 6E 64 6F 77 2C 63 6F 6D 2E 76 ultiwindow,com.v
000001D0 69 76 6F 2E 75 70 6E 70 73 65 72 76 65 72 2C 63 ivo.upnpserver,c
000001E0 6F 6D 2E 76 69 76 6F 2E 77 65 61 74 68 65 72 22 om.vivo.weather"
000001F0 2C 22 66 61 73 74 5F 65 78 63 68 61 6E 67 65 5F ,"fast_exchange_
00000200 73 75 70 70 6F 72 74 22 3A 74 72 75 65 2C 22 66 support":true,"f
00000210 69 6C 74 65 72 44 61 74 61 31 47 53 77 69 74 63 ilterDataIGSwitc
00000220 68 22 3A 66 61 6C 73 65 2C 22 69 73 46 6F 72 6D h":false,"isForm
00000230 61 74 53 69 7A 65 31 30 30 30 22 3A 74 72 75 65 atSize1000":true
```

偏移: 0 只读 覆盖

VIVO手机互传备份解密

在对以上LOG文件格式进行分析前，先来了解3个基础知识点：

记录结点：记录着每个文件夹的字节长度，是有一定规律。

K信息：记录着每个文件夹的属性信息，如名称、路径、大小、占用空间，时间。

V信息：记录着每个文件夹属性的内容，如：com.tencent.mm, \VIVO\MM, 37MB。

VIVO手机互传备份解密

记录结点解析

通过分析，VIVO的LGO文件记录结点是20个字节为一组，记为buf。

记录结点	随机数(4)	长度(2)	标记(1)	其他(13)
1	28 98 6D 04	37 07	01	01 00 00 00 00 00 00 00 00 01 00 00 00 00 01
2	1A 84 4F CB	78 04	01	02 00 00 00 00 00 00 00 00 01 00 00 00 00 01
3	B2 58 3A 27	3C 74	02	03 00 00 00 00 00 00 00 00 00 01 00 00 00 01
4	62 90 EA 60	59 00	01	04 00 00 00 00 00 00 00 00 00 01 00 00 00 01
5	9A 71 CB 7D	27 00	01	05 00 00 00 00 00 00 00 00 00 01 00 00 00 01
6	C8 E4 4B B3	22 00	01	06 00 00 00 00 00 00 00 00 00 01 00 00 00 01
7	01 60 3A 96	A9 00	01	07 00 00 00 00 00 00 00 00 00 01 00 00 00 01
8	F8 5A 5A 4C	7B 00	01	08 00 00 00 00 00 00 00 00 00 01 00 00 00 01
9	65 2D 28 CA	A8 00	01	09 00 00 00 00 00 00 00 00 00 01 00 00 00 01
10	7D C0 71 AD	76 00	01	0A 00 00 00 00 00 00 00 00 00 01 00 00 00 01
11	B7 1F 6E 7C	B2 00	01	0B 00 00 00 00 00 00 00 00 00 01 00 00 00 01
...	...	...	...	...
31	CF 85 65 71	06 00	02	1F 00 00 00 00 00 00 A7 C4 51 26 23 01 04 00
...	...	...	...	...

分析表样本中记录，初步归纳结

(1) 随机数(random) 是由0x00~0x03这4个字节组成。

(2) 长度(nextoff) 是由0x04~0x05这2个字节记为长度或下一个块的偏移长度，计算公式如下

$$nextoff = buf[5] * 0x100 + buf[4]$$

以记录1为例： $nextoff = 0x07 * 0x100 + 0x37 = 0x737$ 。

(3) 标记(flag) 一般是由0x06~0x06这1个字节来记录。

但也由可能是多个块组成，如上个表格中记录3、31标记由2个块组成。

对于一些记录是由多个块组成的，需要进行一次数据拼接否则会出现

如记录31中“其他”字段显示错误。

VIVO手机互传备份解密

K信息

对key的名称进行分析

序号	Key_len	Key_buf	Key
1	05	70 68 6F 6E 65	phone
2	0A	63 61 74 65 67 6F 72 69 65 73	categories
3	08	61 70 70 5F 69 6E 66 6F	app_info
4	08	70 61 73 73 77 6F 72 64	Password
5	0B	63 72 65 61 74 65 5F 74 69 6D 65	create_time
6	0F	6E 6F 74 65 5F 75 73 65 5F 62 61 73 65 36 34	note_use_base64
7	04	63 61 6C 6C	call
8	04	63 61 6C 6C	call
9	03	73 6D 73	sms
10	03	73 6D 73	sms
11	08	73 65 74 74 69 6E 67 73	settings
...	...	...	...
31	36	61 6C 62 75 6D 5F 30 30 30 30 30 31 31 5F 37 35 34 30 34 33 66 39 36 39 32 63 31 35 63 36 37 65 65 33 62 30 32 35 32 63 38 62 64 61 38 37 34 39 65 31 37 39 32 36	album_0000011_754043f9692c15c67ee3b0252c8bda8749e17926
...	...	...	...

分析表样本记录，初步归纳如下

长度（key_len）由0x21~0x21这个字节表示。

key_buf对应的内容为“key”。

VIVO手机互传备份解密

V信息

对val的内容进行分析

序号	Val_len	Val_buf	Val
1	A2 0E	7B 22 50 68 6F 6E 65 50 72 6F 70 65 ...	{"PhonePrope...
2	DE 08	5B 7B 22 63 68 65 63 6B 65 64 22 3A ...	[{"checked":...
3	A5 B3 B1 01	5B 7B 22 61 70 6B 5F 73 69 7A 65 22 ...	[{"apk_size"...
4	42	22 36 65 33 37 64 31 66 37 30 62 61 ...	"6e37d1f70ba...
5	0D	31 35 36 38 34 37 32 33 35 37 35 36 ...	156847235756...
6	04	74 72 75 65	true
7	95 01	7B 22 66 69 6C 65 6E 61 6D 65 22 3A ...	{"filename":...
8	68	7B 22 63 68 65 63 6B 65 64 22 3A 74 ...	{"checked":t...
9	95 01	7B 22 66 69 6C 65 6E 61 6D 65 22 3A ...	{"filename":...
10	64	7B 22 63 68 65 63 6B 65 64 22 3A 74 ...	{"checked":t...
11	9A 01	7B 22 66 69 6C 65 6E 61 6D 65 22 3A ...	{"filename":...
...	...	...	...
31	E3 01	7B 22 66 69 6C 65 6E 61 6D 65 22 3A ...	{"filename":...
...	...	...	...

Val_len是在Key_buf之后紧接的字节，其值是一个变长整数计算公式如下

记Val_len的信息为无符号整数数组array[]，长度为n（其中最后一个元素array[n - 1] < 0x80），则计算方法如下

$$\begin{aligned} Val_len = & [(Array[0] \& 0x7F)] + \\ & [(Array[1] \& 0x7F) \ll 7] + \\ & \dots + \\ & [(Array[n-1] \& 0x7F) \ll (7 * (n-1))] \end{aligned}$$

以记录3为例，array[] =

{0xA5, 0xB3, 0xB1, 0x01}

Val_len

$$\begin{aligned} = & [(Array[0] \& 0x7F)] + [(Array[1] \& 0x7F) \ll 7] + [(Array[2] \& 0x7F) \ll 14] + [(Array[3] \& 0x7F) \ll 21] \\ = & [0xA5 \& 0x7F] \\ & + [(0xB3 \& 0x7F) \ll 7] + [(0xB1 \& 0x7F) \ll 14] + [(0x01 \& 0x7F) \ll 21] \\ = & 0x25 + 0x1980 + 0xC4000 + 0x200000 \\ = & 0x2C59A5 \end{aligned}$$

紧接Val_len之后即为Val_buf，其长度为Val_len。

VIVO手机互传备份解密

经不完全归纳总结得出文件的基本结构由如下数据结构组成

```
//记录结点
struct recNode
{
    uint32_t random; //随机数
    uint16_t nxtoff; //下一个记录结点偏移
    uint8_t flg; //1:一个结点, 2:多个结点, 3:数据内容, 4:最后一个数据内容
};

//数据结点
struct datNode
{
    uint32_t index; //序号
    uint32_t dat0; //常量, 目前观测为0
    uint8_t flg1; //常量, 目前观测为1
    uint32_t dat1; //常量, 目前观测为1

    uint8_t key_len; //key长度, 如"5"
    uint8_t* key_buf; //key名字, 如"phone"
    uint64_t val_len; //val长度, 如"0xA2 0x0E"
    uint8_t* val_buf; //val内容, 如"{xxxx}", 一般为json
};
```

得取整个文件结构大致如下:

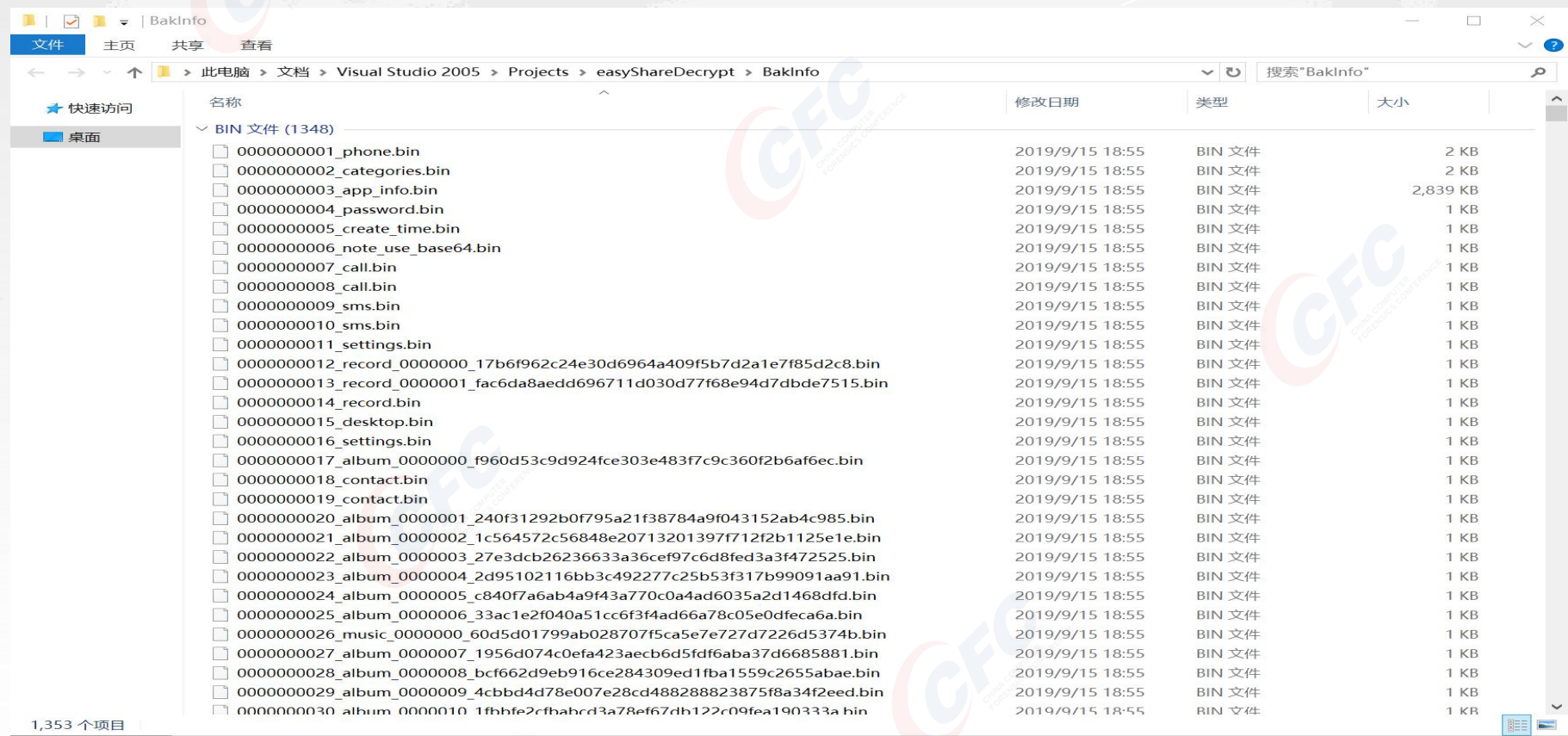
记录号	记录根结点	相同记录下一结点	...	相同记录末尾结点
R e c (1)	rec(1,0)=(r,0x0737,1, dat(1,0))			
R e c (2)	rec(2,0)=(r,0x0478,1, dat(2,0))			
R e c (3)	rec(3,0)=(r,0x743c,2, dat(3,0))	rec(3,1)=(r,0x7ff9,3, dat(3,1))	...	Rec(3,n)=(r,0x67e4,4, dat(3,n))
R e c (4)	rec(4,0)=(r,0x0059,1, dat(4,0))			
R e c (5)	rec(5,0)=(r,0x0027,1, dat(5,0))			
R e c (6)	rec(6,0)=(r,0x0022,1, dat(6,0))			
R e c (7)	rec(7,0)=(r,0x00a9,1, dat(7,0))			
R e c (8)	rec(8,0)=(r,0x007b,1, dat(8,0))			
R e c (9)	rec(9,0)=(r,0x00a8,1, dat(9,0))			
R e c (10)	rec(10,0)=(r,0x0076, 1, dat(10,0))			
R e c (11)	rec(11,0)=(r,0x00b2, 1, dat(11,0))			
...	...			
R e c (31)	rec(31,0)=(r,0x0006, 2, dat(31,0))	rec(31,1)=(r,0x0123,4, dat(31,1))		
...	...			

VIVO手机互传备份解密

即000003.log由n个记录组成，其中前后记录是紧挨着，上一个记录结束会直接通过nextoff指向下一个记录。如果某条记录的信息量比较大，此时该记录会被切分成好几条小记录，相互串连。对于记录的数据也亦是如此，简单用粗略公式表示如下

$$\begin{aligned} 000003.log &= Rec(1) + Rec(2) + \dots + Rec(n) \\ Rec(i) &= rec(i,0) + rec(i,1) + \dots + rec(i,n) \\ Dat(i) &= dat(i,0) + dat(i,1) + \dots + dat(i,n) \end{aligned}$$

套用如上数据结构切分000003.log文件每条记录成一个个小文件，保存在“Bakinfo”文件夹中，如图所示：



VIVO手机互传备份解密

应用识别

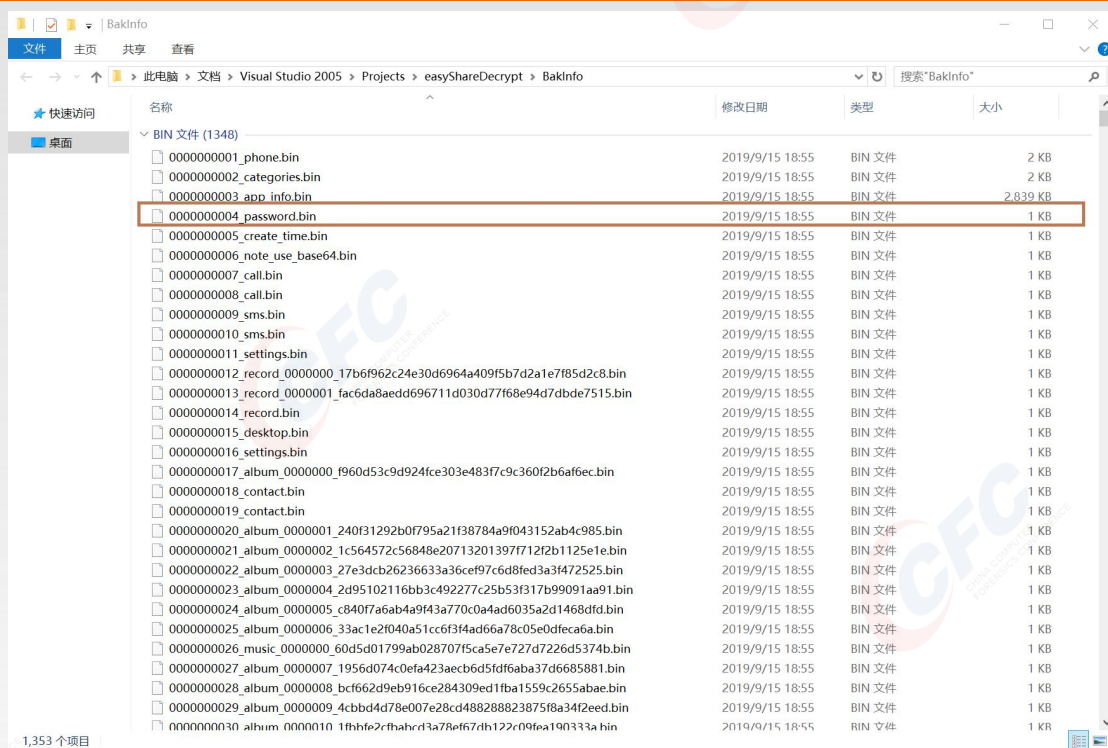
如果要知道“Bakinfo”文件夹中对应的某个应用程序的数据，可以通过该记录进行关联备份中的哈希文件名，以“微信”为例，通过搜索“weixin”即可找到相关文件，如图所示：

The image illustrates the process of identifying application data in a backup. It consists of three main windows:

- File Explorer (Left):** Shows the 'BakInfo' folder structure. The file '0000001233_weixin_data.bin' is selected.
- Hex Editor (Top Right):** Displays the contents of '0000001233_weixin_data.bin'. The hex data is shown in columns, and the corresponding JSON structure is visible on the right. The JSON includes fields like 'filename', 'hash', 'size', 'version', 'create_d', 'count', and 'mtime'.
- File Explorer (Bottom Right):** Shows the 'vivo' folder structure. A search for 'weixin' has been performed, resulting in a list of files. The file '5a656b0891e6321126f9b7da9137994c7...' is highlighted, which corresponds to the hash value found in the hex editor.

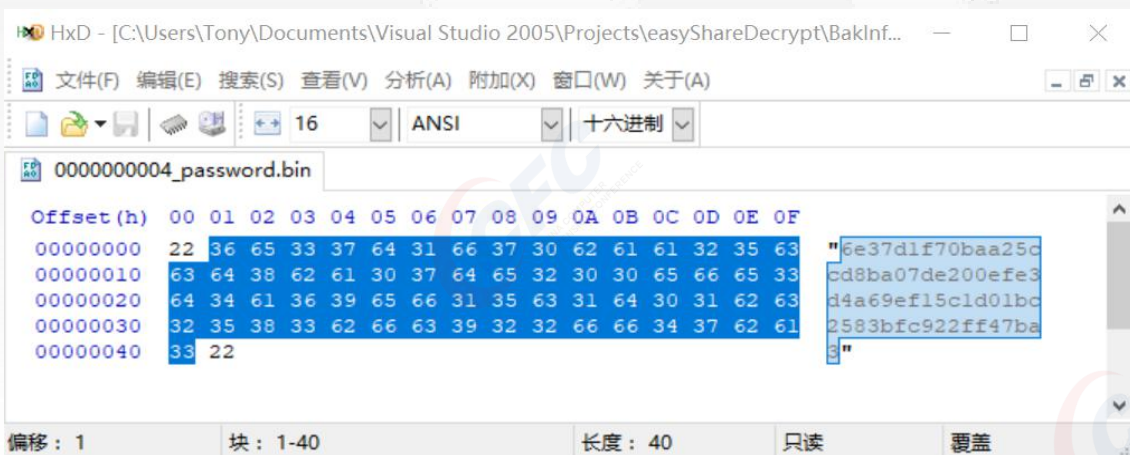
Red arrows indicate the flow of information: from the selected file in the left explorer to the hex editor, and from the search results in the bottom right explorer back to the hex editor.

VIVO手机互传备份解密



密码校验

先前在创建备份文件时，对备份文件输入了密码，要解密需要先对密码进行校验。“互传”应用会把“密码”生成一串HASH值，存放在该文件“0000000004_password.bin”中，如图所示：



VIVO手机互传备份解密

“互传”应用逆向分析，发现该互传应用是通过HmacSha256来进行加密，如下为相关生成代码：

```
7 //用途:校验vivo互传本地备份密码
8 //作者:tonyxqq@dingtalk.com
9 //时间:2019-09-15
10 int main()
11 {
12     char* key = "es4sUVhZj8JMPPrW2q9vD";
13     char* dat = "www.longxintec.com";
14     char out[256] = {0};
15     unsigned int outlen = 0;
16
17     HMAC_CTX* ctx = HMAC_CTX_new();
18     HMAC_Init_ex(ctx, key, strlen(key), EVP_sha256(), NULL);
19     HMAC_Update(ctx, (const unsigned char *)dat, strlen(dat));
20     HMAC_Final(ctx, (unsigned char *)out, &outlen);
21     HMAC_CTX_free(ctx);
22
23     char buf[1024] = {0};
24     memset(buf, 0, 1024);
25     for(int i = 0; i < outlen; ++ i)
26     {
27         sprintf(buf + i * 2, "%02x", (unsigned char)out[i]);
28     }
29     return 0;
30 }
```

监视 1

名称	值
buf	0x0019f9e8 "6e37d1f70baa25ccd8ba07de200efe3d4a69ef15c1d01bc2583bfc922ff47ba3"

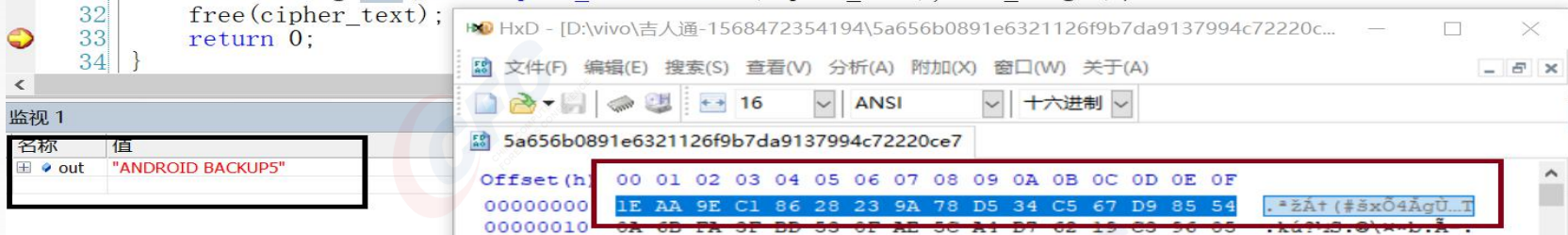
此次实验是知道密码情况进行校验，如未知密码可以结合密码字典进行爆破。

VIVO手机互传备份解密

数据解密

通过逆向分析，得到该备份文件是使用了aes256ctr的加密方式，以微信数据为例，输入密码“www.longxintec.com”，解密数据的前16个字节，内容为“ANDROID BACKUP5”，如下图所示：

```
6 //用途:解密vivo互传本地备份示例代码
7 //作者:tonyxqq@dingtalk.com
8 //时间:2019-09-15
9 int main()
10 {
11     char buf[] = {0x1E, 0xAA, 0x9E, 0xC1, 0x86, 0x28, 0x23, 0x9A, 0x78, 0xD5, 0x34, 0xC5, 0x67, 0xD9, 0x85, 0x54};
12     string data;
13     data.assign(buf, 0x10);
14     int buf_length, out_length;
15     const EVP_CIPHER * mode = EVP_aes_256_ctr();
16     unsigned char *cipher_text = (unsigned char*)malloc(data.length());
17
18     unsigned char key[32] = {0};
19     unsigned char iv[16] = {0};
20     char* pass = "www.longxintec.com";
21     EVP_BytesToKey(mode, EVP_md5(), NULL, (const unsigned char *)pass, strlen(pass), 0, key, iv);
22
23     EVP_CIPHER_CTX *ctx = EVP_CIPHER_CTX_new();
24     if (!ctx) return -1;
25     if (!EVP_DecryptInit_ex(ctx, mode, NULL, key, iv)) return -1;
26     if (!EVP_DecryptUpdate(ctx, cipher_text, &buf_length, (unsigned char*)data.c_str(), data.length())) return -1;
27     out_length = buf_length;
28     if (!EVP_DecryptFinal_ex(ctx, cipher_text + buf_length, &buf_length)) return -1;
29     out_length += buf_length;
30     EVP_CIPHER_CTX_free(ctx);
31     std::string out(reinterpret_cast<char*>(cipher_text), out_length);
32     free(cipher_text);
33     return 0;
34 }
```



VIVO手机互传备份解密

对备份文件进行解密成功后，在用取证工具对微信数据进行解析：

显示全部对话

序号	数据状态	名称(ID)	消息总数
1	已删除	政研會 友好一號群 (27@chatroom)	7\1838
2	已删除	Apple 2019 秋季特別活動 (21@chatroom)	3\67
3	已删除	iWechat(11773162159@cha...	2\19
4	存在	(759@chatroom)	2\157
5	存在	(989@chatroom)	0\92
6	存在	purecpp社區群 (9953167028@chatroom)	0\49
7	存在	稀酷客1群 (10299066154@chatroom)	0\1

显示全部消息



[求助]脱壳应用中的Asset.car资源文件如何重签名,使用iOS App Signer 应用重签名无效

2019-09-11 18:43:31



TinXie()

「hello world: [求助]脱壳应用中的Asset.car资源文件如何重签名,使用iOS App Signer 应用重签名无效」-----重签，需要有開發者憑證，需要付費的才行

2019-09-12 09:29:42



hello world()

使用 iOS app signer重签了,证书是企业证书没问题

2019-09-12 09:32:54



hello world()

闪退的原因是Assert加载异常,app包里面有Assert.car的资源文件

2019-09-12 09:33:51



hello world()

所以问一下,开发的时候放在Assert里面的图片资源,逆向开发的时候是否需要特殊处理

2019-09-12 09:34:33



TinXie()

說說你的改法？

2019-09-12 09:56:06



hello world(v)

已删除

WhatsApp

2019-09-12 09:57:15



hello world()

已删除

重签名使用的是工具iOS App Signer

2019-09-12 09:57:42



Natsuki(r)

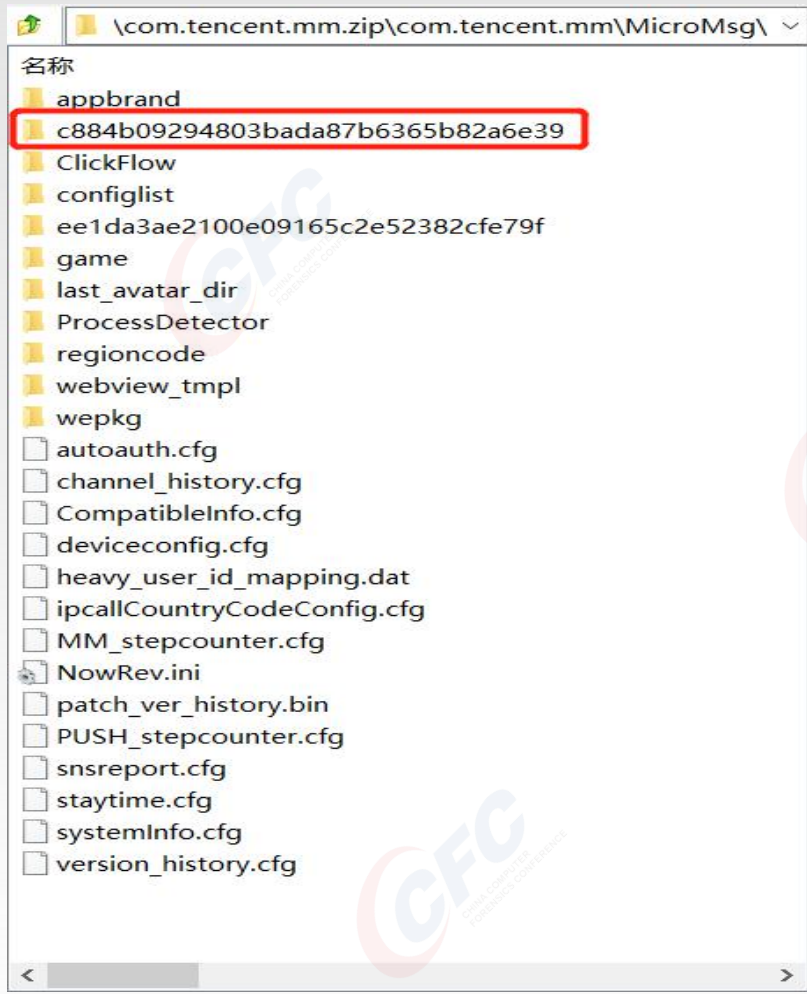
7)

手机取证案例

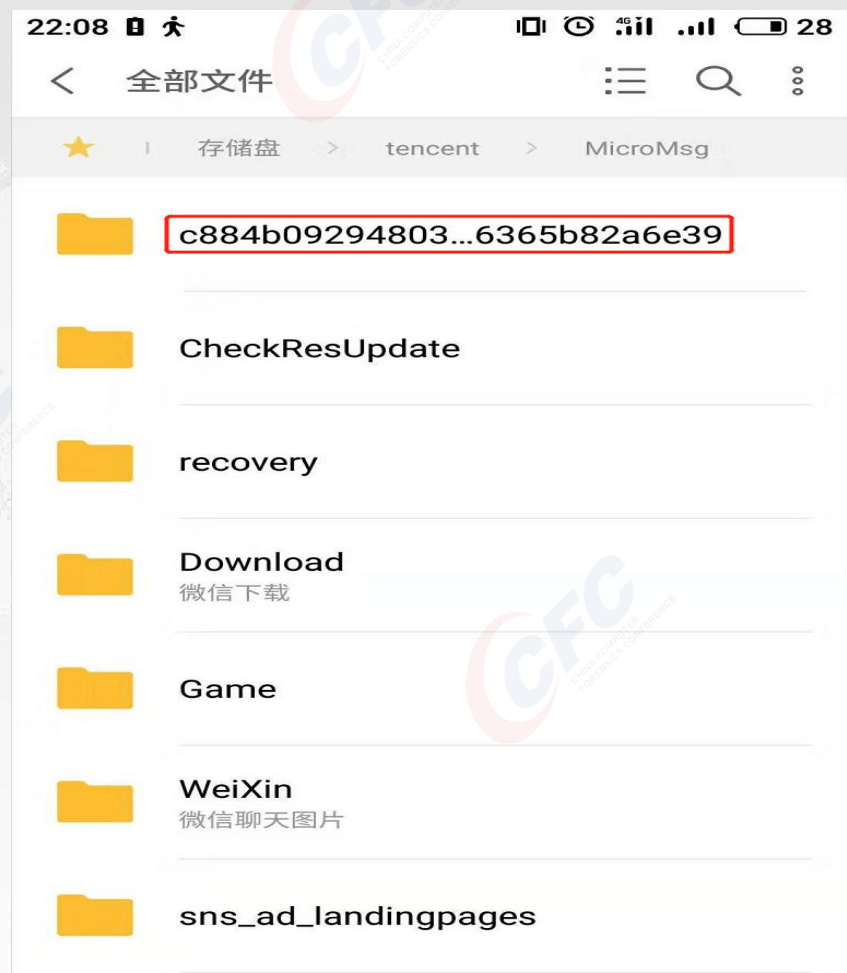
- 支持宝数据提取及恢复
- 手机地图APP取证
- VIVO手机互传备份解密
- 微信7.0.6版本附件取证

微信7.0.6版本附件取证

以往安卓微信聊天数据库与附件的目录名都是一样(7.0.5)



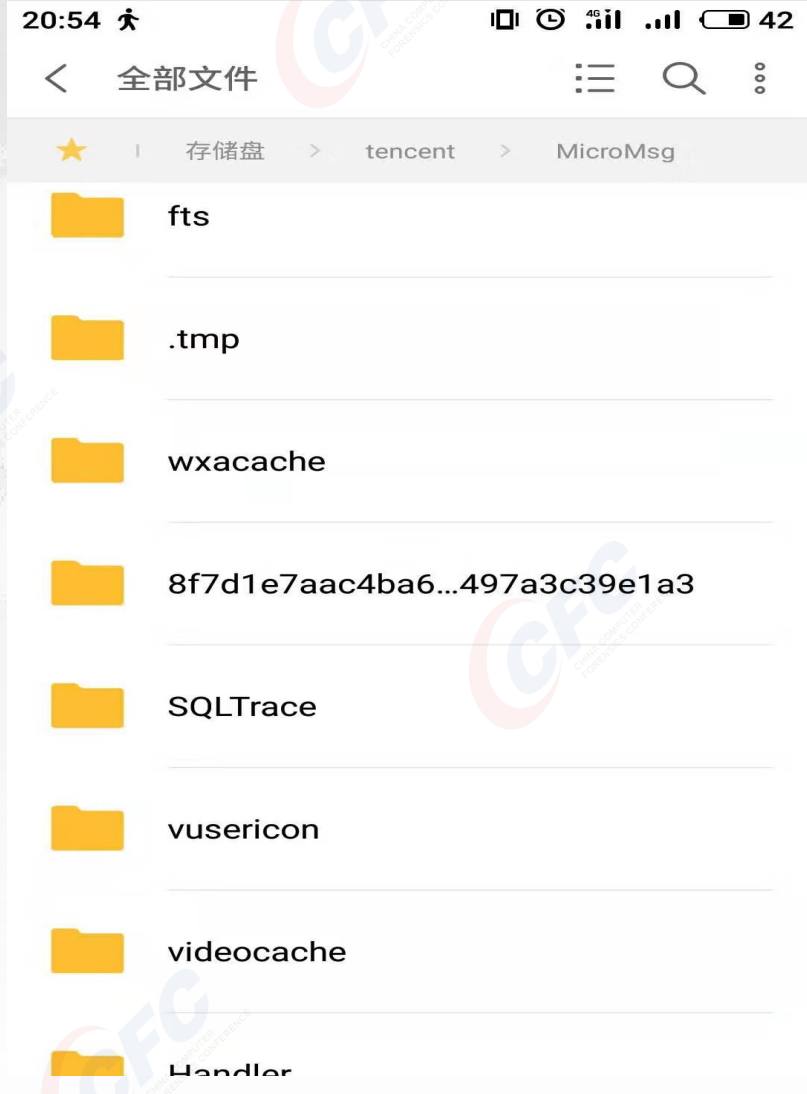
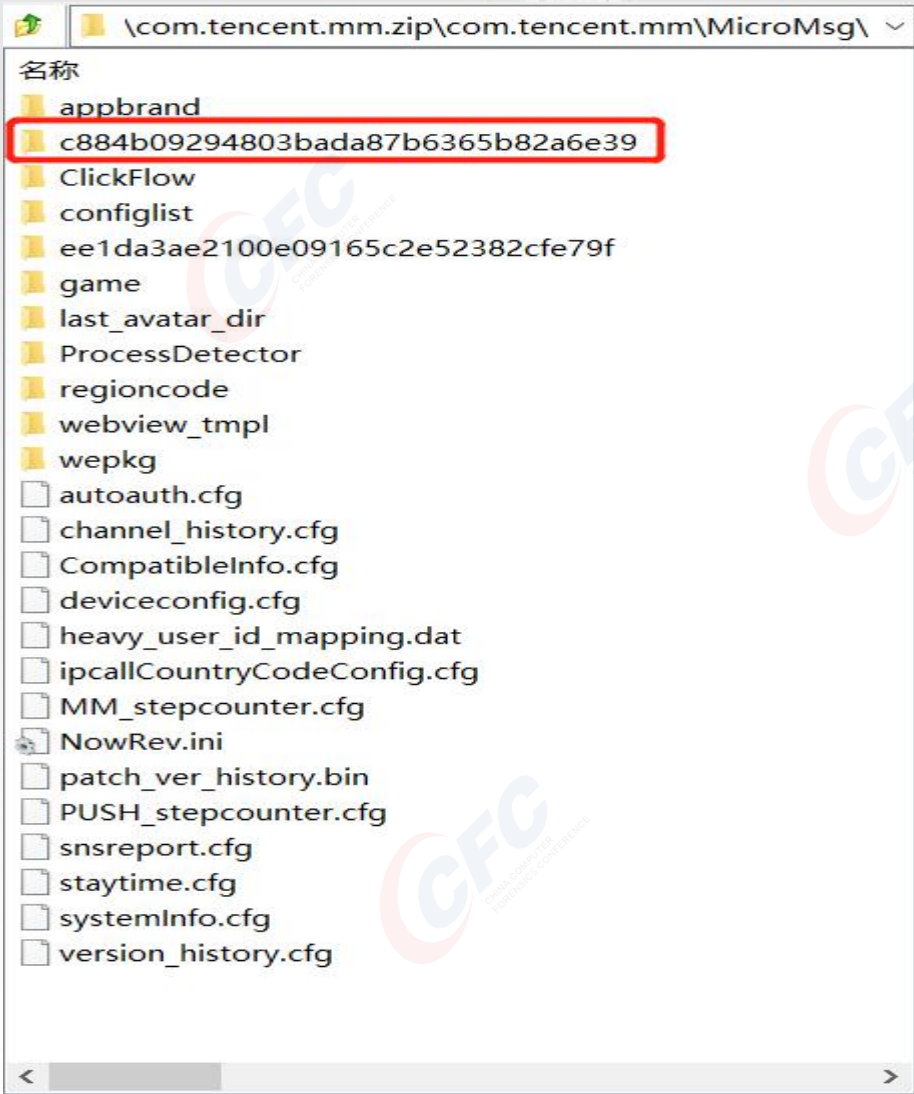
数据库目录
(c884b09294803bada87b6365b82a6e39)



附件目录
(c884b09294803bada87b6365b82a6e39)

微信7.0.6版本附件取证

但从7.0.6起出现附件目录命名规则就开始变更导致



微信7.0.6版本附件取证

逆向安卓微信

```
long currentTimeMillis = System.currentTimeMillis();
int a2 = b.a(fbu);
ab.i("MMKernel.CoreAccount", "dkacc setAccuin %s hash:%d thread:%d[%s] stack:%s", p.getString(a2), Integer.valueOf(i.cb(a2, 100)), L
if (a2 != 0) {
    z2 = true;
} else {
    z2 = false;
}
if (!z2) {
    ab.w("MMKernel.CoreAccount", "setAccUin, Reset by MMCore.resetAccUin");
} else {
    p.getString(a2);
    com.tencent.mm.sdk.a.b.dzB();
    g.Wc();
    e Wb = g.Wb();
    AnonymousClass1 r0 = new Runnable() {
        public final void run() {
            AppMethodBeat.i(57880);
            a.this.fbI = C0055a.AccountHasReady;
            AppMethodBeat.o(57880);
        }
    };
    ah.getContext().getSharedPreferences(ah.dAo(), 0).edit().putBoolean("isLogin", true).apply();
    String C = g.C("mm".concat(String.valueOf(a2)).getBytes());
    String l = e.l(a2, C);
    ab.i("MMKernel.CoreStorage", "uinPath: %s, uinSaltPath: %s", C, l);
    boolean Qt = com.tencent.mm.compatible.util.f.Qt();
    if (l == null) {
        ab.w("MMKernel.CoreStorage", "Cannot generate account path, skip account renaming!");
        i = 6;
        z3 = false;
    } else if (!Wb.fct.startsWith(com.tencent.mm.compatible.util.e.fla) || !Qt) {
        ab.w("MMKernel.CoreStorage", "SDCard not available, skip account renaming!");
        i = 1;
        z3 = false;
    } else {
        File file = new File(Wb.fct + C);
        File file2 = new File(Wb.fct + l);
        if (!file.isDirectory()) {
            if (!file2.isDirectory()) {
                file2.delete();
            }
            file2.mkdirs();
            i = 5;
            z3 = true;
        } else if (file2.isDirectory()) {
            ab.i("MMKernel.CoreStorage", "Both uinPath exists, migration shall be taken.");
            i = 2;
            z3 = true;
        } else {
            file2.delete();
            ab.i("MMKernel.CoreStorage", "Move account directory: %s => %s", file, file2);
            if (!file.renameTo(file2)) {
                ab.w("MMKernel.CoreStorage", "Failed to move uinPath, use old accPath");
            }
        }
    }
}
```

C:用户目录, md5(mm+uin)

a2: 微信uin

微信7.0.6版本附件取证

```
static String l(int i, String str) {
    byte[] aTA;
    boolean z;
    AppMethodBeat.o(162739);
    com.tencent.mm.vfs.b bVar = new com.tencent.mm.vfs.b(com.tencent.mm.compatible.util.e.fkX, "account.bin");
    com.tencent.mm.vfs.b bVar2 = new com.tencent.mm.vfs.b(com.tencent.mm.compatible.util.e.fkX + "MicroMsg/" + str + "/account.bin");
    byte[] t = t(bVar);
    byte[] t2 = t(bVar2);
    if (t2 != null) {
        z = false;
        aTA = t2;
    } else if (t != null) {
        z = false;
        aTA = t;
    } else {
        aTA = aTA();
        if (aTA == null) {
            AppMethodBeat.o(162739);
            return null;
        }
        z = true;
    }
    boolean z2 = false;
    if (t2 == null || bVar2.length() != 4112) {
        z2 = a(bVar2, aTA) | false;
    }
    if (t == null || bVar.length() != 4112) {
        z2 |= a(bVar, aTA);
    }
    if (!z || z2) {
        try {
            MessageDigest instance = MessageDigest.getInstance("MD5");
            instance.update(aTA);
            instance.update(Integer.toString(i).getBytes());
            byte[] digest = instance.digest();
            StringBuilder sb = new StringBuilder(digest.length * 2);
            char[] cArr = {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f'};
            for (int i2 = 0; i2 < 16; i2++) {
                byte b2 = digest[i2];
                sb.append(cArr[(b2 >> 4) & 15]).append(cArr[b2 & 15]);
            }
            String sb2 = sb.toString();
            AppMethodBeat.o(162739);
            return sb2;
        } catch (NoSuchAlgorithmException e2) {
            RuntimeException runtimeException = new RuntimeException(e2);
            AppMethodBeat.o(162739);
            throw runtimeException;
        }
    } else {
        ab.e("MMKernel.CoreStorage", "Cannot write new generated data to account files.");
        AppMethodBeat.o(162739);
        return null;
    }
}
```

aTA:MicroMsg/用户目录/account.bin文件内容

i: 微信uin

经分析知附件目录的命名规则如下

FolderName = md5(account.bin + uin)

谢谢

案件技术支持电话：

18652914943（微信号）

公众号：

suzhoulongxintec



王海啸

江苏 南京



扫一扫上面的二维码图案，加我微信