



# Криминалистический анализ данных Android приложений

Карондеев Андрей



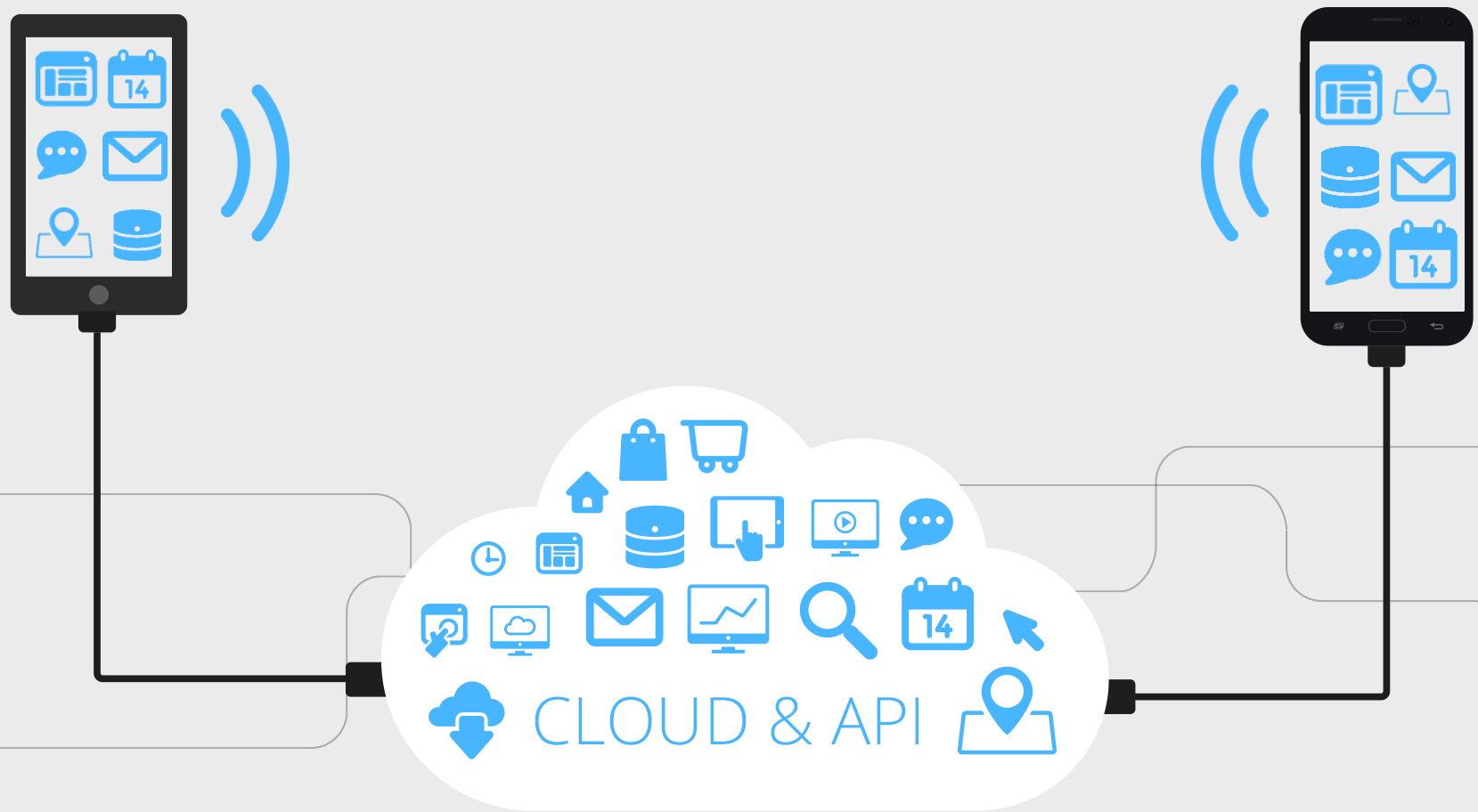
# Данные мобильных приложений



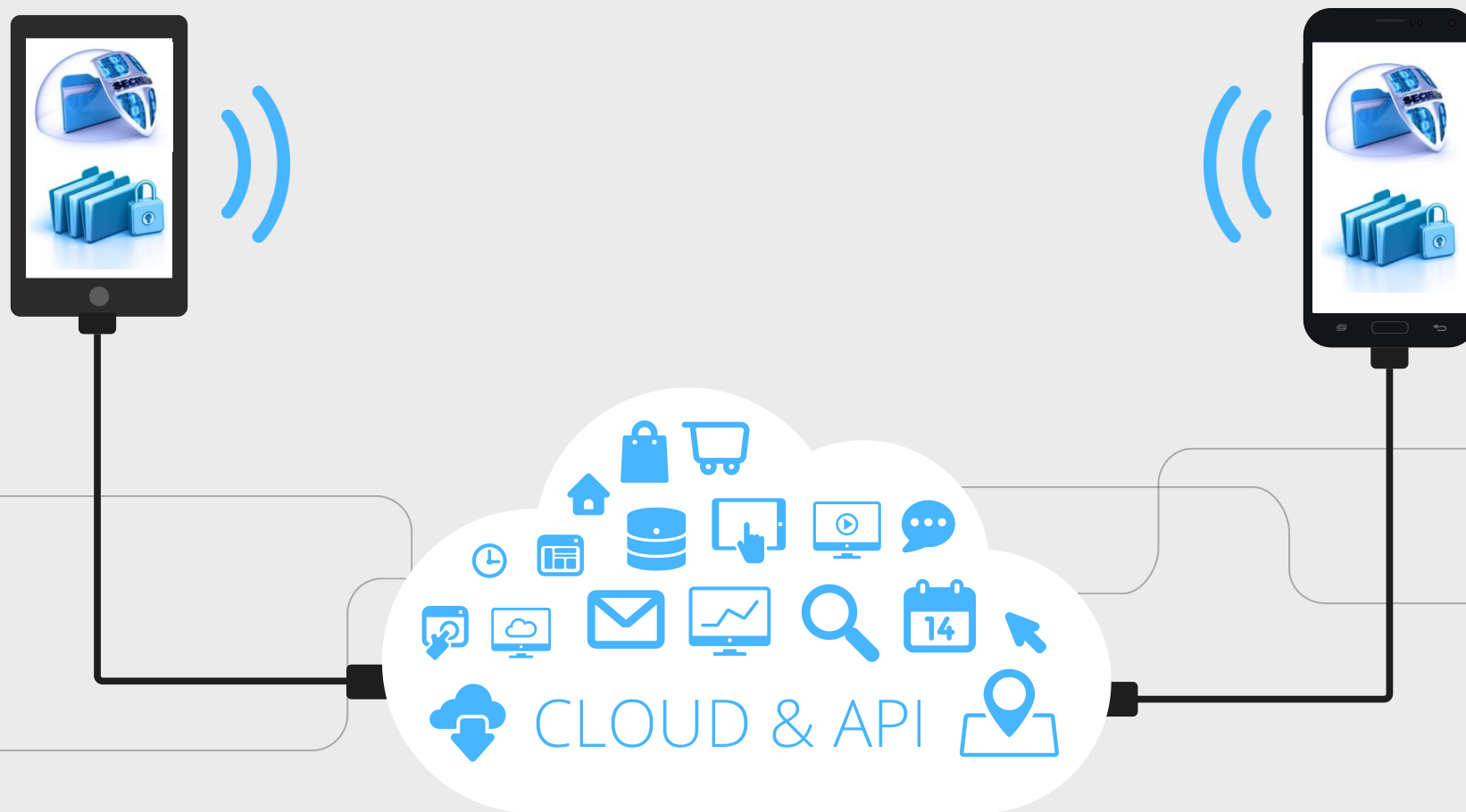
# Данные мобильных приложений



# Данные мобильных приложений



# Данные мобильных приложений



# Разнообразие мобильных платформ и приложений



# Разнообразие мобильных платформ и приложений

## Worldwide Smartphone Sales to End Users by Operating System in 4Q15 (Thousands of Units)

Operating System	4Q15 Units	4Q15 Market Share (%)	4Q14 Units	4Q14 Market Share (%)
Android	325,394.4	80.7	279,057.5	76.0
iOS	71,525.9	17.7	74,831.7	20.4
Windows	4,395.0	1.1	10,424.5	2.8
Blackberry	906.9	0.2	1,733.9	0.5
Others	887.3	0.2	1,286.9	0.4
<b>Total</b>	<b>403,109.4</b>	<b>100.0</b>	<b>367,334.4</b>	<b>100.0</b>

Source: Gartner (February 2016)

# Разнообразие мобильных платформ и приложений





# Основные этапы криминалистического анализа мобильного приложения

- Изучение окружения приложения
- Изучение внутреннего устройства приложения
- Расшифровывание данных
- Преобразование данных к понятному следователю виду

# Android месенджер Threema



# Эксперт приступает к анализу



**Threema.**

Seriously secure mobile messaging.

# Android мессенджер Threema



← → ↻ <https://play.google.com/store/apps/details?id=ch.threema.app&hl=en>

**Google Play** Search


**Apps** Categories Home Top Charts New Releases

My apps  
**Shop**  
Games  
Family  
Editors' Choice

My account  
My Play activity  
My wishlist  
Redeem  
Parent Guide

## Threema

Threema GmbH Communication **Top Developer**  
★★★★★ 41,159

 Add to Wishlist **RUB178.14 Buy**

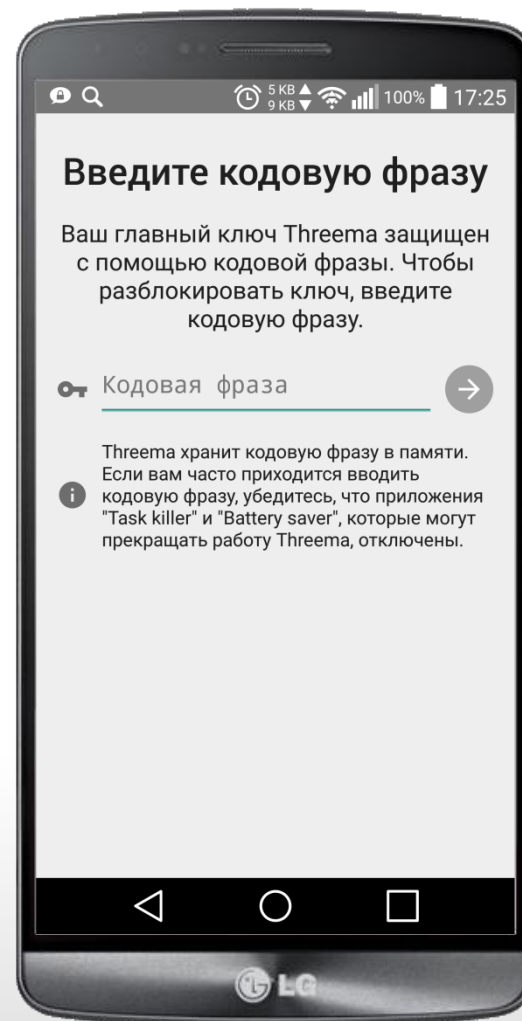
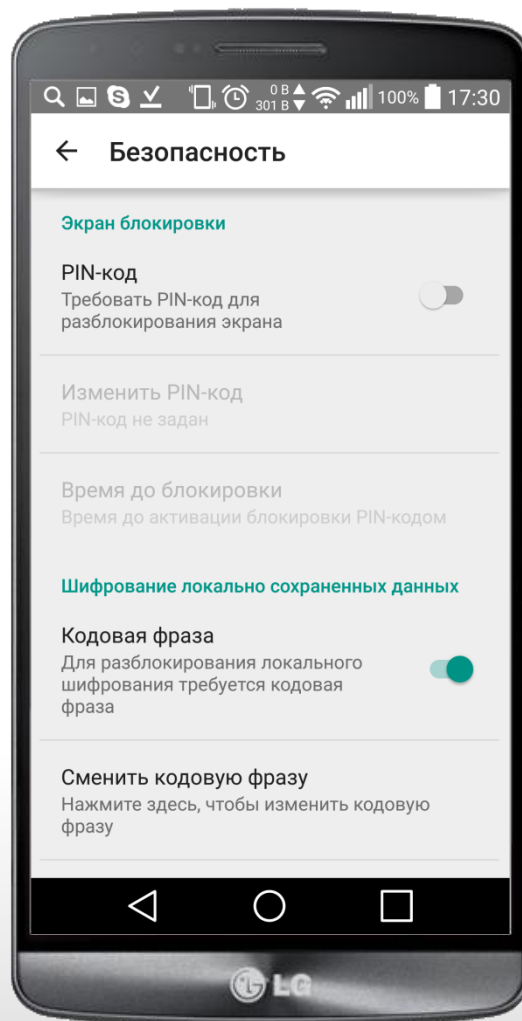
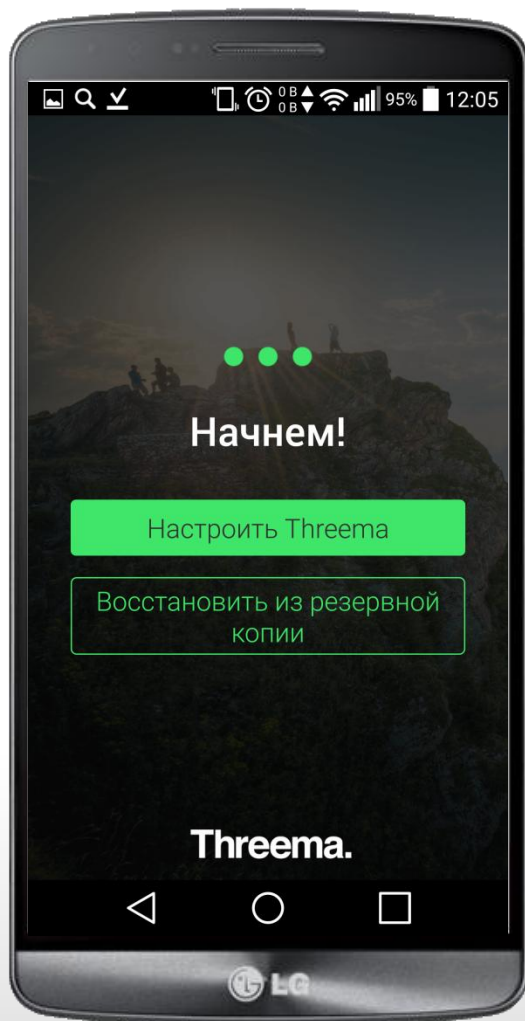
Threema encrypts all your conversations

Threema is feature-rich and easy to use

Send photos, videos, voice messages and more

Threema is the world's favorite secure messenger and keeps your data out of the hands of hackers, corporations and governments. Threema can be used completely anonymously, and offers a rich set of features.

# Android мессенджер Threema



# Данные Android приложения Threema

Total Commander

Файлы Выделение Навигация Сеть FTP Вид Вкладки Конфигурация Инструменты Запуск Справка

с d \ \ .. [\_нет\_] c d \ \ .. [lenovo] 5,5 Гб из 24,9 Гб свободно

▼ \\ADB\LG855c20f60bf\data\data\ch.threema.app\\*.\*

Имя	Тип	Owner	Group	Size	Date
..					
cache		u0_a137	u0_a137	<Папка>	10.03.2016
databases		u0_a137	u0_a137	<Папка>	13.03.2016
files		u0_a137	u0_a137	<Папка>	10.03.2016
no_backup		u0_a137	u0_a137	<Папка>	10.03.2016
shared_prefs		u0_a137	u0_a137	<Папка>	13.03.2016
lib		install	install	0	13.03.2016

0 байт из 0 байт, файлов: 0 из 1, папок: 0 из 5

▼ d:\ch.threema.app\databases\\*.\*

Имя	Тип	Размер	Дата
..		<Папка>	12.03.2016 18:38
threema	db	54 272	10.03.2016 13:28

0 байт из 53,0 Кб, файлов: 0 из 1

\\ADB\LG855c20f60bf\data\data\ch.threema.app>

F3 Просмотр F4 Правка F5 Копирование F6 Перемещение F7 Каталог F8 Удаление Alt+F4 Выход

# Данные Android приложения Threema

D:\ch.threema.app\databases\threema.db - Notepad++

Файл Правка Поиск Вид Кодировки Синтаксисы Опции Макросы Запуск Плагины Окна ?

threema.db

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	1b	1d	6b	7d	2a	f7	e6	ba	aa	fa	0c	a6	c5	fd	16	b5	..k}*чжеЄъ.¡Еэ.μ
00000010	b4	e6	63	08	0f	c4	c6	92	6a	a0	d1	29	21	3d	87	20	гжс..ДЖ'ј.С)!=#
00000020	35	22	b7	89	7e	46	31	c5	b4	16	1a	01	9c	ea	30	af	5"·%~F1ЕГ...њк0İ
00000030	65	85	81	06	f9	28	f3	24	fb	ca	2c	88	fa	8e	59	28	е... .щ(у\$ык,ЄЪЪУ(
00000040	13	4d	cf	5e	1d	78	8e	c9	6a	a2	a0	51	69	fe	fc	24	.МП^ .хЪЙjÿ.Qiюь\$
00000050	56	0d	6d	c7	87	66	1c	b8	9d	fd	95	b1	86	2c	39	c8	V.m3†f.ё.э•±†,9И
00000060	b6	6f	e9	b3	36	41	9d	e7	97	5c	25	63	51	dc	91	07	¶ойi6A.э-\%сQЪ\.
00000070	7f	c8	31	53	c2	d4	f9	98	f5	39	27	f0	35	a1	11	14	.И1SBФщ.x9'p5ÿ..
00000080	ab	f9	5e	a8	12	d2	e0	f3	c6	ea	3b	e7	53	c8	a1	0d	«щ^ё.ТауЖк;эСИÿ.
00000090	0e	08	27	3b	4b	65	ff	c8	56	08	e0	6c	a0	8f	bb	ef	..'';КеяИV.al...»п
000000a0	94	7b	90	e5	7d	c6	da	ad	2f	83	79	18	c4	8a	66	62	"{.е}ЖЪ-/гү.ДЪfb
000000b0	0c	4a	bc	c2	a4	9d	02	78	3f	d9	cf	1b	52	dc	02	1f	.JjBα...x?ЩП.РЬ..
000000c0	41	10	6f	37	b8	94	1a	10	58	c0	e7	5c	1d	38	a9	18	A.о7ё"...ХАэ\.8©.
000000d0	6c	a4	ae	fc	a9	e1	c8	49	33	98	af	f0	53	5f	08	cb	lα@Ъ@БИИ3.İpS_.Л
000000e0	7b	8a	b6	f9	31	b7	e1	41	d8	12	31	a1	6b	94	09	9f	{Ъ¶щ1·бАШ.1ÿк"...ц
000000f0	a2	d1	8d	70	59	03	91	81	94	eb	0b	05	f0	0f	1f	8c	ÿС.pY.\."л..р..Ъ

# Данные Android приложения Viber



Total Commander

Файлы Выделение Навигация Сеть FTP Вид Вкладки Конфигурация Инструменты Запуск Справка

с d \\.\ \ .. [\_нет\_] с d \\.\ \ .. [lenovo] 5,4 Гб из 24,9 Гб свободно

\\.\ADB\4d004400309430a3\data\data\com.viber.voip\\*.\*

Имя	Тип	Owner	Group	Size	Date
..					
shared_prefs		u0_a205	u0_a205	<Папка>	10.02.2016
files		u0_a205	u0_a205	<Папка>	05.03.2014
databases		u0_a205	u0_a205	<Папка>	17.02.2015
cache		u0_a205	u0_a205	<Папка>	04.02.2016
app_working		u0_a205	u0_a205	<Папка>	05.03.2014
app_sslcache		u0_a205	u0_a205	<Папка>	05.03.2014
app_optimized		u0_a205	u0_a205	<Папка>	05.03.2014
lib		install	install	0	20.08.2014
_ptt_id_counter		u0_a205	u0_a205	4	18.11.2014

0 байт из 4 байт, файлов: 0 из 2, папок: 0 из 7

d:\com.viber.voip\databases\\*.\*

Имя	Тип	Размер	Дата
..		<Папка>	15.03.2016 16:12
google_analytics_v2	db	20 480	20.11.2015 01:49
google_analytics_v2	db-journal	8 720	26.12.2014 11:30
viber_data		1 273 856	16.03.2016 01:01
viber_data-journal		524 288	16.03.2016 01:01
viber_messages		106 496	01.12.2015 01:14
viber_messages-journal		49 760	07.04.2015 11:45
webview	db	4 096	05.03.2014 14:24
webview	db-shm	32 768	17.02.2015 11:01
webview	db-wal	53 592	05.03.2014 14:24
webviewCookiesChro..	db	28 672	17.02.2015 11:01
webviewCookiesChro..	db	0	05.03.2014 14:29
zoobedata	db	131 072	18.11.2014 13:05
zoobedata	db-journal	33 344	18.11.2014 13:04

0 байт из 2,1 Мб, файлов: 0 из 13

d:\com.viber.voip\databases>

F3 Просмотр F4 Правка F5 Копирование F6 Перемещение F7 Каталог F8 Удаление Alt+F4 Выход



# Данные Android приложения Viber



```
D:\com.viber.voip\databases\viber_data - Notepad++
Файл Правка Поиск Вид Кодировки Синтаксисы Опции Макросы Запуск Плагины Окна ?
viber_data
Address  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f  Dump
00000000 53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 SQLite format 3.
00000010 10 00 01 01 00 40 20 20 00 00 9e cd 00 00 01 37 .....@ ..hH...7
00000020 00 00 00 00 00 00 00 00 00 00 00 13 00 00 00 04 .....
00000030 00 00 00 00 00 00 00 0f 00 00 00 01 00 00 00 34 .....4
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 9e cd .....hH
00000060 00 2d e2 23 0d 09 80 00 0d 05 7b 00 0f a7 0e 08 .-в#..Ъ...{..$.
00000070 0d b6 0b 39 0d 6b 05 7b 0c 40 09 db 08 a3 08 16 .Д.9.k.{.@.Ы.Ж..
00000080 07 cf 0c 8f 09 9a 00 00 00 00 00 00 00 00 00 00 .П...Ь.....
00000090 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 .....
000000b0 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 .....
000000d0 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 .....
000000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

# Данные Android приложения Viber



viber\_data.db - Oxygen Forensic® SQLite Viewer

Файл Инструменты Поддержка Справка

Открыть Восстановить удаленные записи Поиск Экспорт Печать Названия столбцов Настройки Справка

Настройки фильтра ...

- Таблицы
- android\_metadata (1/0)
- blockednumbers (0/0)
- calls (13/0)
- phonebookcontact (992/0)
- phonebookdata (15131/0)
- phonebookrawcontact (2/0)
- sqlite\_sequence (3/0)
- vibernumbers (8/0)
- Все удаленные данные

#	_id	call_id	aggregate_hash	number	canonized_number	viber_call	viber_call_type	date	duration	type
1	1	-1	-1604080841	+79104405218	+79104405218	1	1	1383921224324	310	1
2	2	-1	-2097591488	+79169699042	+79169699042	0	2	1394014801315	0	2
3	3	-1	-249327244	+79036589825	+79036589825	0	2	1394014838098	0	2
4	4	-1	39500142	+447944244522	+447944244522	1	1	1397198565902	0	3
5	5	-1	-635048417	+79263487243	+79263487243	1	2	1399899208559	0	2
6	6	-1	-635048417	+79263487243	+79263487243	1	1	1399899356940	26	1
7	7	-1	-635048417	+79263487243	+79263487243	1	1	1399899413963	0	2
8	8	-1	-635048417	+79263487243	+79263487243	1	1	1399899427868	25	2
9	9	-1	1797281858	+79175938713	+79175938713	1	1	1415698604210	0	2
10	10	-1	1797281858	+79175938713	+79175938713	1	1	1415698798406	44	1
11	11	-1	1797281857	+79175938713	+79175938713	1	1	1416304524045	0	3
12	12	-1	1797281858	+79175938713	+79175938713	1	1	1416305498877	4	2
13	13	-1	-1604080842	+79104405218	+79104405218	1	1	1428396351572	0	3

```
1399899356940
```

Тип	Значение
UTF-8	139989935...
Unicode (UTF-16...	球喉悒...
Unicode (UTF-16...	球喉悒...
OLE Automation ...	25.09.1465...
Unix Epoch Time	17.01.4633...
Unix Epoch Time...	12.05.2014...
OS X Epoch Time	17.01.4636...
BlackBerry Time	<Ошибка п...
Chrome Time	17.01.1601...
Symbian Epoch ...	<Ошибка п...
MS File Time	02.01.1601...
Unsigned-8	<Ошибка п...
Signed-8	<Ошибка п...
Unsigned-16	<Ошибка п...
Signed-16	<Ошибка п...
Unsigned-32	<Ошибка п...
Signed-32	<Ошибка п...
Signed-64	139989935...
Single	<Ошибка п...
Double	139989935...
Uuencoded	E6Ya?SUft
Base64	Ч0уЯwзIх

Заканчивается через 181 дней Тип файла: sqlite Размер файла: 1,2 Мб Таблицы: 8 Элементы таблицы: 13 SHA-2 Hash: 932c48d19ca5d37d4b924273a522a252433cda726353a17affbc2ae9...





# Данные Android приложения Viber



viber\_data.db - Oxygen Forensic® SQLite Viewer

Файл Инструменты Поддержка Справка

Открыть Восстановить удаленные записи Поиск Экспорт Печать Названия столбцов Настройки Справка

Настройки фильтра ...

- Таблицы
- android\_metadata (1/0)
- blockednumbers (0/0)
- calls (13/0)
- phonebookcontact (992/0)
- phonebookdata (15131/0)
- phonebookrawcontact (2/0)
- sqlite\_sequence (3/0)
- vibernumbers (8/0)
- Все удаленные данные

#	_id	call_id	aggregate_hash	number	canonized_number	viber_call	viber_call_type	date (Время UTC)	duration	type
1	1	-1	-1604080841	+79104405218	+79104405218	1	1	08.11.2013 14:33:44	310	1
2	2	-1	-2097591488	+79169699042	+79169699042	0	2	05.03.2014 10:20:01	0	2
3	3	-1	-249327244	+79036589825	+79036589825	0	2	05.03.2014 10:20:38	0	2
4	4	-1	39500142	+447944244522	+447944244522	1	1	11.04.2014 6:42:45	0	3
5	5	-1	-635048417	+79263487243	+79263487243	1	2	12.05.2014 12:53:28	0	2
6	6	-1	-635048417	+79263487243	+79263487243	1	1	12.05.2014 12:55:56	26	1
7	7	-1	-635048417	+79263487243	+79263487243	1	1	12.05.2014 12:56:53	0	2
8	8	-1	-635048417	+79263487243	+79263487243	1	1	12.05.2014 12:57:07	25	2
9	9	-1	1797281858	+79175938713	+79175938713	1	1	11.11.2014 9:36:44	0	2
10	10	-1	1797281858	+79175938713	+79175938713	1	1	11.11.2014 9:39:58	44	1
11	11	-1	1797281857	+79175938713	+79175938713	1	1	18.11.2014 9:55:24	0	3
12	12	-1	1797281858	+79175938713	+79175938713	1	1	18.11.2014 10:11:38	4	2
13	13	-1	-1604080842	+79104405218	+79104405218	1	1	07.04.2015 8:45:51	0	3

Тип	Значение
UTF-8	139989935...
Unicode (UTF-16...	球响悟...
Unicode (UTF-16...	球响悟...
OLE Automation ...	25.09.1465...
Unix Epoch Time	17.01.4633...
Unix Epoch Time...	12.05.2014...
OS X Epoch Time	17.01.4636...
BlackBerry Time	<Ошибка п...
Chrome Time	17.01.1601...
Symbian Epoch ...	<Ошибка п...
MS File Time	02.01.1601...
Unsigned-8	<Ошибка п...
Signed-8	<Ошибка п...
Unsigned-16	<Ошибка п...
Signed-16	<Ошибка п...
Unsigned-32	<Ошибка п...
Signed-32	<Ошибка п...
Signed-64	139989935...
Single	<Ошибка п...
Double	139989935...
Uuencoded	E6Ya?SUfT
Base64	Ч0уЯwзIх

1399899356940

Заканчивается через 181 дней Тип файла: sqlite Размер файла: 1,2 Мб Таблицы: 8 Элементы таблицы: 13 SHA-2 Hash: 932c48d19ca5d37d4b924273a522a252433cda726353a17affbc2ae9...



# Данные Android приложения Threema

Total Commander

Файлы Выделение Навигация Сеть FTP Вид Вкладки Конфигурация Инструменты Запуск Справка

с d \ \ .. [\_нет\_]

с d \ \ .. [lenovo] 5,5 Гб из 24,9 Гб свободно

▼ \\ADB\LG855c20f60bf\data\data\ch.threema.app\\*.\*

Имя	Тип	Owner	Group	Size	Date
..					
cache		u0_a137	u0_a137	<Папка>	10.03.2016
databases		u0_a137	u0_a137	<Папка>	13.03.2016
files		u0_a137	u0_a137	<Папка>	10.03.2016
no_backup		u0_a137	u0_a137	<Папка>	10.03.2016
shared_prefs		u0_a137	u0_a137	<Папка>	13.03.2016
lib		install	install	0	13.03.2016

0 байт из 0 байт, файлов: 0 из 1, папок: 0 из 5

▼ d:\ch.threema.app\databases\\*.\*

Имя	Тип	Размер	Дата
..		<Папка>	12.03.2016 18:38
threema	db	54 272	10.03.2016 13:28

0 байт из 53,0 Кб, файлов: 0 из 1

\\ADB\LG855c20f60bf\data\data\ch.threema.app>

F3 Просмотр F4 Правка F5 Копирование F6 Перемещение F7 Каталог F8 Удаление Alt+F4 Выход

# Изучение внутреннего устройства Android приложения

- Статический анализ:
  - dex2jar + Java Decompiler
  - IDA Pro
- Динамический анализ:
  - IDA Pro Dalvik debugger
  - IDA Pro Remote ARM Linux/Android debugger
  - Xposed Modules

# Изучение внутреннего устройства Android приложения

- Статический анализ:



- dex2jar + Java Decompiler

- IDA Pro

- Динамический анализ:

- IDA Pro Dalvik debugger

- IDA Pro Remote ARM Linux/Android debugger



- Xposed Modules

# Изучение внутреннего устройства Android приложения Threema



```
Командная строка
D:\dex2jar-2.0>d2j-dex2jar.bat ch.threema.app.apk
dex2jar ch.threema.app.apk -> .\ch.threema.app-dex2jar.jar
D:\dex2jar-2.0>
```

```
aaq.class
aah.class
aai.class
aaj.class
aak.class
aal.class
aam.class
aan.class
aao.class
aap.class
aaq.class
aar.class
aas.class
aat.class
aau.class
aav.class
aaw.class
aax.class
aay.class

this.a = paramContext;
SQLiteDatabase.loadLibs(paramContext);
this.b = ("x\\" + cip.a(this.c.b()) + "\\");
}

public SQLiteDatabase a()
{
    try
    {
        SQLiteDatabase localSQLiteDatabase = super.getWritableDatabase(this.b);
        return localSQLiteDatabase;
    }
    finally
    {
        localObject = finally;
    }
}
```



# Android приложение Threema dex2jar + Java Decompiler



Командная строка

```
D:\dex2jar-2.0>d2j-dex2jar.bat ch.threema.app.apk
dex2jar ch.threema.app.apk -o ch.threema.app-dex2jar.jar
```

D:\dex2jar-2.0>

ch.threema.app-dex2jar.jar

android.support  
ch.threema.app  
com  
net.sqlcipher  
a.class  
aa.class  
aaa.class  
aab.class  
aac.class  
aad.class  
aae.class  
aaf.class  
aaq.class  
aaah.class  
aai.class  
aaaj.class  
aak.class  
aal.class  
aam.class  
aan.class  
aao.class  
aap.class  
aaq.class  
aar.class  
aas.class  
aat.class  
aau.class  
aav.class  
aaw.class  
aax.class  
aay.class

File Edit Navigation Search Help

ch.threema.app-dex2jar.jar

cjq.class

```
public class Cjq {
    public Cjq(Context paramContext, Cjl paramcjl, Bug parambug)
    {
        super(paramContext, "threema.db", null, 34, new Cjr(paramContext));
        this.c = paramcjl;
        this.d = parambug;
        this.a = paramContext;
        SQLiteDatabase.loadLibs(paramContext);
        this.b = ("x" + cip.a(this.c.b()) + "");
    }

    public SQLiteDatabase a()
    {
        try
        {
            SQLiteDatabase localSQLiteDatabase = super.getWritableDatabase(this.b);
            return localSQLiteDatabase;
        }
        finally
        {
            localObject = finally;
        }
    }
}
```

# Изучение внутреннего устройства Android приложения Threema



ch.threema.app-dex2jar.jar

File Edit Navigation Search Help

- android.support
- ch.threema.app
- com
- net.sqlcipher
- a.class
- aa.class
- aaa.class
- aab.class
- aac.class
- aad.class
- aae.class
- aaf.class
- aaq.class
- aah.class
- aa\_i.class
- aa\_j.class
- aa\_k.class
- aa\_l.class
- aa\_m.class
- aa\_n.class
- aa\_o.class
- aa\_p.class
- aa\_q.class
- aa\_r.class
- aa\_s.class
- aa\_t.class
- aa\_u.class
- aa\_v.class
- aa\_w.class
- aa\_x.class
- aa\_y.class

```
public cjq(Context paramContext, cjl paramcjl, bug parambug)
{
    super(paramContext, "threema.db", null, 34, new cjr(paramContext));
    this.c = paramcjl;
    this.d = parambug;
    this.a = paramContext;
    SQLiteDatabase.loadLibs(paramContext);
    this.b = ("x\" + cip.a(this.c.b()) + "\"");
}

public SQLiteDatabase a()
{
    try
    {
        SQLiteDatabase localSQLiteDatabase = super.getWritableDatabase(this.b);
        return localSQLiteDatabase;
    }
    finally
    {
        localObject = finally;
    }
}
```

# Android приложения KakaoTalk dex2jar + Java Decompiler



avd.class - Java Decompiler

File Edit Navigation Search Help

com.kakao,talk-dex2jar.jar

- android.support
- com
  - ahnlab
  - cns
  - dreamsecurity
  - github.dazoe.android
  - google.android
  - kakao
    - digitalitem.image.lib
    - sdk
    - talk
    - vox.jni
  - lqcns
  - nshc
  - sothree.slidinguppanel
  - tonicartos.superslim
  - viewpagerindicator
- net
- o
  - A.class
  - AA.class
  - AB.class
  - AC.class
  - AD.class
  - AE.class
  - AF.class
  - AG.class
  - AH.class
  - AI.class
  - AJ.class
  - AK.class

```
import org.json.JSONException;
import org.json.JSONObject;

public final class avd
{
    private static final String[] = { "A3JR7sXQN7", "ssxnV14Taj", "t+x8Nf4-

    /* Error */
    private static String (int paramInt, String paramString)
    {
        // Byte code:
        // 0: ldc 2
        // 2: monitorenter
        // 3: getstatic 32 o/avd:~ [Ljava/lang/String;
        // 6: astore_2
        // 7: aload_2
        // 8: iload_0
        // 9: aaload
        // 10: astore_2
        // 11: getstatic 45 o/lk:f [Ljava/lang/String;
```

# Android приложение KakaoTalk

## IDA Pro



IDA - D:\com.kakao.talk-1\classes.dex

File Edit Jump Search View Debugger Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Functions window

- d\_clinit\_@V
- NativeThread\_clinit\_@V
- NativeMapLoopScheduling\_clinit\_@V
- NativeTileUrlInfo\_clinit\_@V
- NativeMapBuildSettings\_clinit\_@V
- NativeMapController\_clinit\_@V
- NativeMapTrafficManager\_clinit\_@V
- NativeMapEnvironmentType\_clinit\_@V
- NativeMapCoordConverter\_clinit\_@V
- NativeMapEngine\_clinit\_@V
- NativeMapGraphicsViewGles\_clinit\_@V
- NativeMapViewUiEvent\_clinit\_@V
- AM\_@V
- \_\_\_@V\_47
- NativeBaseNetConnection\_clinit\_@V
- auu\_@V
- Ge\_@V
- Ng\_@V
- Pd\_@V

Graph overview

Output window

Search completed

Python

AU: idle Down Disk: 5GB

```
private static java.lang.String o.avd.TK(
    int p0,
    java.lang.String p1)
p0 = v5
p1 = v6
const-class          u4, <t: avd>
monitor-enter        u4

# try 0x611CAA-0x611CAE:
loc_611CAA:
.line 3593
sget-object          v3, avd___

# try 0x611D0C-0x611D12:
loc_611D0C:
invoke-virtual      {v0}, <void Exception.println>
.line 2610
monitor-exit        u4
const/4             v0, 0
return-object        v0

# try 0x611CAE-0x611D04:
loc_611CAE:
.line 2597
.line 2600
aget-object         p0, v3, p0
.line 2601
sget-object         u0, stru_6EF0C
invoke-static       {v0}, <ref Mac.getInstance(ref) imp. @_def_Mac.getInstance@LL_0>
move-result-object v3
.line 2602
new-instance        u0, <t: SecretKeySpec>
```

# Изучение внутреннего устройства Android приложения Threema



ch.threema.app-dex2jar.jar

android.support  
ch.threema.app  
com  
net.sqlcipher  
a.class  
aa.class  
aaa.class  
aab.class  
aac.class  
aad.class  
aae.class  
aaf.class  
aaq.class  
aah.class  
aai.class  
aaj.class  
aak.class  
aal.class  
aam.class  
aan.class  
aao.class  
aap.class  
aaq.class  
aar.class  
aas.class  
aat.class  
aau.class  
aav.class  
aaw.class  
aax.class  
aay.class

cjq.class

```
public cjq(Context paramContext, cjl paramcjl, bug parambug)
{
    super(paramContext, "threema.db", null, 34, new cjr(paramContext));
    this.c = paramcjl;
    this.d = parambug;
    this.a = paramContext;
    SQLiteDatabase.loadLibs(paramContext);
    this.b = ("x\" + cip.a(this.c.b()) + "\"");
}

public SQLiteDatabase a()
{
    try
    {
        SQLiteDatabase localSQLiteDatabase = super.getWritableDatabase(this.b);
        return localSQLiteDatabase;
    }
    finally
    {
        localObject = finally;
    }
}
```

# Android приложение Threema IDA Pro Dalvik debugger



IDA - D:\dex2jar-2.0\classes.dex

File Edit Jump Search View Debugger Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Functions window

- Function name
- cjl\_c@Z
- cjm\_init@VL
- cjn\_clinit@V
- cjn\_init@VL
- cjn\_g@LL
- cjn\_a@LL
- cjn\_a@LL\_0
- cjn\_a@LL\_1
- cjn\_b@LL
- cjn\_c@LL
- cjn\_d@ZL
- cjn\_e@LL
- cjn\_f@LL
- SQLiteOpenHelper\_clinit@V
- SQLiteOpenHelper\_init@VLLLL
- SQLiteOpenHelper\_init@VLLLLL
- SQLiteOpenHelper\_init@VLLLLLL
- SQLiteOpenHelper\_close@V
- SQLiteOpenHelper\_getReadableDatabas

Line 15835 of 25283

Graph overview

```
this = v1
.prologue_end
.line 120
monitor-enter          this
```

```
# try 0x1D9E2A-0x1D9E34:
loc_1D9E2A:
iget-object           v0, this, cjq_b
invoke-super         (this, v0), <ref SQLiteOpenHelper.getWritableDatabase(ref) SQLI
move-result-object   v0
monitor-exit         this

locret:
return-object        v0
```

156.25% (-25,59) (467,131) 001D9E2E 001D9E2E: cjq\_a@L+6 (Synchronized with Hex View-1)

Output window

Search completed

Caching 'Strings window'... ok

Python

AU: idle Down Disk: 3GB

# Android приложение Threema Xposed Modules



```
public class testhook implements IXposedHookLoadPackage {

    public void handleLoadPackage(final LoadPackageParam lpparam) throws Throwable {

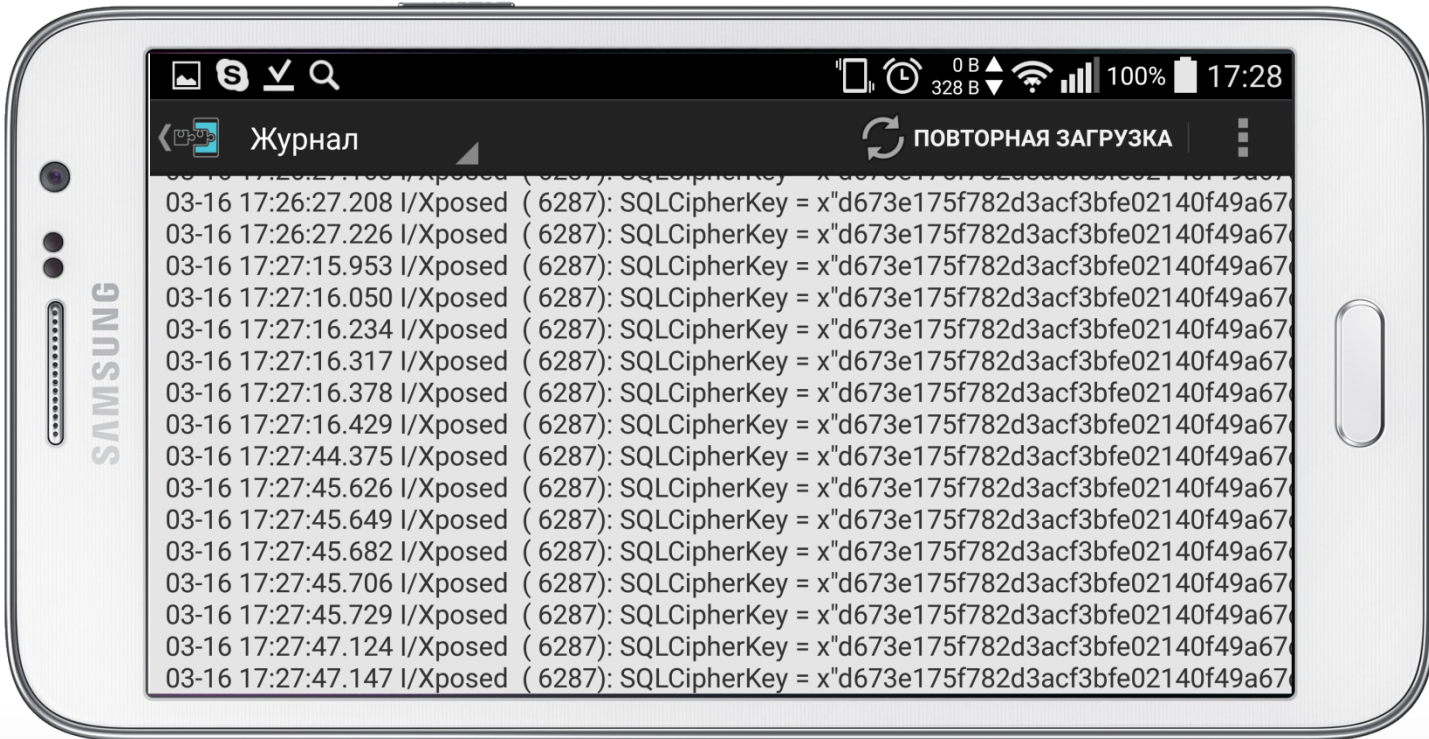
        String packageName = "ch.threema.app";
        String classToHook = "cjq";
        String functionToHook = "a";

        if (!lpparam.packageName.equals(packageName))
            return;

        XposedBridge.log("we are in SystemUI");

        findAndHookMethod(classToHook, lpparam.classLoader, functionToHook, new XC_MethodHook() {
            @Override
            protected void afterHookedMethod(MethodHookParam param) throws Throwable {
                Field SQLCipherKeyField = XposedHelpers.findField(param.thisObject.getClass(), "b");
                String SQLCipherKeyString = (String) SQLCipherKeyField.get(param.thisObject);
                XposedBridge.log("SQLCipherKey = " + SQLCipherKeyString);
            }
        });
    }
}
```

# Android приложение Threema Xposed Modules





# Изучение внутреннего устройства Android приложения Threema



threema.db - Oxygen Forensic SQLite Viewer

File Tools Service Help

Open Export Print Options Help

Recover deleted records Filtering criteria ...

Tables

- sqlite\_sequence (4/0)
- message (5/0)
- m\_group\_message (19/0)
- m\_group (2/0)
- group\_member (8/0)
- contacts (4/0)
- android\_metadata (1/0)
- All Deleted Data

Table data Blocks containing deleted data

#	body	isRead	isSaved	state	postedAt	createdAt	n
1	Group created.	1	1		2014-07-07 15:17:34.000159	2014-07-07 15:17:34.000159	
2	«XE74NMN5» added to group.	1	1		2014-07-07 15:17:34.000203	2014-07-07 15:17:34.000203	
3	«Karabas Barabas» added to group.	1	1		2014-07-07 15:17:34.000249	2014-07-07 15:17:34.000249	
4	«You» added to group.	1	1		2014-07-07 15:17:34.000283	2014-07-07 15:17:34.000283	
5	Group renamed to «nexus 7. samsung s4. iphone 4s (JB)»	1	1		2014-07-07 15:17:34.000488	2014-07-07 15:17:34.000488	
6	Lets talk about 11 07	0	1	SENT	2014-07-07 15:18:16.000214	2014-07-07 15:18:16.000214	
7	and wha rt?	1	1		2014-07-07 15:17:12.000000	2014-07-07 15:18:33.000466	
8	«XE74NMN5» added to group.	0	0		2014-07-07 17:28:18.000613	2014-07-07 17:28:18.000613	
9	«R22D6MAC» added to group.	0	0		2014-07-07 17:28:20.000004	2014-07-07 17:28:20.000004	
10	«AH5BBW9» added to group.	0	0		2014-07-07 17:28:20.000743	2014-07-07 17:28:20.000743	
11	«Karabas Barabas» added to group.	0	0		2014-07-07 17:28:20.000837	2014-07-07 17:28:20.000837	
12	«You» added to group.	0	0		2014-07-07 17:28:20.000889	2014-07-07 17:28:20.000890	
13	Group created.	0	0		2014-07-07 17:28:21.000063	2014-07-07 17:28:21.000063	
14	Send to all my contacts	0	1		2014-07-07 17:26:55.000000	2014-07-07 17:28:21.000166	

00000000: 4C 65 74 73 20 74 61 6C 6B 20 61 62 6F 75 74 20 Lets talk about  
00000010: 31 31 20 30 37 11 07

File type: sqlite File size: 23 KB Tables: 7 Table items: 19 SHA-2 Hash: 63a998e8d322f3cf0d2c043156e22e9ea2203293022a8b99e8ebf683c41856e

# Изучение внутреннего устройства Android приложения Threema



cjq.class - Java Decompiler

File Edit Navigation Search Help

ch.threema.app-dex2jar.jar

- android.support
- ch.threema.app
- com
- net.sqlcipher
- a.class
- aa.class
- aaa.class
- aab.class
- aac.class
- aad.class
- aae.class
- aaf.class
- aaq.class
- aah.class
- aa\_i.class
- aa\_j.class
- aa\_k.class
- aa\_l.class
- aa\_m.class
- aa\_n.class
- aa\_o.class
- aa\_p.class
- aa\_q.class
- aa\_r.class
- aa\_s.class
- aa\_t.class
- aa\_u.class
- aa\_v.class
- aa\_w.class
- aa\_x.class
- aa\_y.class

```
public cjq(Context paramContext, cjl paramcjl, bug parambug)
{
    super(paramContext, "threema.db", null, 34, new cjr(paramContext));
    this.c = paramcjl;
    this.d = parambug;
    this.a = paramContext;
    SQLiteDatabase.loadLibs(paramContext);
    this.b = ("x\" + cip.a(this.c.b()) + "\"");
}

public SQLiteDatabase a()
{
    try
    {
        SQLiteDatabase localSQLiteDatabase = super.getWritableDatabase(this.b);
        return localSQLiteDatabase;
    }
    finally
    {
        localObject = finally;
    }
}
```

# Изучение внутреннего устройства Android приложения Threema



Total Commander

Файлы Выделение Навигация Сеть FTP Вид Вкладки Конфигурация Инструменты Запуск Справка

с d \ \ .. [\_нет\_] с d \ \ .. [lenovo] 4,2 Гб из 24,9 Гб свободно

\\ADB\LG855c20f60bf\data\data\ch.threema.app\files\\*.\*

Имя	Тип	Owner	Group	Size	Date
..					
icu		u0_a137	u0_a137	<Папка>	10.03.20
key	dat	u0_a137	u0_a137	45	12.03.20
msgqueue ser		u0_a137	u0_a137	32	16.03.20

0 байт из 77 байт, файлов: 0 из 2, папок: 0 из 1

d:\ch.threema.app\databases>

d:\ch.threema.app\databases\\*.\*

Имя	Тип	Размер	Дата
..			
threema	db	54 272	10.03.2016 13:28

0 байт из 53,0 Кб, файлов: 0 из 1

F3 Просмотр F4 Правка F5 Копирование F6 Перемещение F7 Каталог F8 Удаление Alt+F4 Выход

# Изучение внутреннего устройства Android приложения Threema



D:\ch.threema.app\files\key.dat - Notepad++

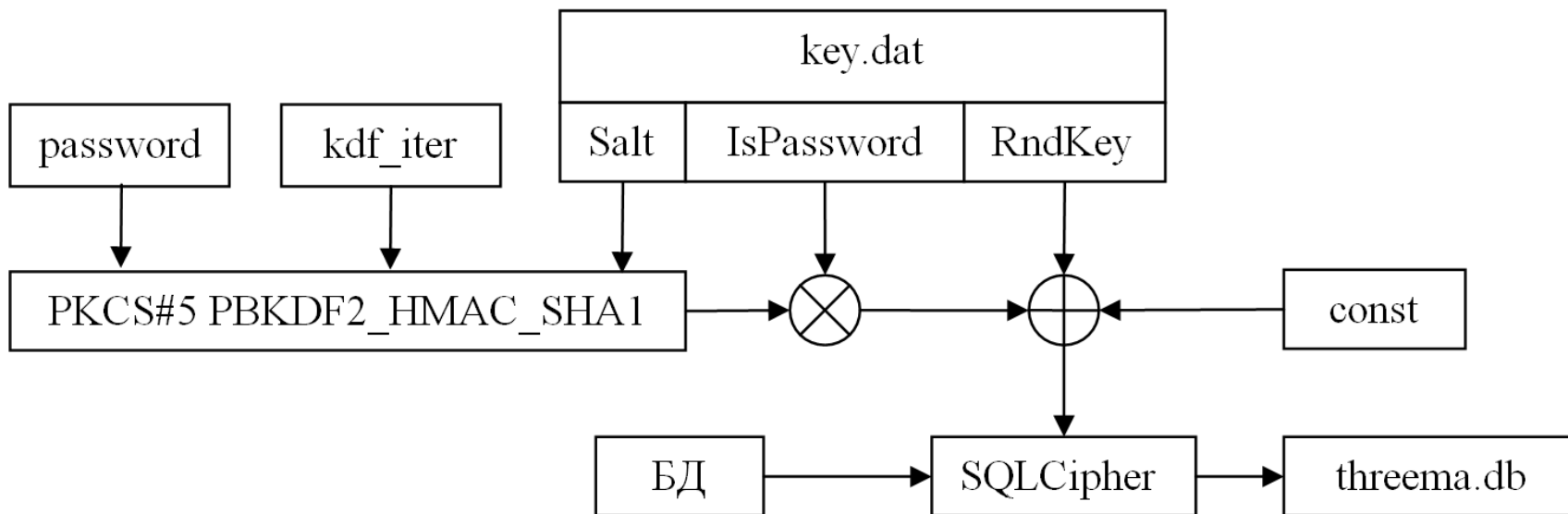
Файл Правка Поиск Вид Кодировки Синтаксисы Опции Макросы Запуск Плагины Окна ?

key.dat

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	00	43	7e	c7	0f	7f	68	a4	bc	6f	ef	07	1e	07	14	f3	.C~3..hαjоп....у
00000010	15	07	7f	7e	f1	cc	50	8d	16	5d	f2	b9	f1	61	84	d0	...~сMP..]т№са,,Р
00000020	9c	0d	c9	63	6b	7b	f5	e1	90	2d	43	52	f9				ъ.Йск{хб.-CRщ

Hex Edit View      nb char : 45      Ln : 0 Col : 9 Sel : 8      Hex      BigEndian

# Изучение внутреннего устройства Android приложения Threema



# Изучение внутреннего устройства Android приложения Threema



threema.db - Oxygen Forensic SQLite Viewer

File Tools Service Help

Open Export Print Options Help

Recover deleted records Filtering criteria ...

Tables

- sqlite\_sequence (4/0)
- message (5/0)
- m\_group\_message (19/0)
- m\_group (2/0)
- group\_member (8/0)
- contacts (4/0)
- android\_metadata (1/0)
- All Deleted Data

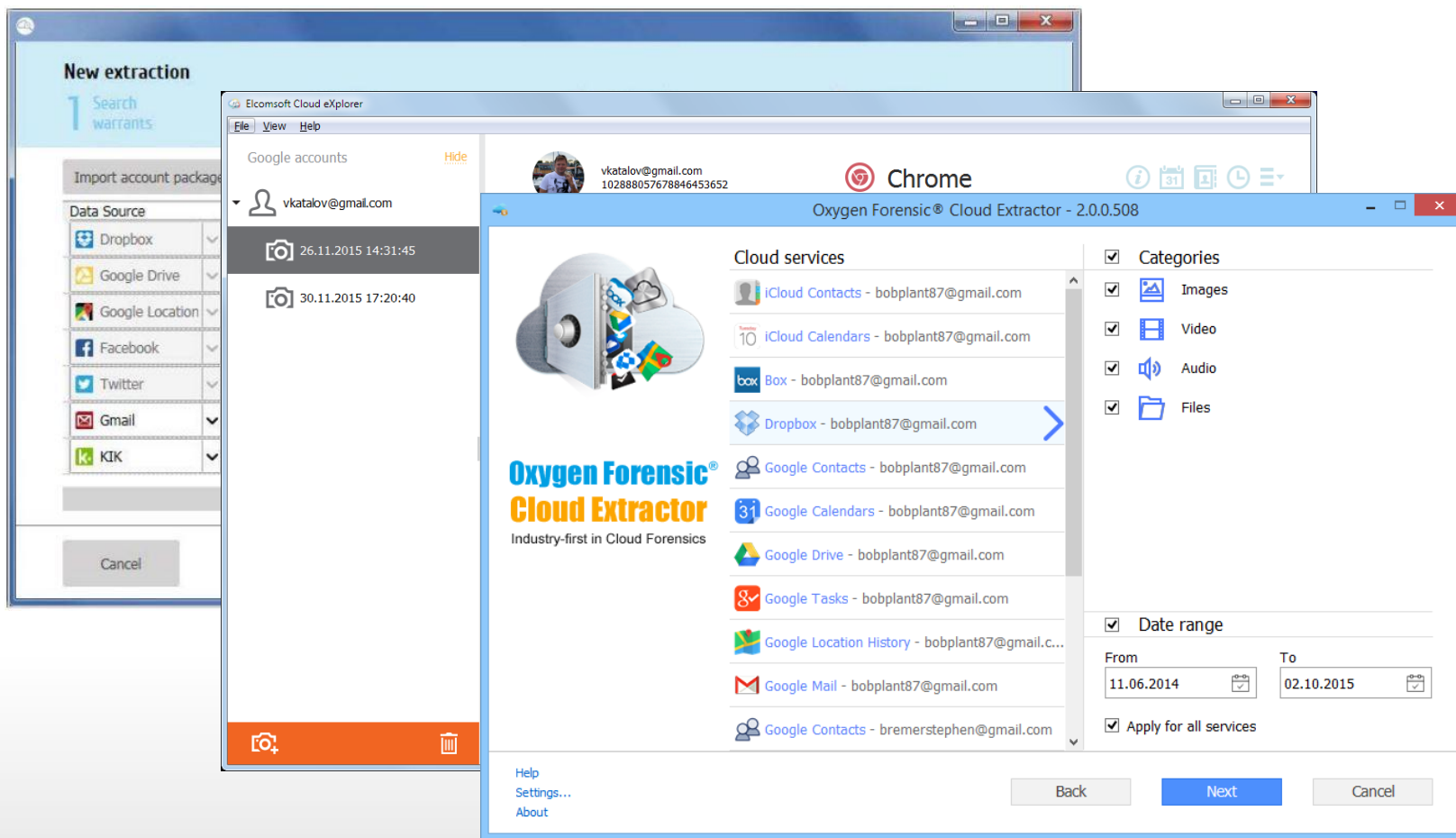
Table data Blocks containing deleted data

#	body	isRead	isSaved	state	postedAt	createdAt	n
1	Group created.	1	1		2014-07-07 15:17:34.000159	2014-07-07 15:17:34.000159	
2	«XE74NMN5» added to group.	1	1		2014-07-07 15:17:34.000203	2014-07-07 15:17:34.000203	
3	«Karabas Barabas» added to group.	1	1		2014-07-07 15:17:34.000249	2014-07-07 15:17:34.000249	
4	«You» added to group.	1	1		2014-07-07 15:17:34.000283	2014-07-07 15:17:34.000283	
5	Group renamed to «nexus 7. samsung s4. iphone 4s (JB)»	1	1		2014-07-07 15:17:34.000488	2014-07-07 15:17:34.000488	
6	Lets talk about 11 07	0	1	SENT	2014-07-07 15:18:16.000214	2014-07-07 15:18:16.000214	
7	and wha rt?	1	1		2014-07-07 15:17:12.000000	2014-07-07 15:18:33.000466	
8	«XE74NMN5» added to group.	0	0		2014-07-07 17:28:18.000613	2014-07-07 17:28:18.000613	
9	«R22D6MAC» added to group.	0	0		2014-07-07 17:28:20.000004	2014-07-07 17:28:20.000004	
10	«AH5BBBW9» added to group.	0	0		2014-07-07 17:28:20.000743	2014-07-07 17:28:20.000743	
11	«Karabas Barabas» added to group.	0	0		2014-07-07 17:28:20.000837	2014-07-07 17:28:20.000837	
12	«You» added to group.	0	0		2014-07-07 17:28:20.000889	2014-07-07 17:28:20.000890	
13	Group created.	0	0		2014-07-07 17:28:21.000063	2014-07-07 17:28:21.000063	
14	Send to all my contacts	0	1		2014-07-07 17:26:55.000000	2014-07-07 17:28:21.000166	

00000000: 4C 65 74 73 20 74 61 6C 6B 20 61 62 6F 75 74 20 Lets talk about  
00000010: 31 31 20 30 37 11 07

File type: sqlite File size: 23 KB Tables: 7 Table items: 19 SHA-2 Hash: 63a998e8d322f3cf0d2c043156e22e9ea2203293022a8b99e8ebf683c41856e

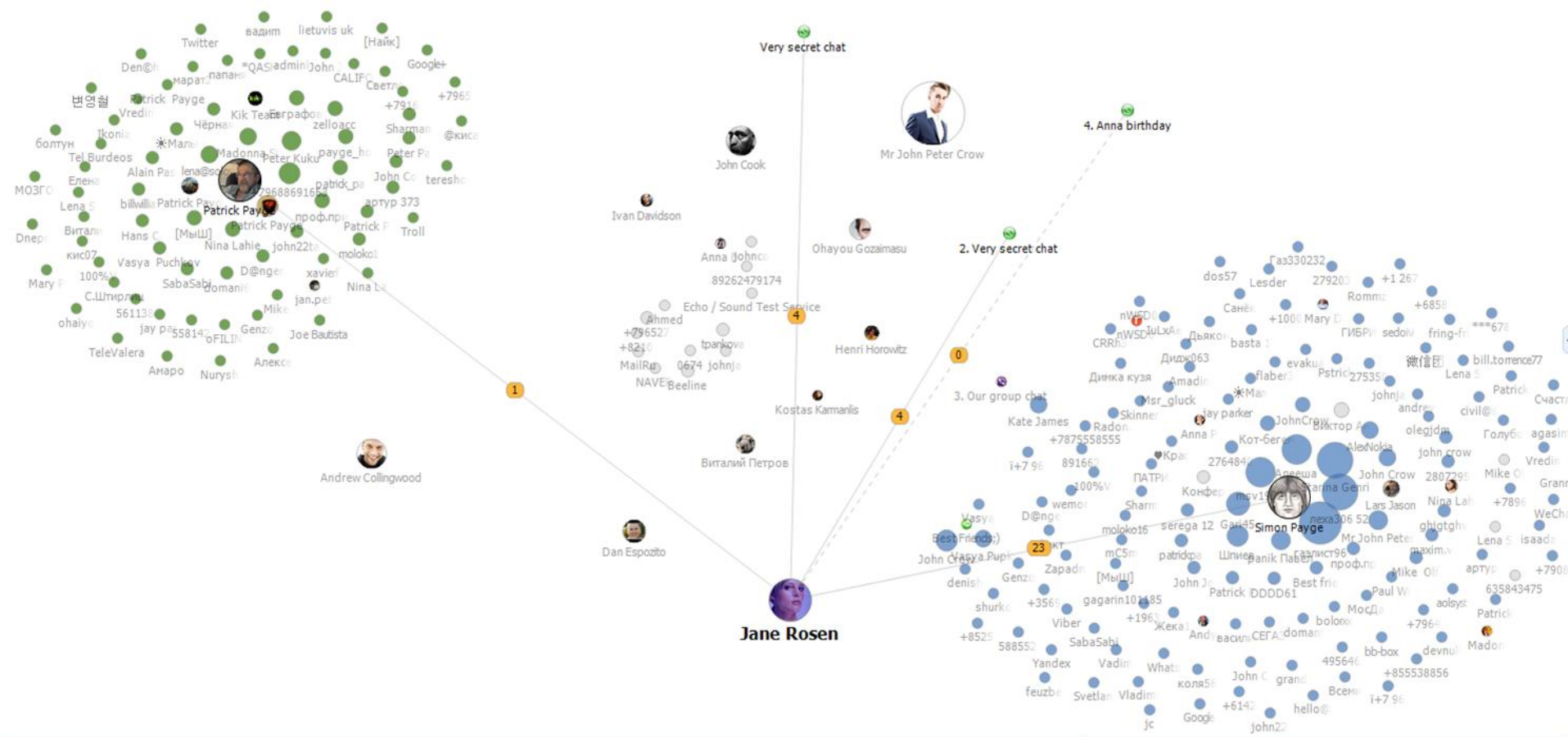
# Извлечение данных из облачных хранилищ



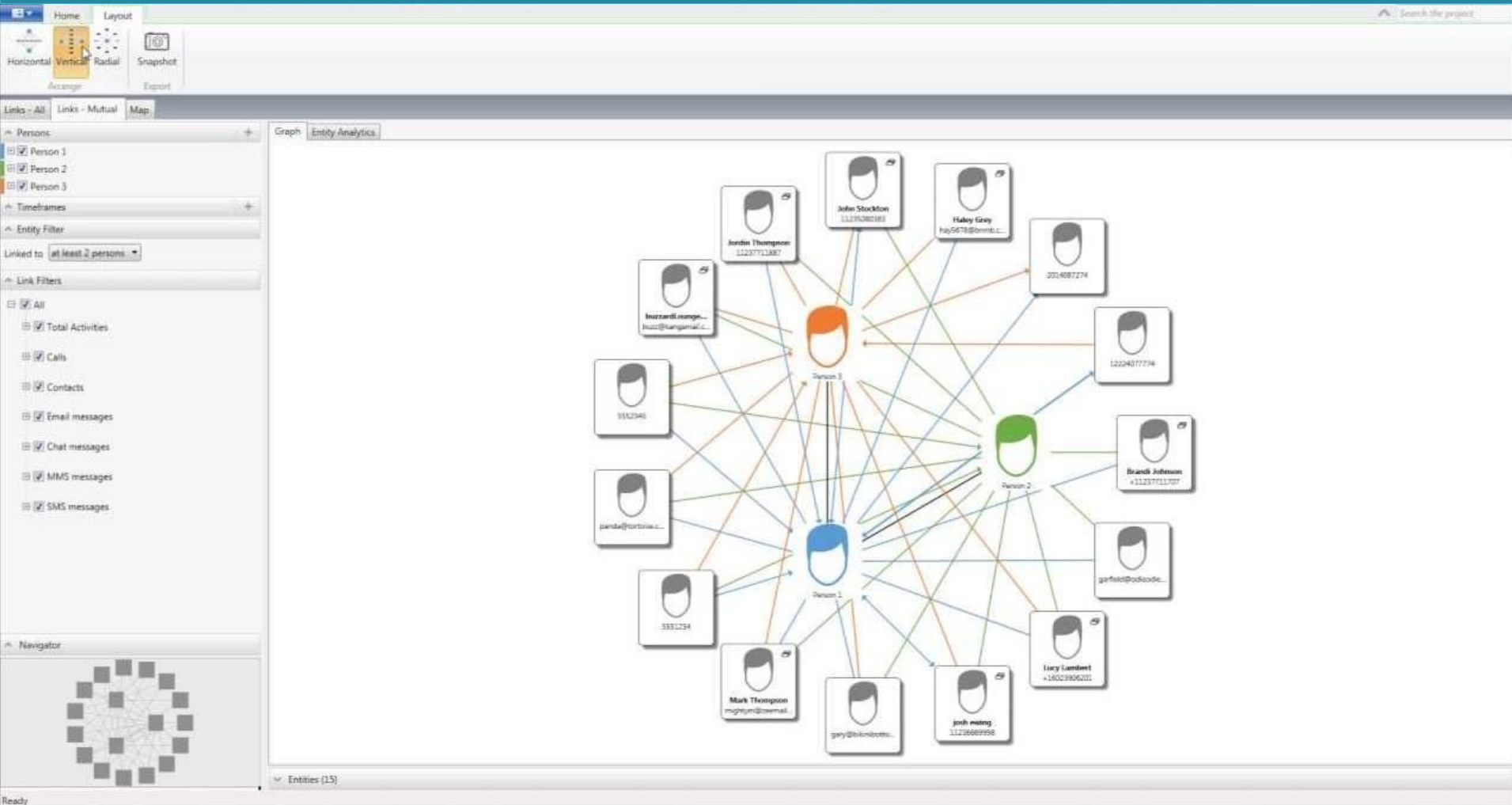




# Агрегация данных из нескольких телефонов



# Агрегация данных из нескольких телефонов



# Детализация определенного периода времени

Connect device Export Print Set time zones Maps and routes Export to Google Earth Diagrams Columns Reset Filters Help

Information << List Date Contact GEO data Sort Color settings Autize columns

**Event information**

Data source: Kik Messenger  
 Type: Kik Message  
 Direction: (Incoming message)  
 From: John Crow <johncrow\_4ba@talk.kik.com>  
 To: Patrick Payge <patrickpayge\_0a0@talk.kik.com>  
 Time stamp (Device time): 06.09.2012 14:11:22  
 Time stamp (UTC): 06.09.2012 10:11:22  
 ID: 20  
 Remote party: John Crow  
 Source file: kik.sqllite  
 Source table: ZKIKMESSAGE, ZKIKUSER  
[Show event card](#)

**Remote Party**

**John Crow**  
 johncrow  
 No photo  
 Internet  
 Email: johncrow\_4ba@talk.kik.com

Type	Time stamp (Device time)	Description	Remote party
Kik Message	06.09.2012 14:11:22		John Crow <johncrow_4ba@talk.kik.com>
SMS	06.09.2012 16:41:27	Hi Andrew how are you?	+7 965 276-42-90
Skype chat (patrick.p...)	06.09.2012 19:56:55	Patrick Payge: <sms alt="Need ...	+68587234984
Kik Message	06.09.2012 14:12:11	049f2198-ff59-4005-9252-eb7b...	John Crow <johncrow_4ba@talk.kik.com>
MMS	06.09.2012 15:59:26	4th window on the upper right	Mr John Peter Crow <+796886865325>
iMessage	06.09.2012 16:26:40	All righty	Patrick Jr <patrickpaygehome@gmail.com>
SMS	06.09.2012 16:36:51	As usual...	Mr John Peter Crow <+796886865325>
iMessage	06.09.2012 16:40:17	Black one	Patrick Jr <patrickpaygehome@gmail.com>

**Activity matrix**

Activity Hours

Legend:

- Low activity (1-39)
- Intermediate activity (40-79)
- High activity (80-119)
- Extreme activity (120-159)

**Filters:**

Date filter: 09.04.2010 - 01.09.2035

Remote party filter

**Contact names**

- [MyL] (4)
- \*Мальшка\* (6)
- \*Красавчик\* (5)
- 100%VIRUS (1)
- Ahmed (5)
- Alexey Glotov (1)
- AlexNokia (25)
- Amadinka (2)
- Andrew Collingwood ...
- andrey117 (7)
- Andy Williams (4)
- Anna Bobson (6)
- Anna Peterson (5)
- aolsystemsg (3)
- basta 19 (2)
- bb-box (1)
- Beeline (9)
- Best friend (10)
- bill.torrence77 (2)
- Carla (24)
- CRRh3AvZxvXqnRyh\_eA...
- D@nger1979 (1)
- Dan Esposito (17)
- DDDD61 (10)

Additional: All events Communications



# Подводим итоги



# Основные этапы криминалистического анализа мобильного приложения

- Изучение окружения приложения
- Изучение внутреннего устройства приложения
- Расшифровывание данных
- Преобразование данных к понятному следователю виду

# Изучение внутреннего устройства Android приложения

- Статический анализ:
  - dex2jar + Java Decompiler
  - IDA Pro
- Динамический анализ:
  - IDA Pro Dalvik debugger
  - IDA Pro Remote ARM Linux/Android debugger
  - Xposed Modules

# Что осталось за кадром



- Извлечение данных
  - Извлечение из «живого» устройства
  - Резервные копии
  - JTAG образы
  - Chip-off образы
  - Данные из облачных хранилищ



СПАСИБО ЗА ВНИМАНИЕ!



# Вопросы???



