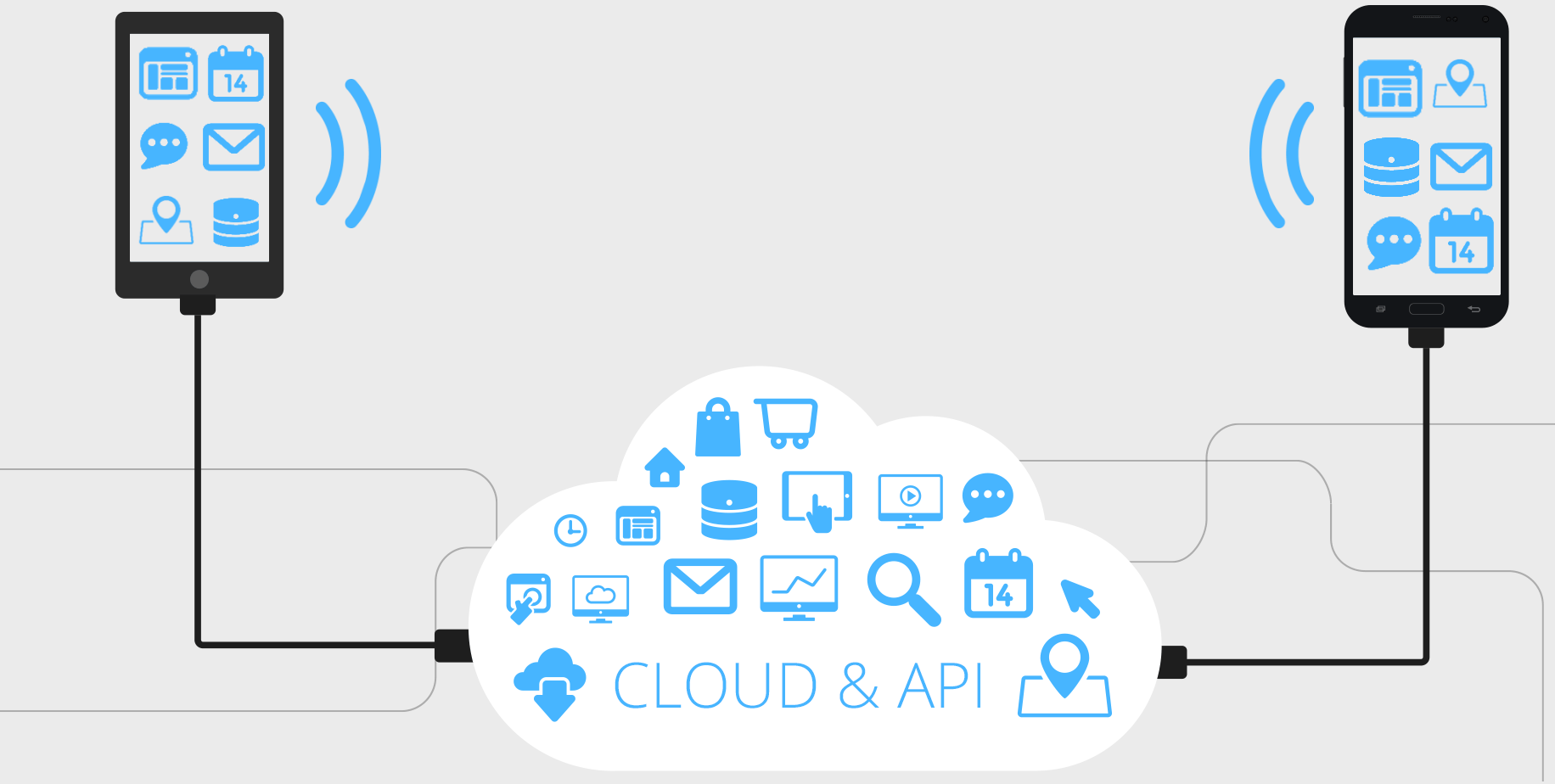
Криминалистический анализ данных Android приложений

Карондеев Андрей

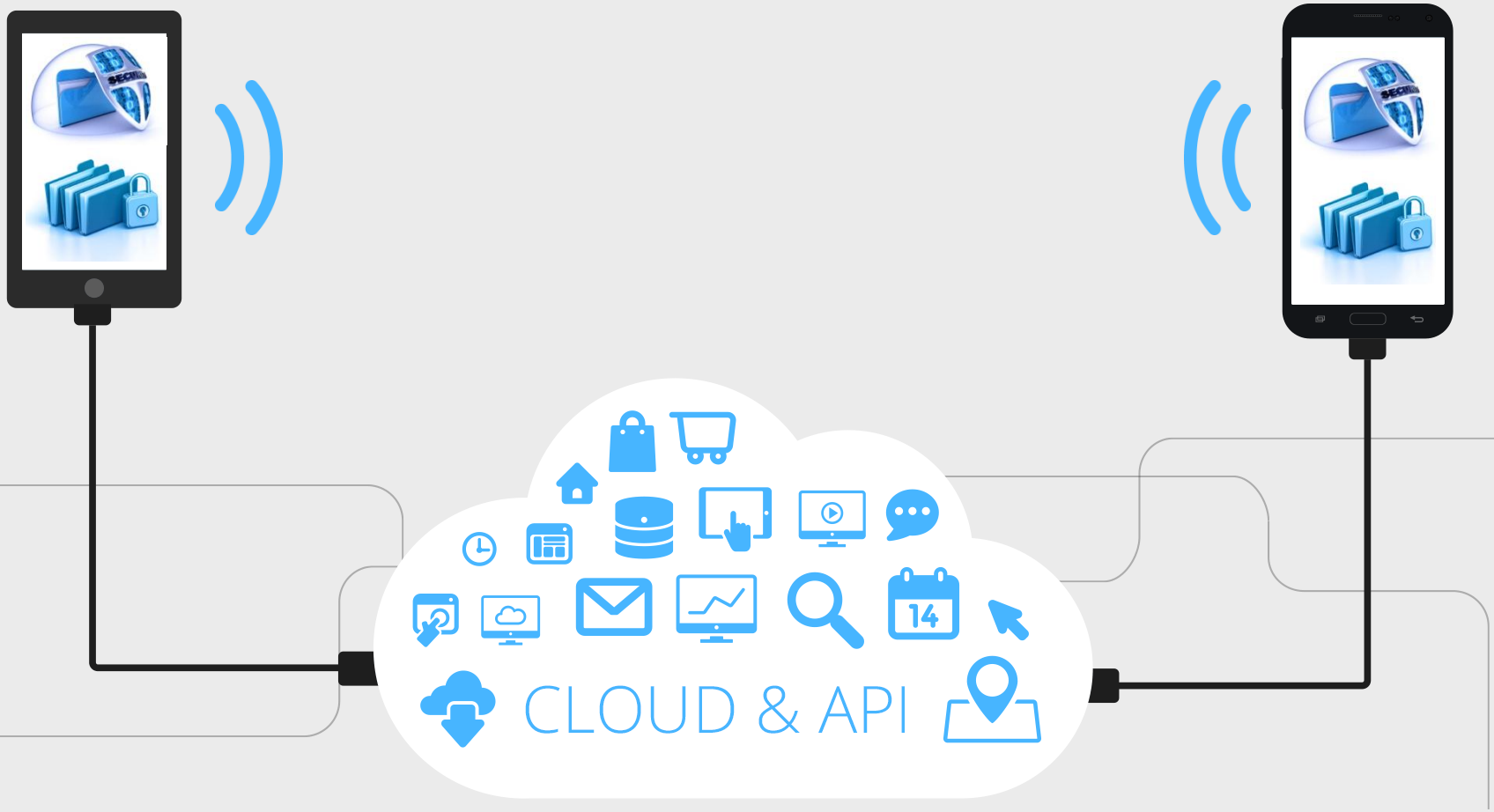
Данные мобильных приложений

Данные мобильных приложений

Данные мобильных приложений



Данные мобильных приложений



Разнообразия мобильных платформ и приложений

Разнообразия 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
Total	**403,109.4**	**100.0**	**367,334.4**	**100.0**

Source: Gartner (February 2016)

Разнообразия 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

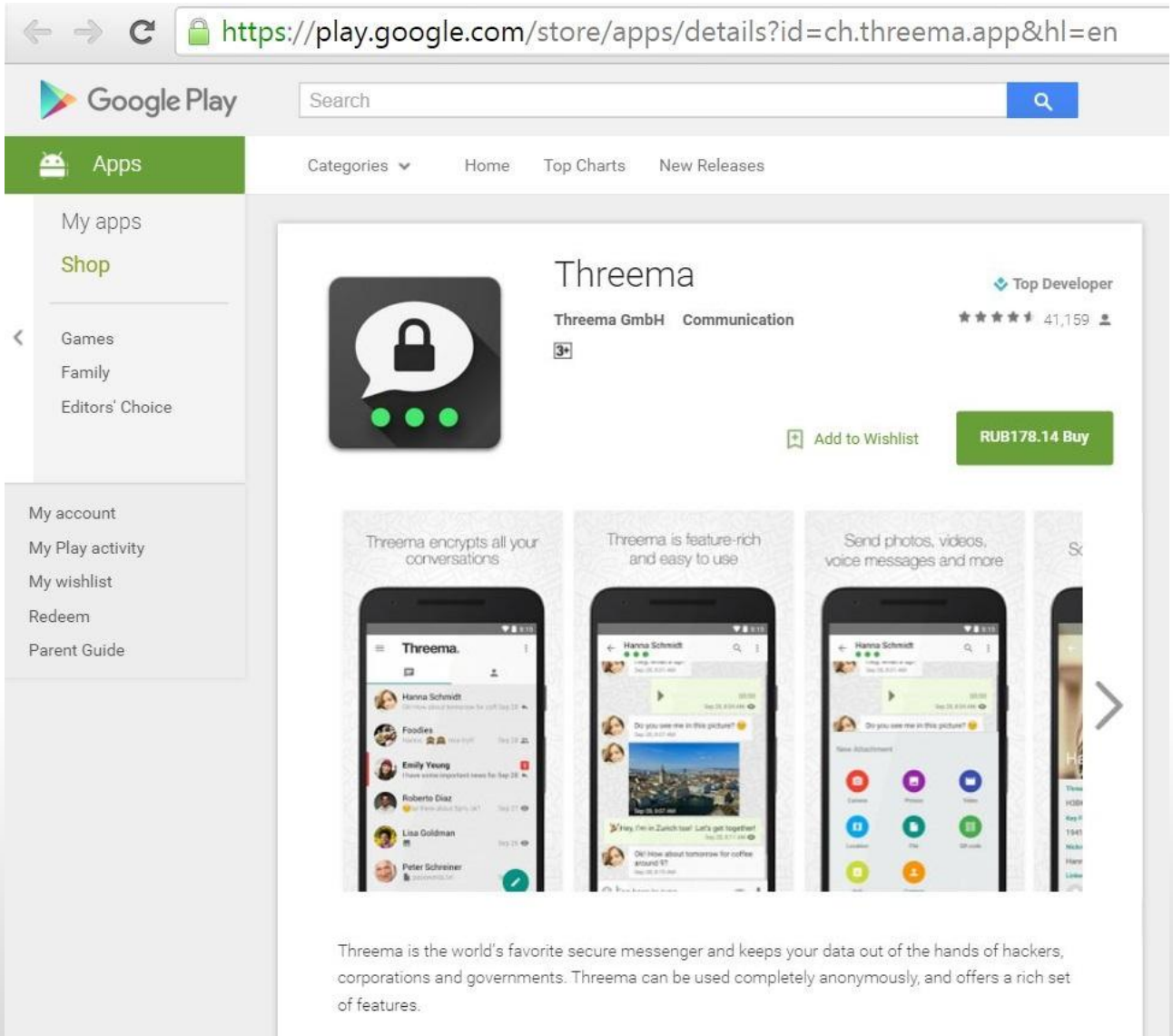
http://www.мобильный-криминалист.рф

Эксперт приступает к анализу

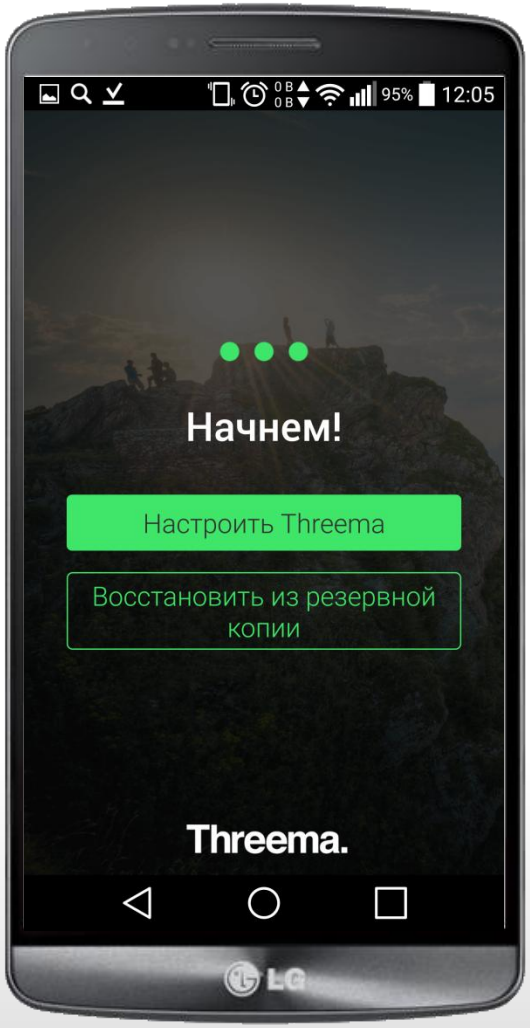
Threema.

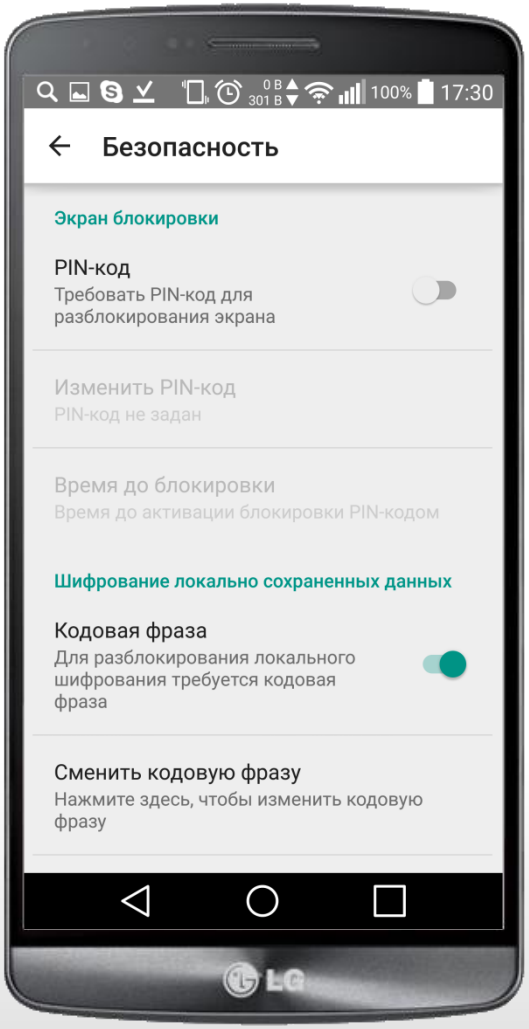
Seriously secure mobile messaging.

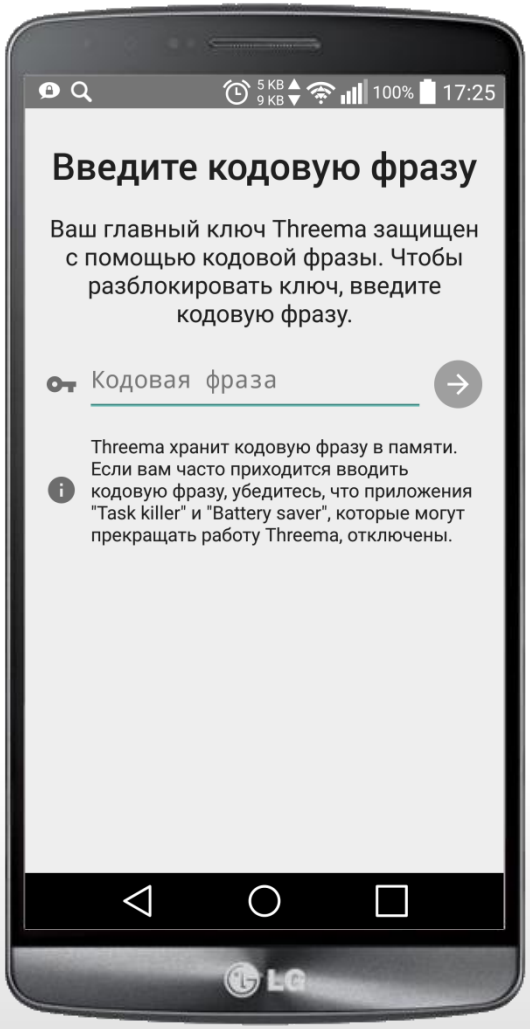
Android мессенджер Threema



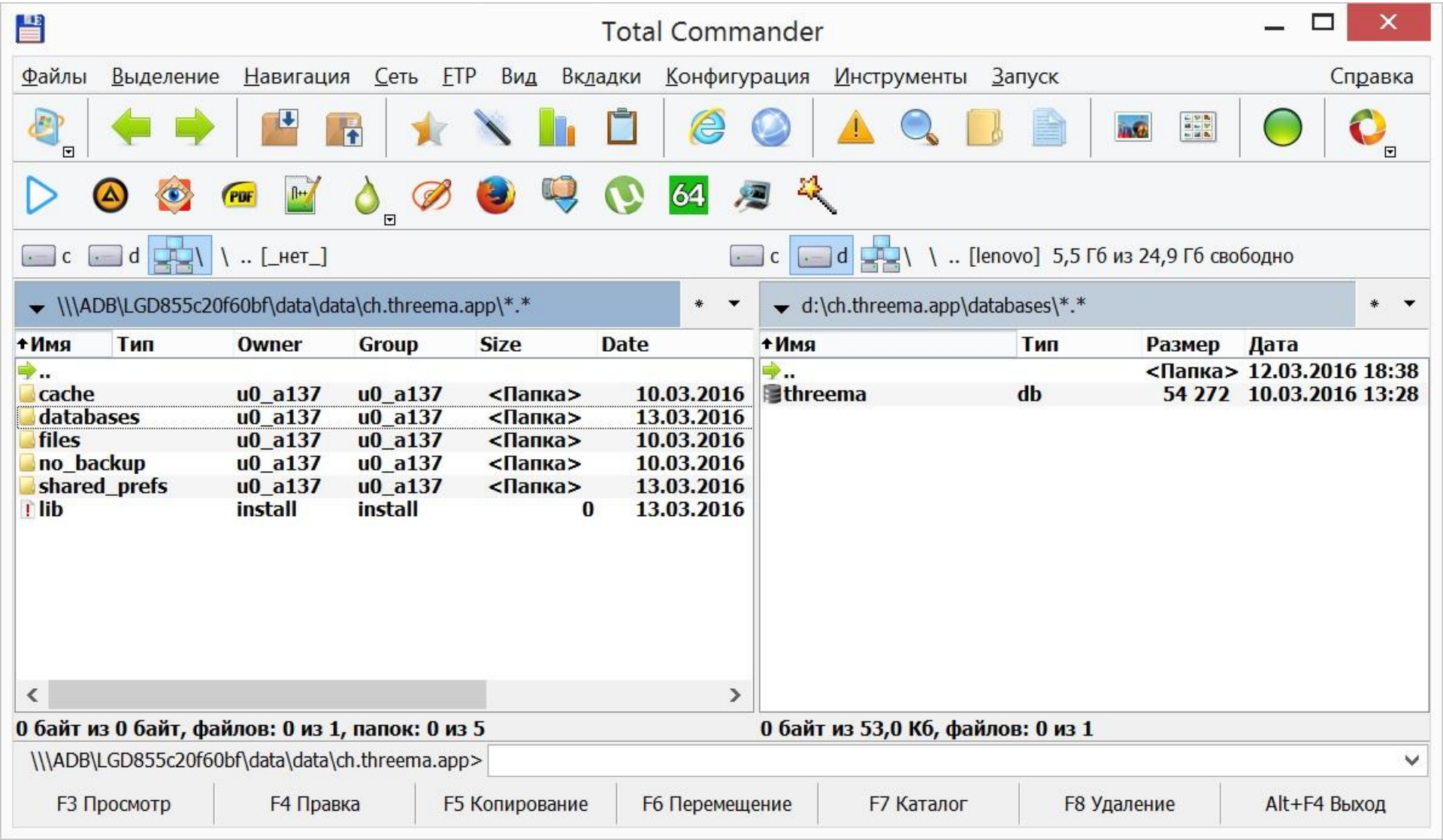
Android мессенджер Threema



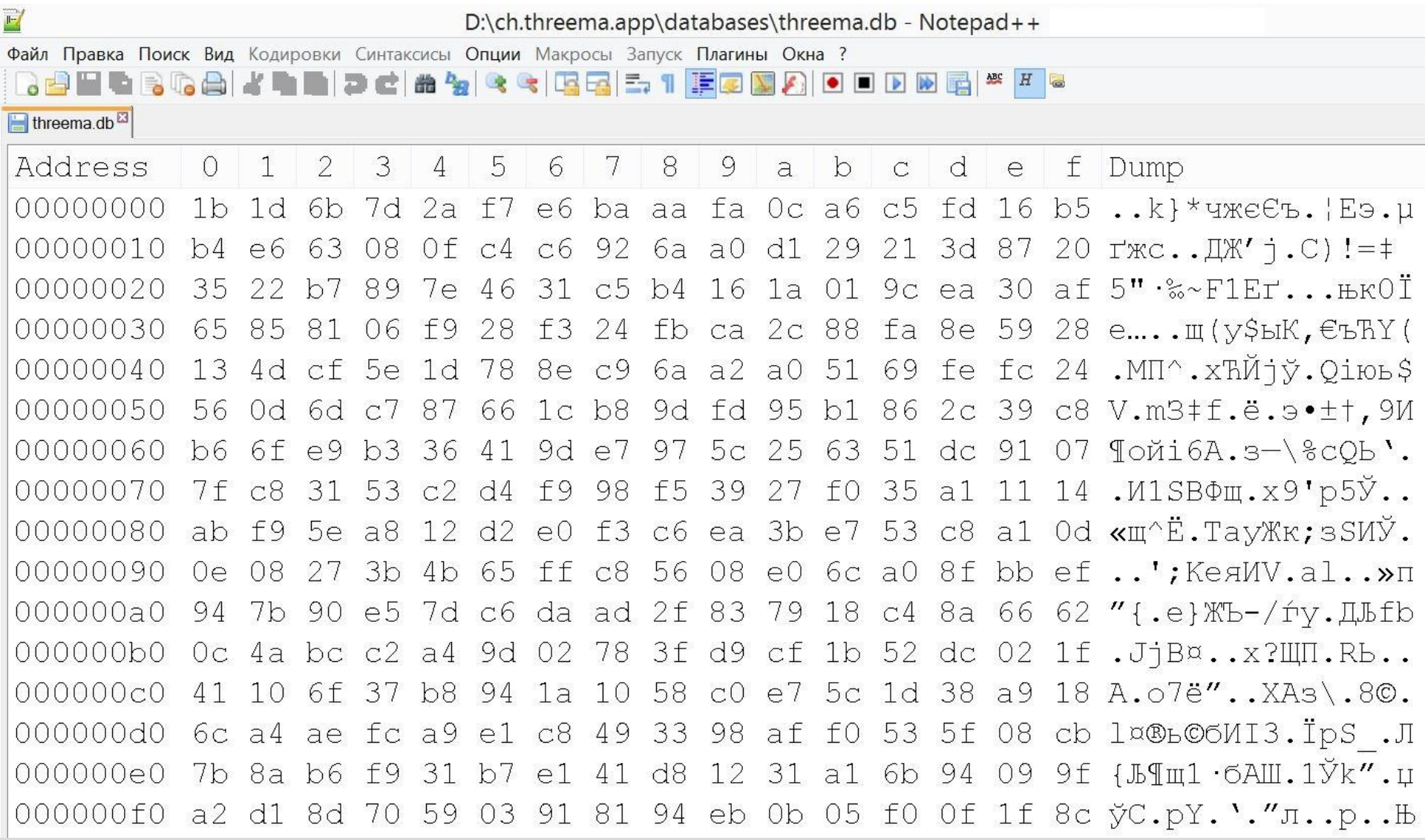




Данные Android приложения Threema

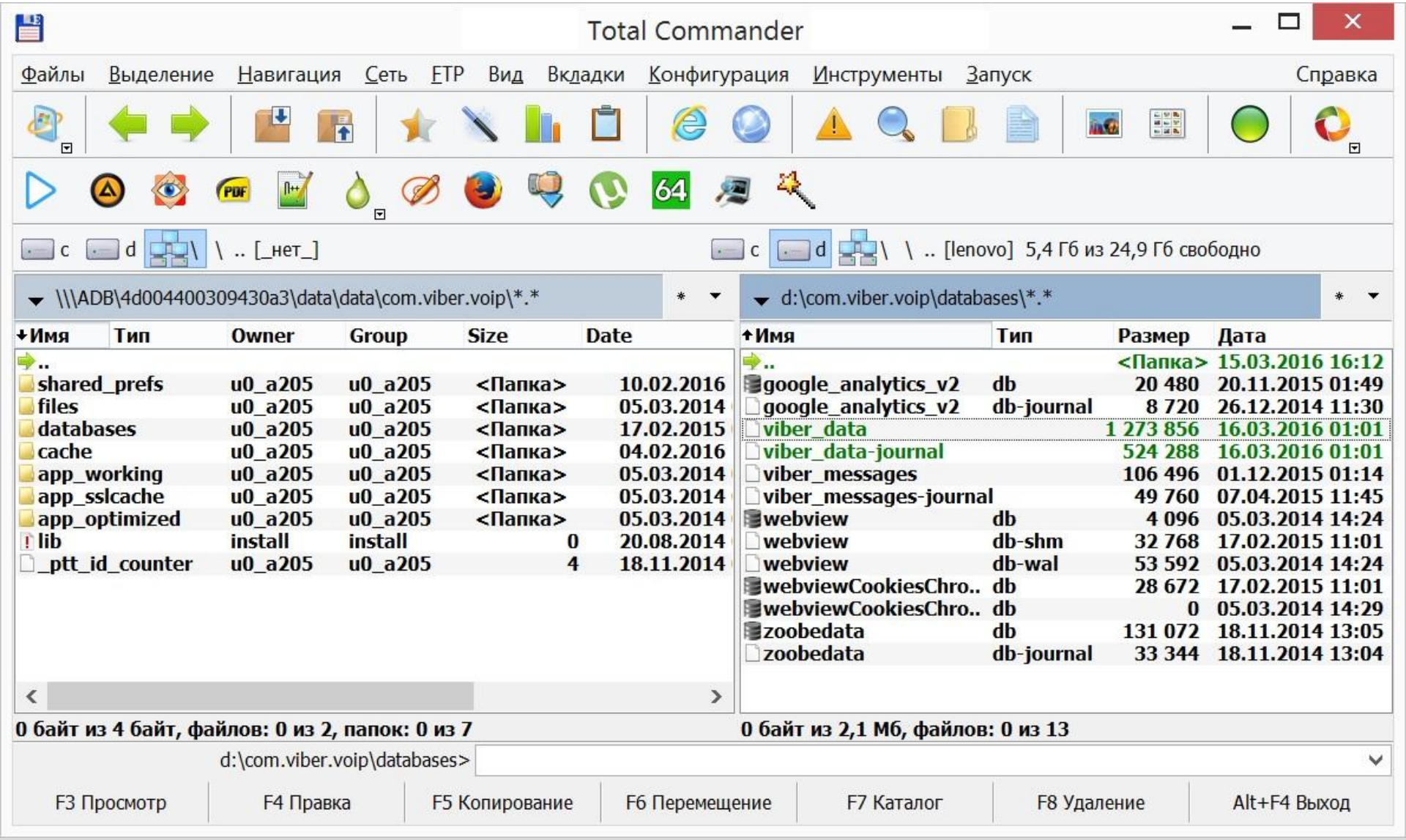


Данные Android приложения Threema



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}*чжєЄъ.¦Еэ.µ
00000010	b4	e6	63	08	0f	c4	c6	92	6a	a0	d1	29	21	3d	87	20	ґжс..ДЖ'j.С)!=‡
00000020	35	22	b7	89	7e	46	31	c5	b4	16	1a	01	9c	ea	30	af	5"·‰~F1Еґ...њк0Ї
00000030	65	85	81	06	f9	28	f3	24	fb	ca	2c	88	fa	8e	59	28	e…..щ(у$ыК,€ъЋY(
00000040	13	4d	cf	5e	1d	78	8e	c9	6a	a2	a0	51	69	fe	fc	24	.МП^.xЋЙjў.Qiюь$
00000050	56	0d	6d	c7	87	66	1c	b8	9d	fd	95	b1	86	2c	39	c8	V.mЗ‡f.ё.э•±†,9И
00000060	b6	6f	e9	b3	36	41	9d	e7	97	5c	25	63	51	dc	91	07	¶ойі6A.з—\%cQЬ'.
00000070	7f	c8	31	53	c2	d4	f9	98	f5	39	27	f0	35	a1	11	14	.И1SВФщ.x9'р5Ў..
00000080	ab	f9	5e	a8	12	d2	e0	f3	c6	ea	3b	e7	53	c8	a1	0d	«щ^Ё.ТауЖк;зSИЎ.
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-/ѓу.ДЉfb
000000b0	0c	4a	bc	c2	a4	9d	02	78	3f	d9	cf	1b	52	dc	02	1f	.Jjв¤..x?ЩП.RЬ..
000000c0	41	10	6f	37	b8	94	1a	10	58	c0	e7	5c	1d	38	a9	18	A.o7ё”..ХАз\.8©.
000000d0	6c	a4	ae	fc	a9	e1	c8	49	33	98	af	f0	53	5f	08	cb	l¤®ь©бИI3.ЇрS_.Л
000000e0	7b	8a	b6	f9	31	b7	e1	41	d8	12	31	a1	6b	94	09	9f	{Љ¶щ1·бАШ.1Ўk”.ц
000000f0	a2	d1	8d	70	59	03	91	81	94	eb	0b	05	f0	0f	1f	8c	ўС.pY.‘.”л..р..Њ

Данные Android приложения Viber



Данные Android приложения Viber

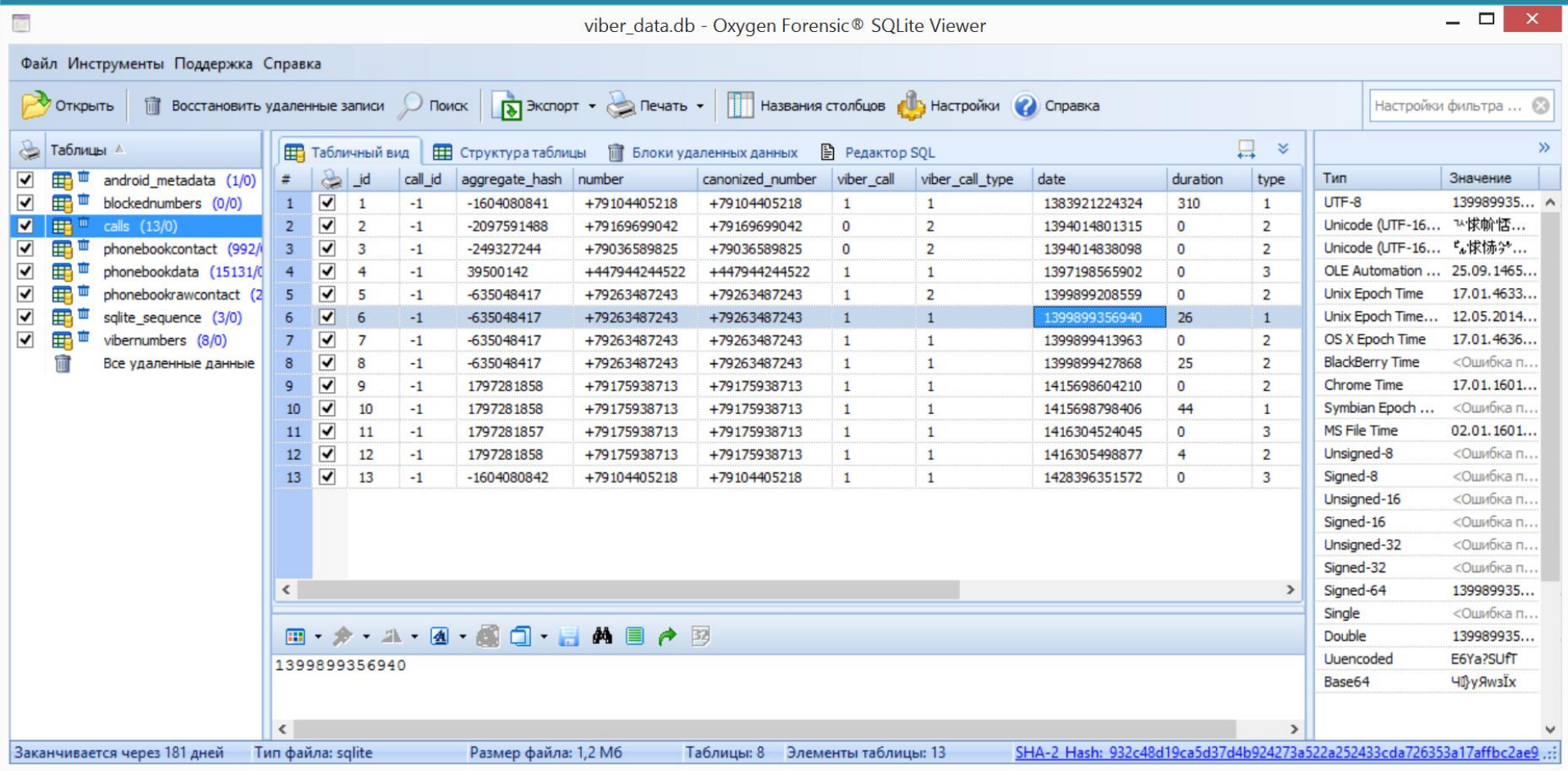
D:\com.viber.voip\databases\viber_data - Notepad++

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

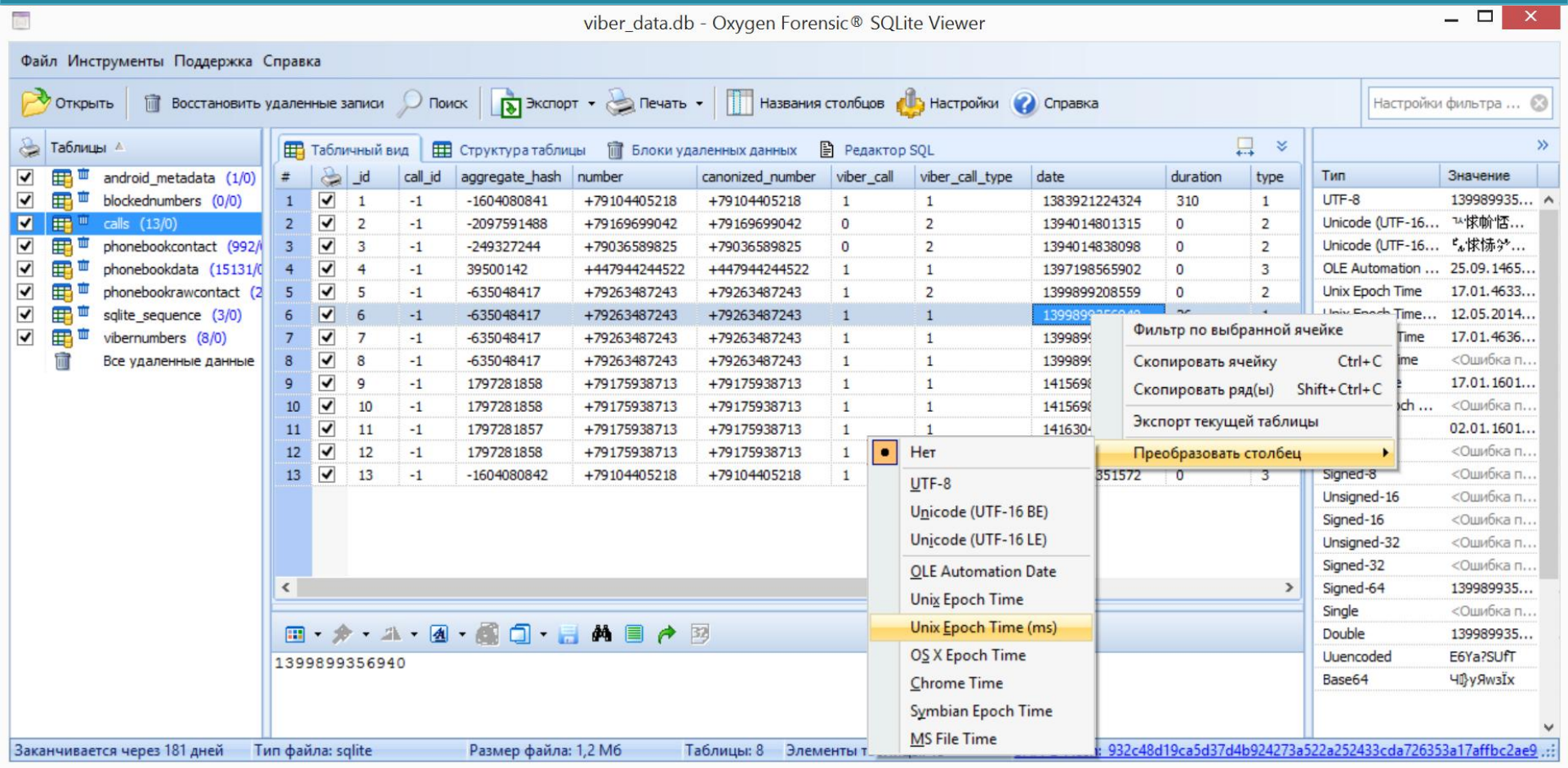
viber_data

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	.....@ ..ћH...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	00	9e	cd	.....ћH
00000060	00	2d	e2	23	0d	09	80	00	0d	05	7b	00	0f	a7	0e	08	.-в#..Ђ...{..§..
00000070	0d	b6	0b	39	0d	6b	05	7b	0c	40	09	db	08	a3	08	16	.¶.9.k.{.@.Ы.J..
00000080	07	cf	0c	8f	09	9a	00	00	00	00	00	00	00	00	00	00	.П...љ.....
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	.....

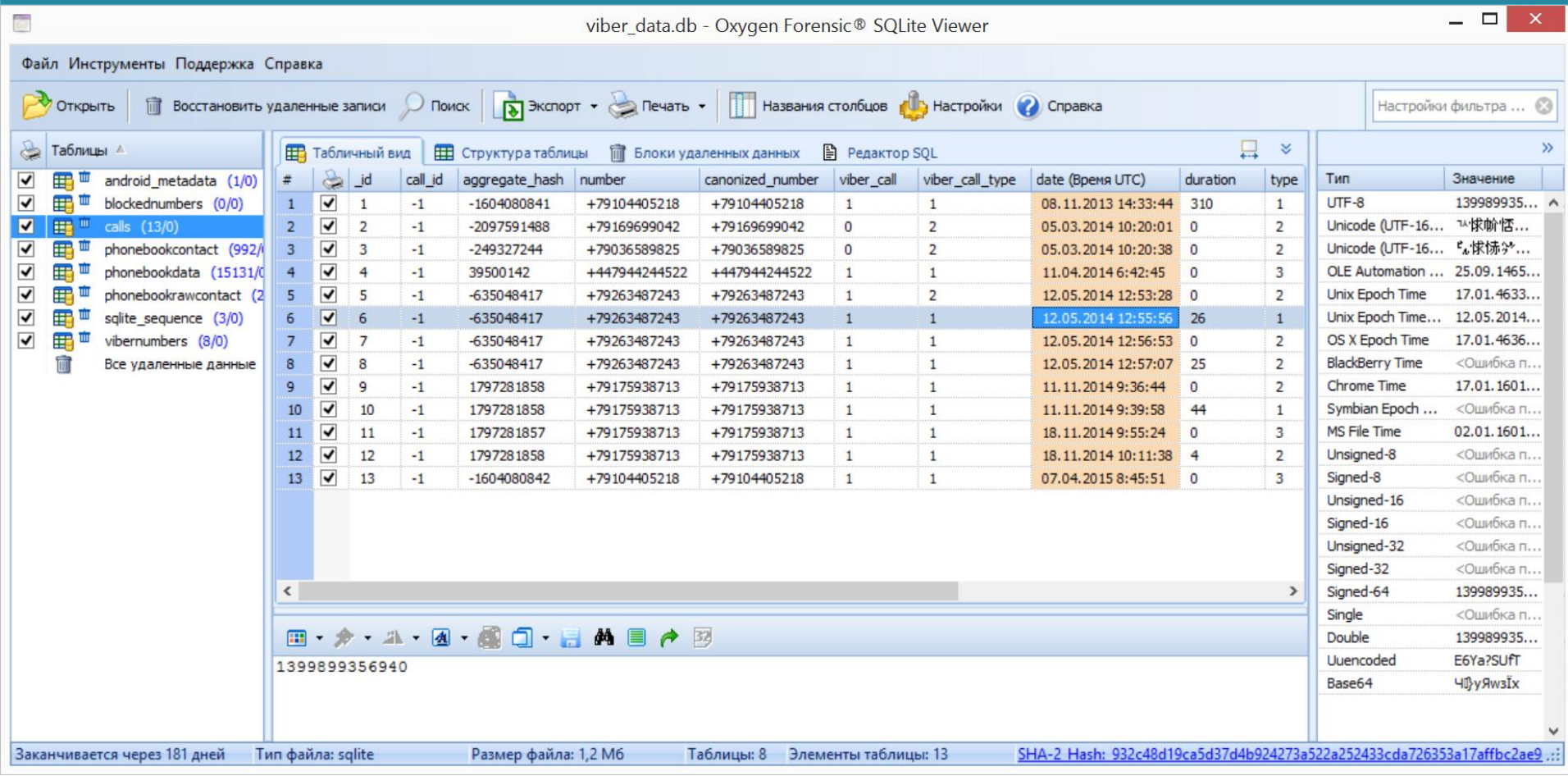
Данные Android приложения Viber



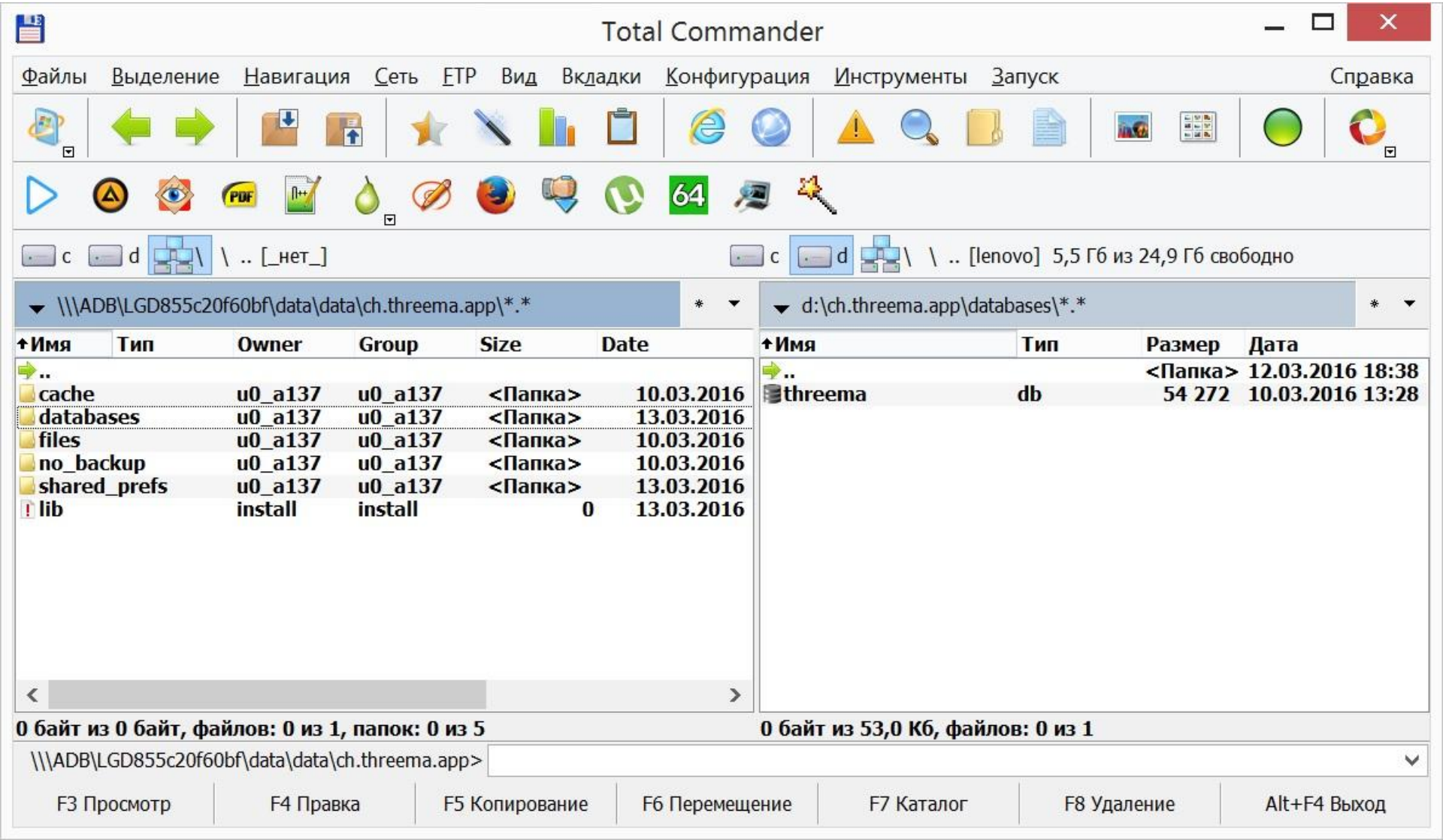
Данные Android приложения Viber



Данные Android приложения Viber



Данные Android приложения Threema



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

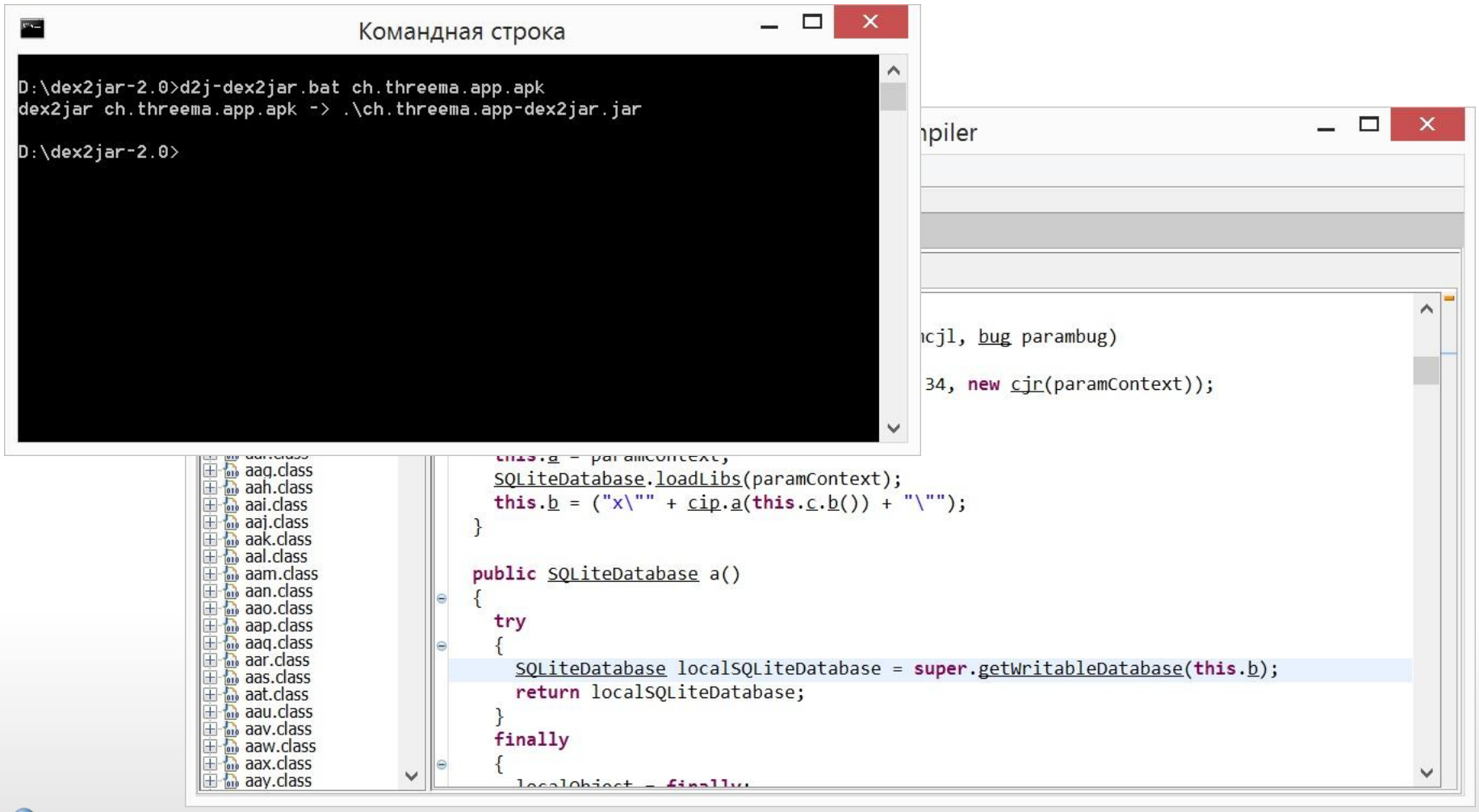
Изучение внутреннего устройства Android приложения

- Статический анализ:
  - 

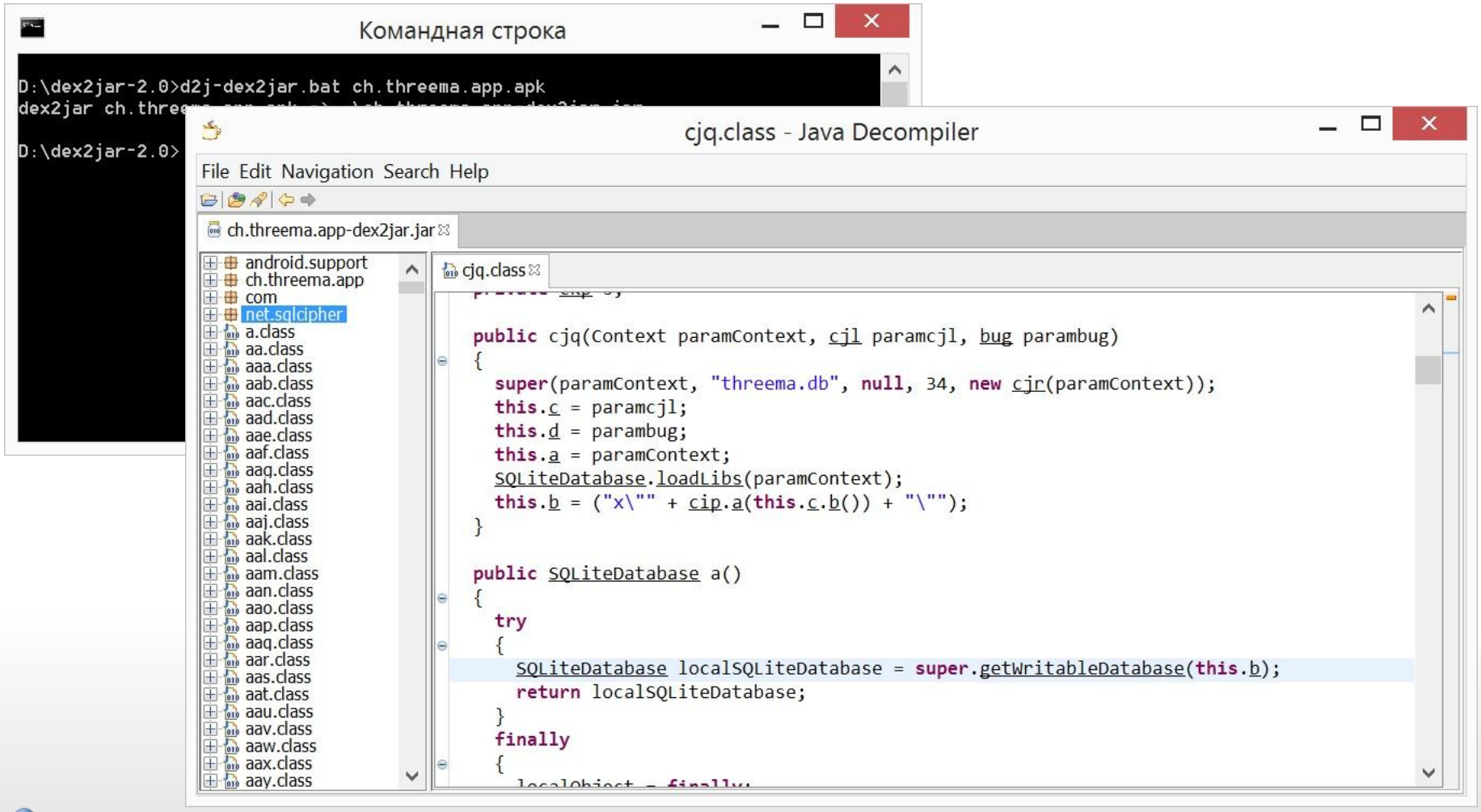
dex2jar + Java Decompiler
  - IDA Pro
- Динамический анализ:
  - IDA Pro Dalvik debugger
  - IDA Pro Remote ARM Linux/Android debugger
  - 

Xposed Modules

Изучение внутреннего устройства Android приложения Threema



Android приложение Threema dex2jar + Java Decompiler



Изучение внутреннего устройства Android приложения Threema

cjq.class - Java Decompiler

File Edit Navigation Search Help

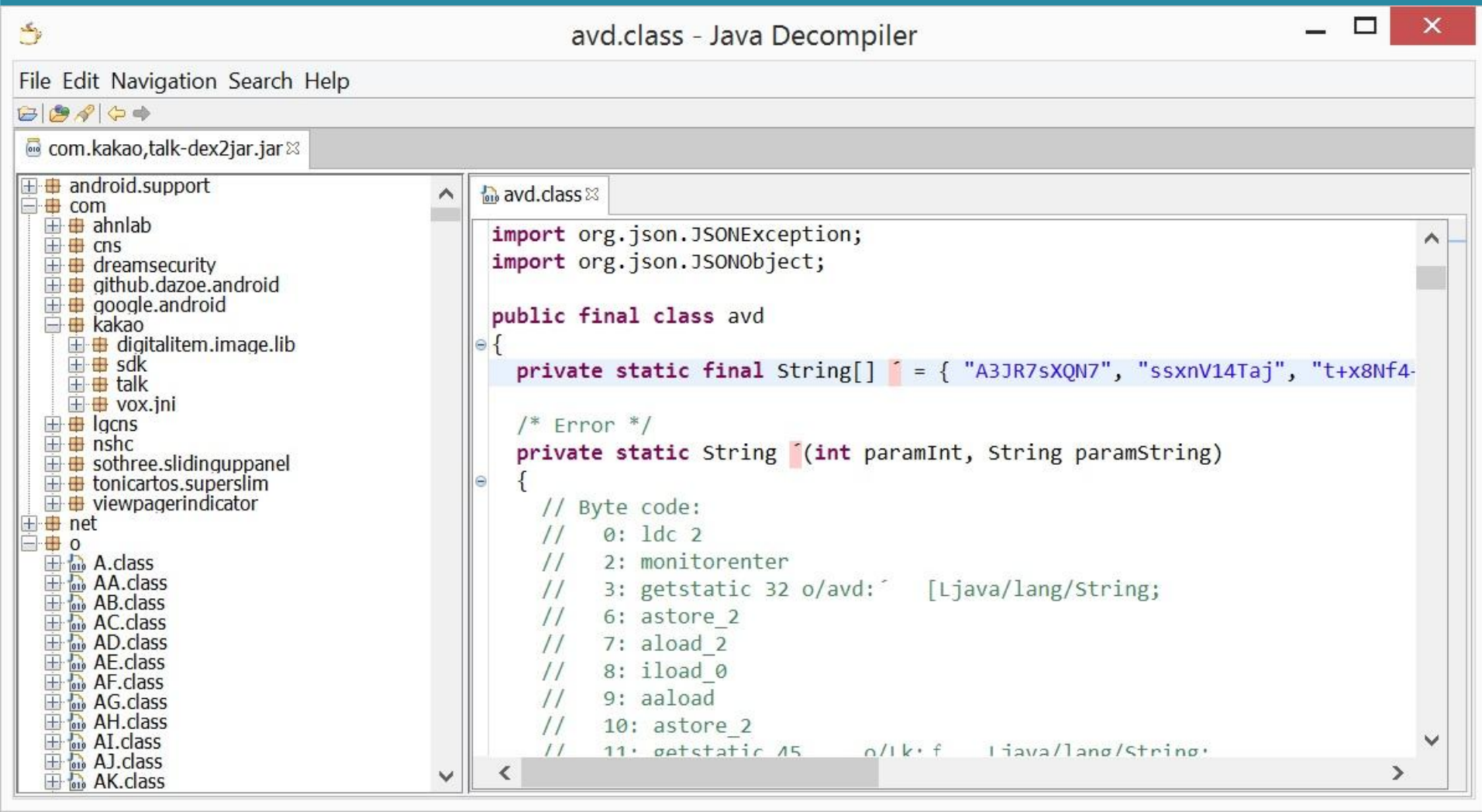
ch.threema.app-dex2jar.jar

- android.support
- ch.threema.app
- com
- net.sqlcipher
- a.class
- aa.class
- aaa.class
- aab.class
- aac.class
- aad.class
- aae.class
- aaf.class
- aag.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

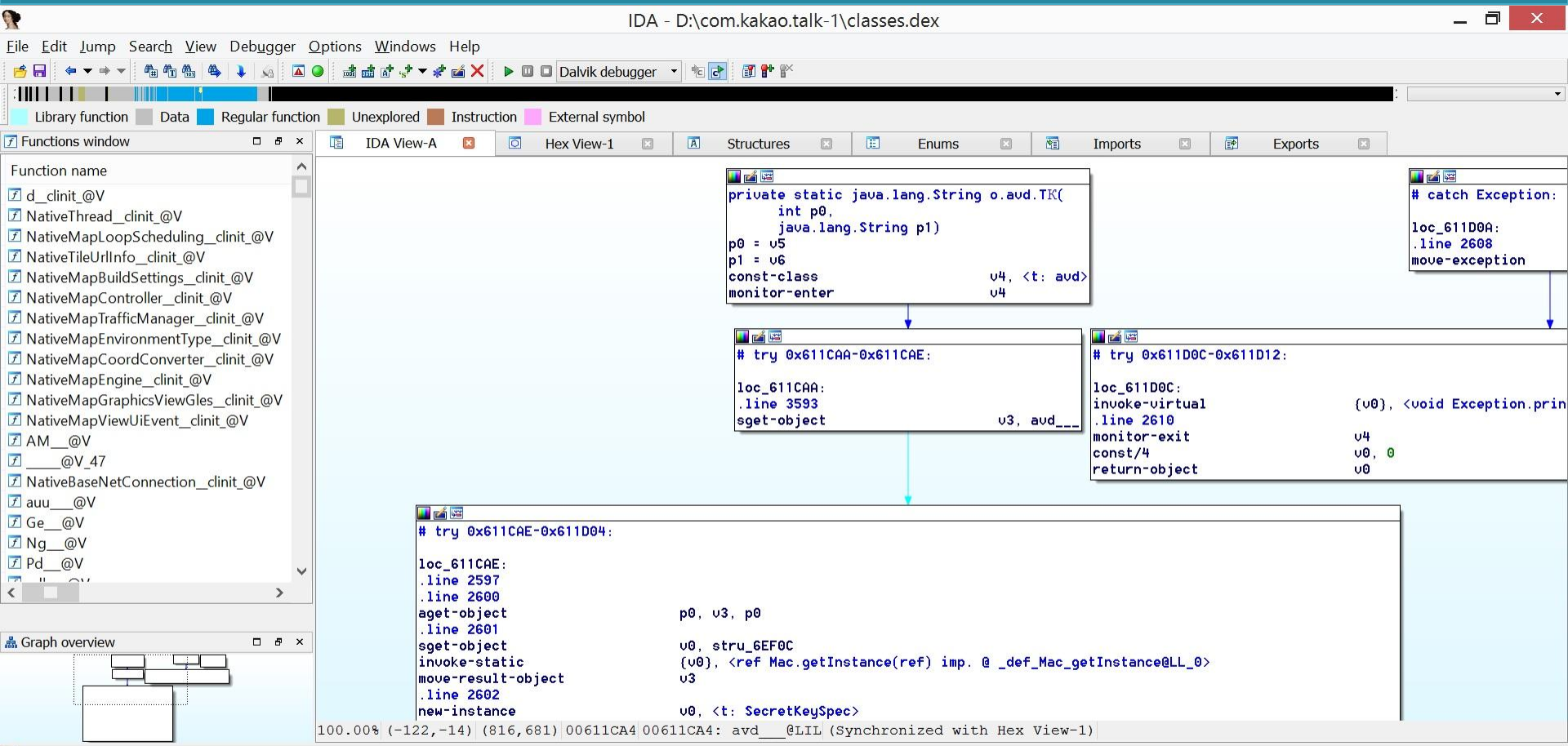
cjq.class

```
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
  {
```

Android приложения KakaoTalk dex2jar + Java Decompiler



Android приложение KakaoTalk
IDA Pro



Изучение внутреннего устройства Android приложения Threema

cjq.class - Java Decompiler

File Edit Navigation Search Help

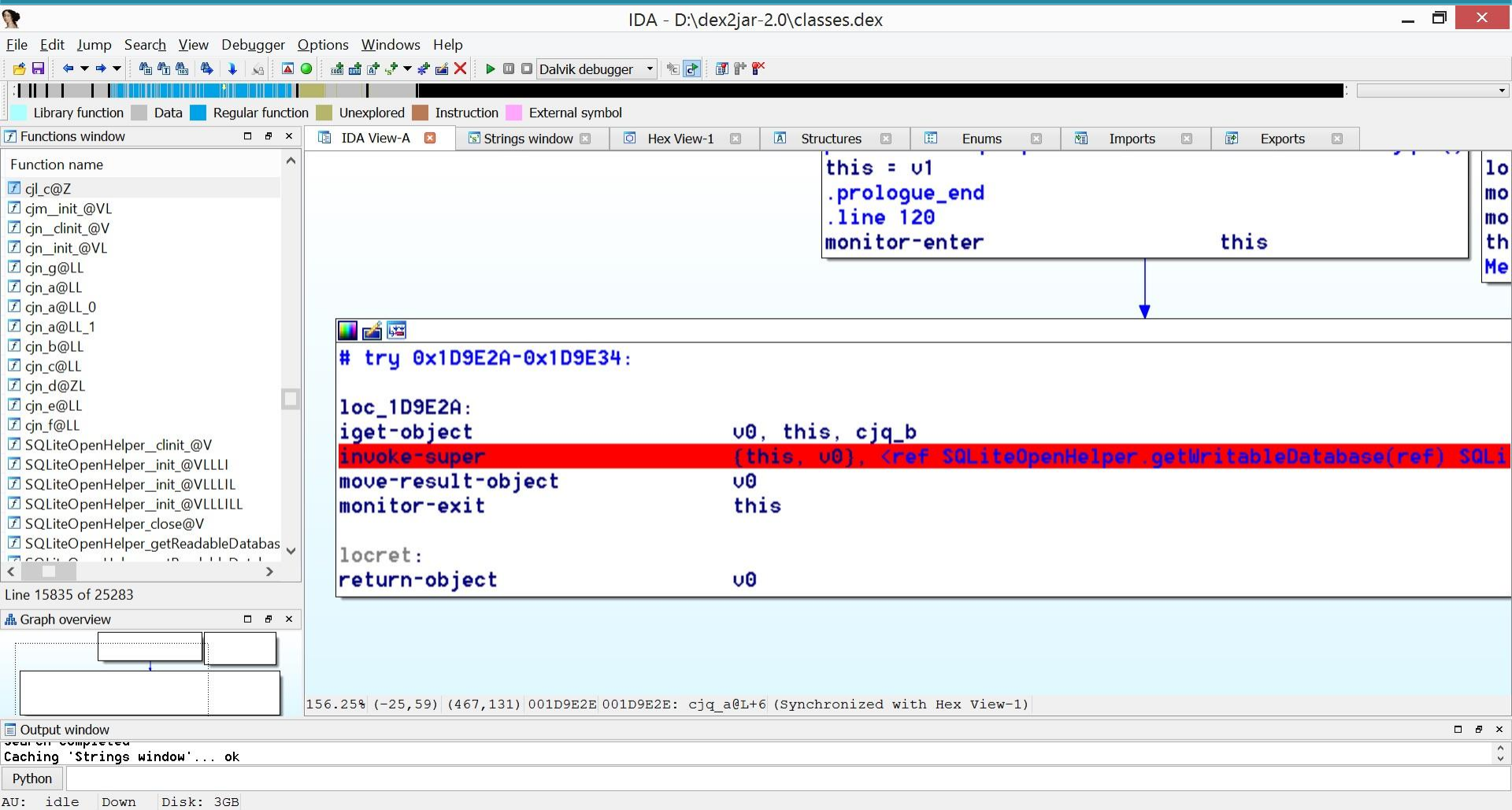
ch.threema.app-dex2jar.jar

- android.support
- ch.threema.app
- com
- net.sqlcipher
- a.class
- aa.class
- aaa.class
- aab.class
- aac.class
- aad.class
- aae.class
- aaf.class
- aag.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
  {
```

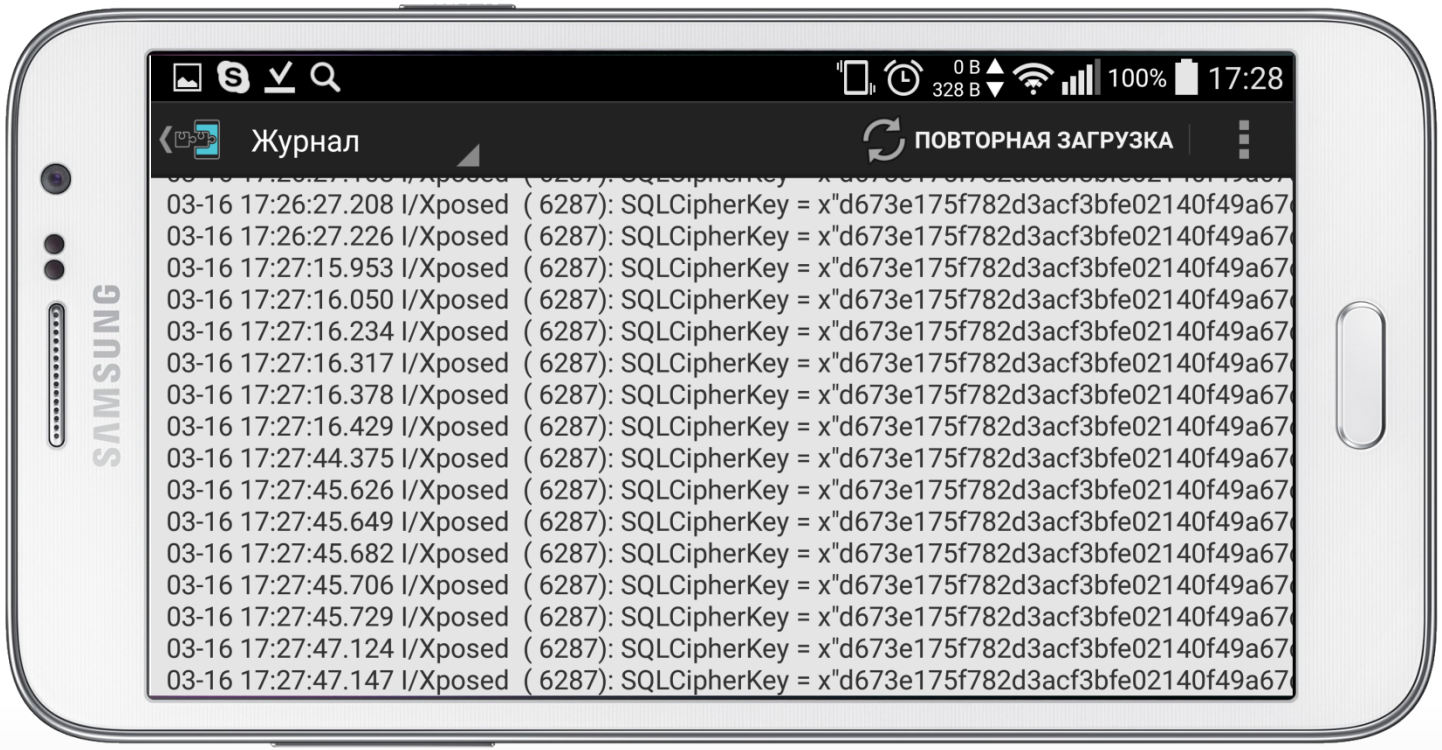
Android приложение Threema
IDA Pro Dalvik debugger



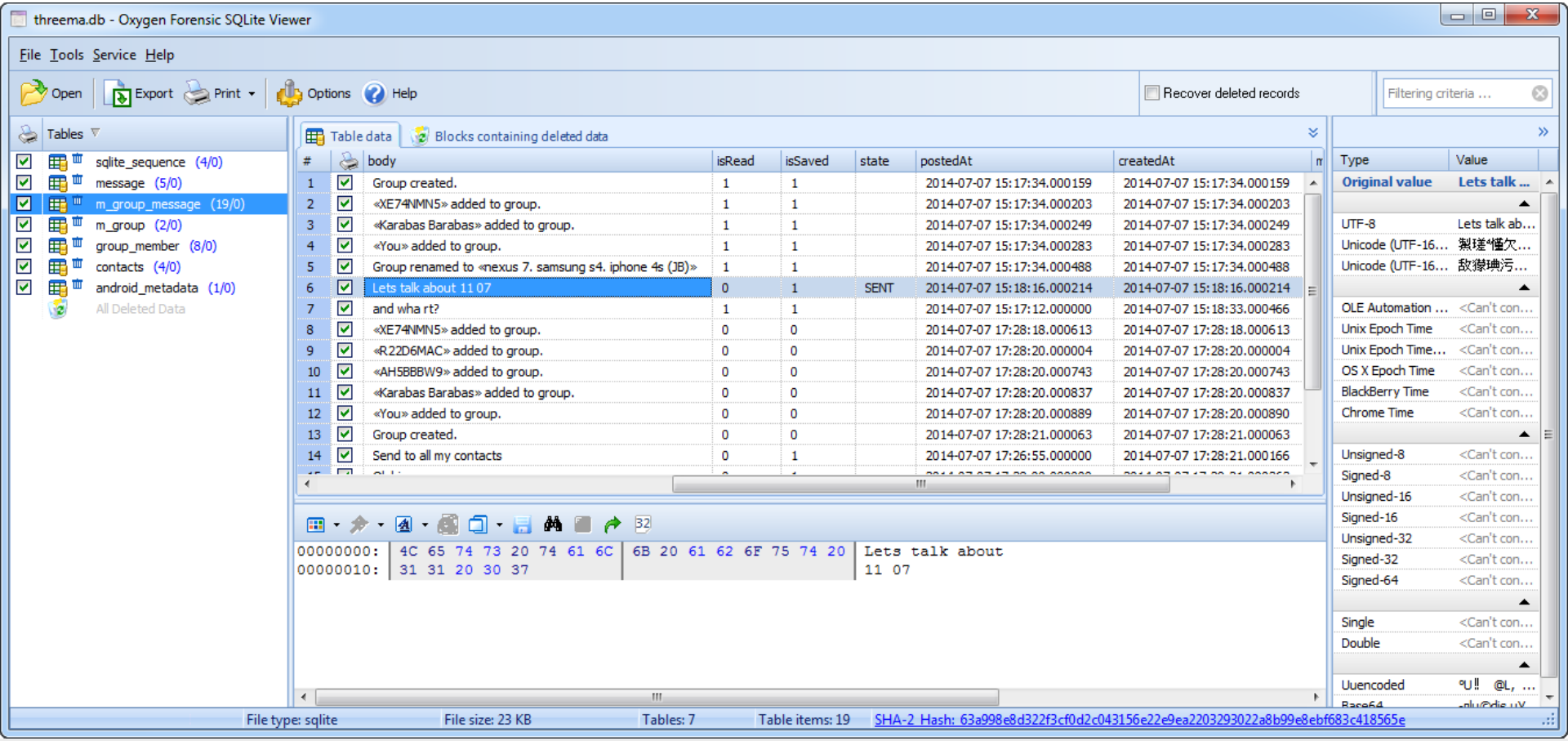
Android приложение Threema Xposed Modules

```
public class testhook implements IXposedHookLoadPackage  {

    public void handleLoadPackage(final LoadPackageParam lpparm) throws Throwable {

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

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

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

        findAndHookMethod(classToHook, lpparm.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



Изучение внутреннего устройства Android приложения Threema

cjq.class - Java Decompiler

File Edit Navigation Search Help

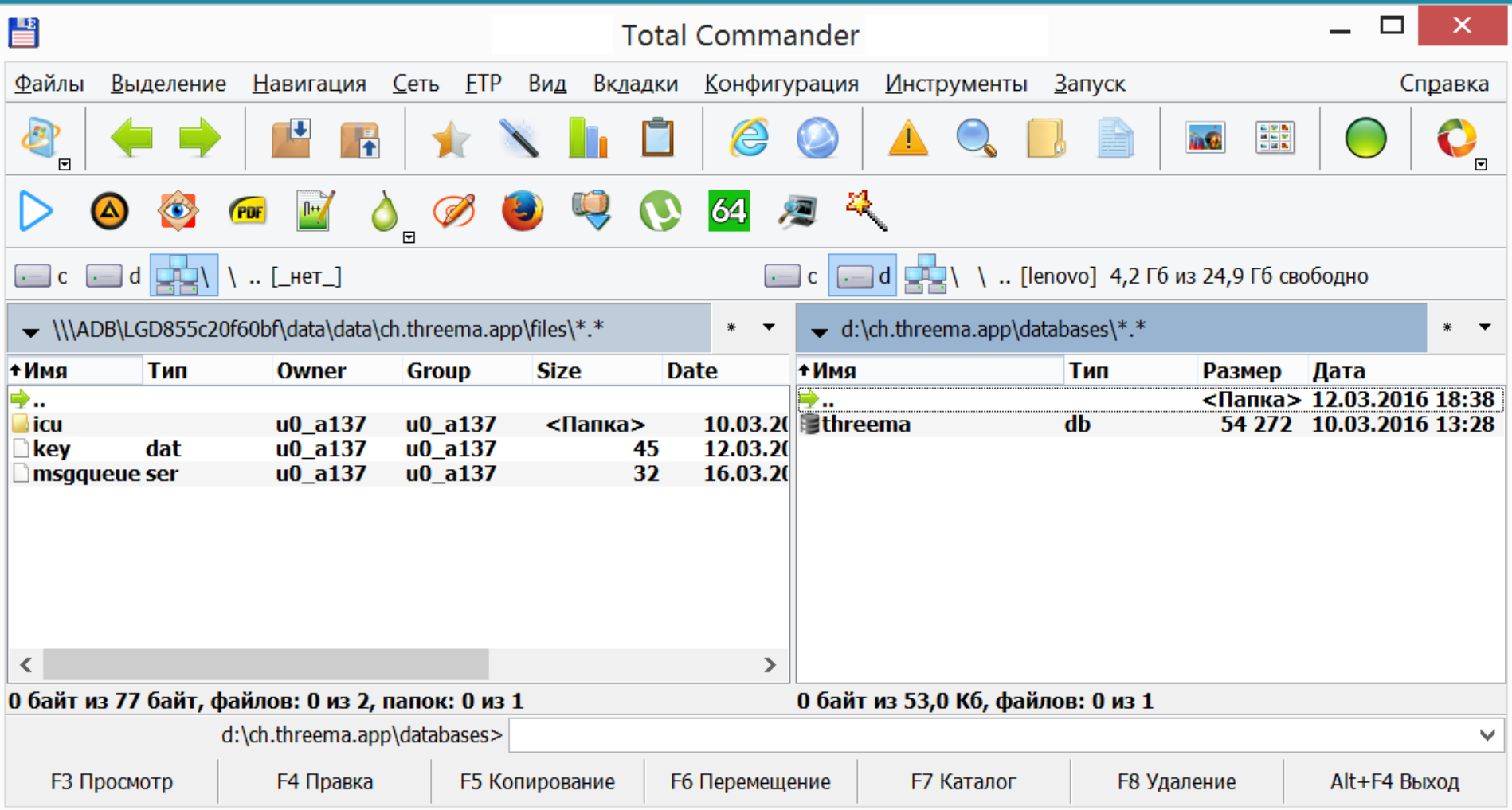
ch.threema.app-dex2jar.jar

- android.support
- ch.threema.app
- com
- net.sqlcipher
- a.class
- aa.class
- aaa.class
- aab.class
- aac.class
- aad.class
- aae.class
- aaf.class
- aag.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
  {
```

Изучение внутреннего устройства Android приложения Threema



Изучение внутреннего устройства Android приложения Threema

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

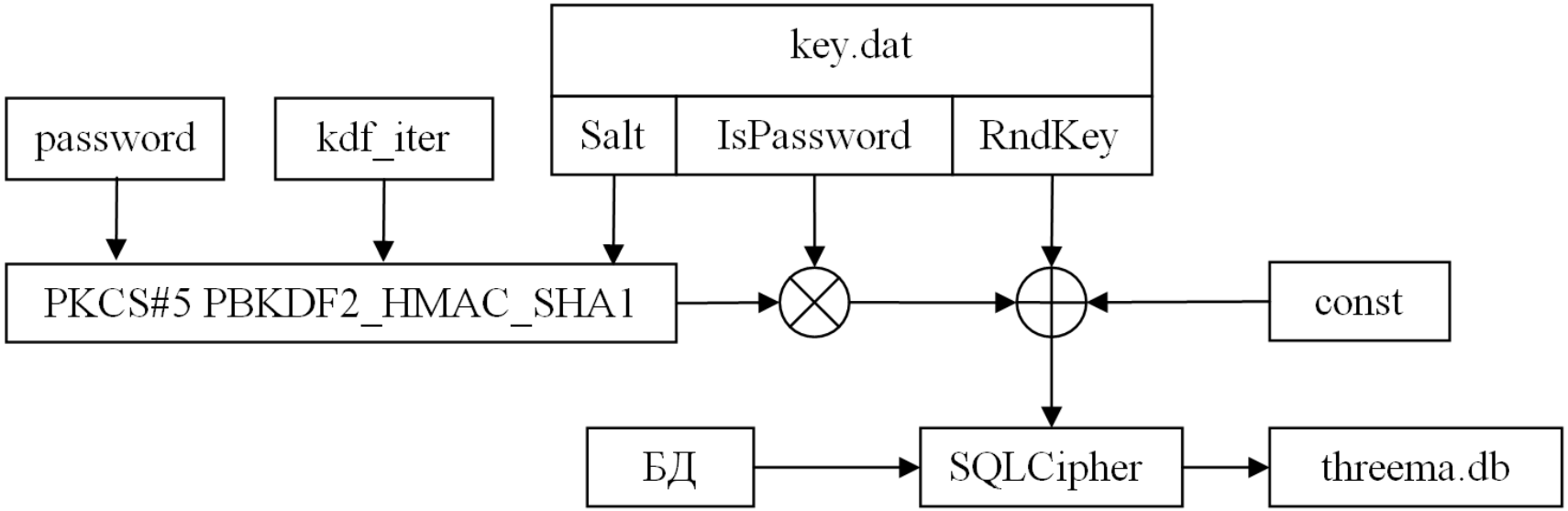
Файл Правка Поиск Вид Кодировки Синтаксисы Опции Макросы Запуск Плагины Окна ?

key.dat

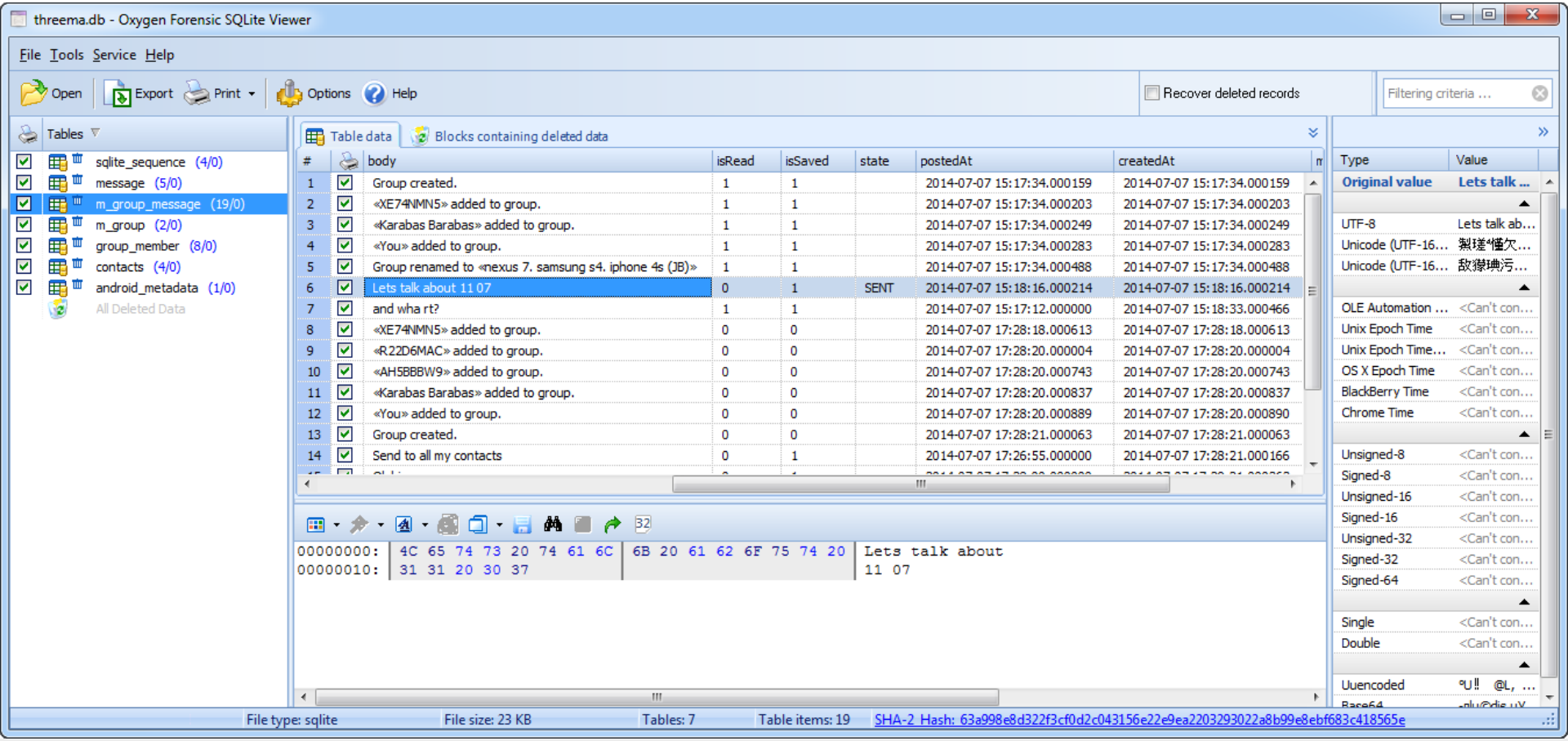
Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	00	43	7e	c7	0f	7f	68	a4	bc	6f	ef	07	1e	07	14	f3	.C~З..h¤joп....y
00000010	15	07	7f	7e	f1	cc	50	8d	16	5d	f2	b9	f1	61	84	d0	...~cMP..]т№ca„P
00000020	9c	0d	c9	63	6b	7b	f5	e1	90	2d	43	52	f9				њ.Йck{хб.-CRщ

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

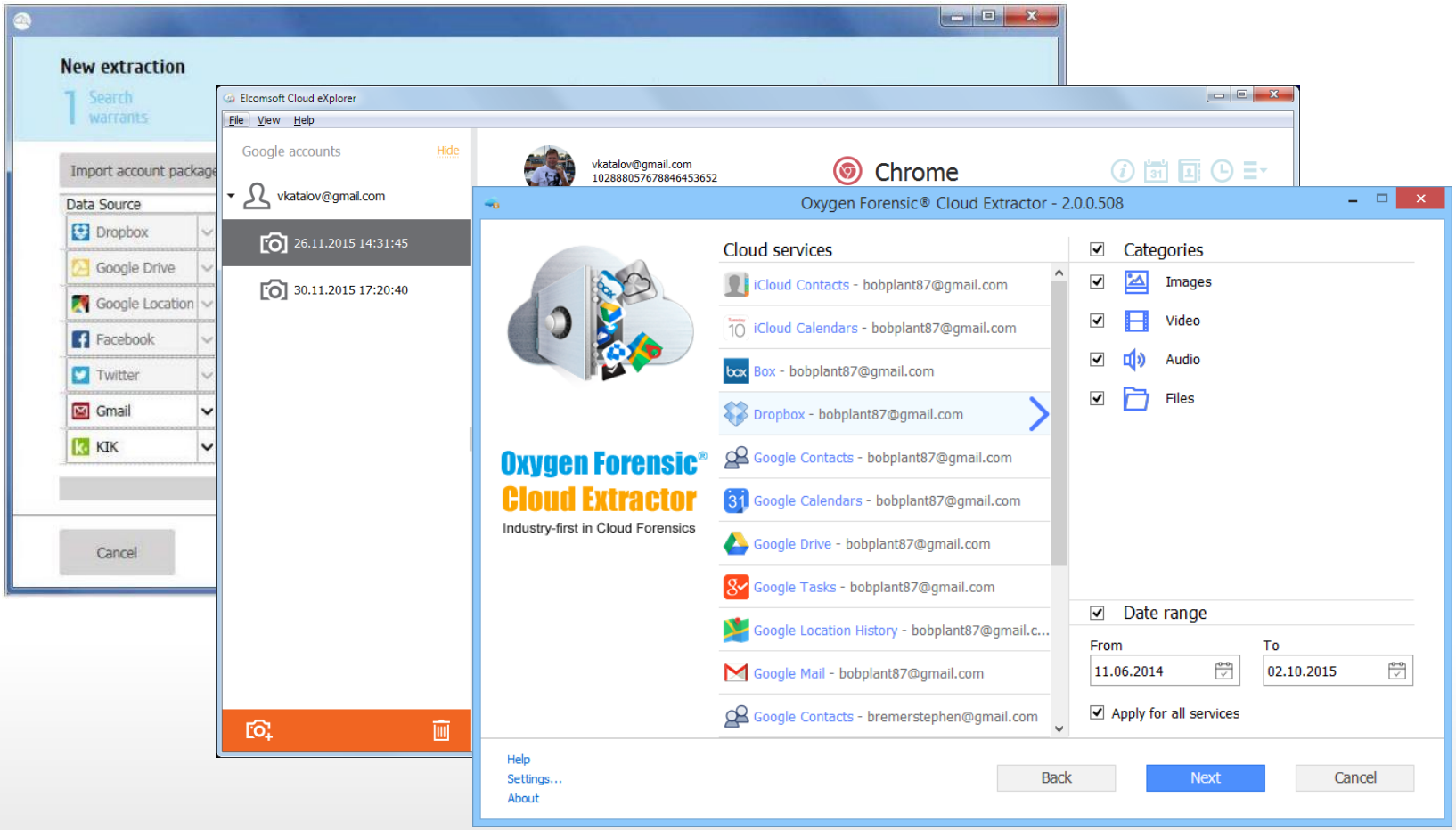
Изучение внутреннего устройства Android приложения Threema



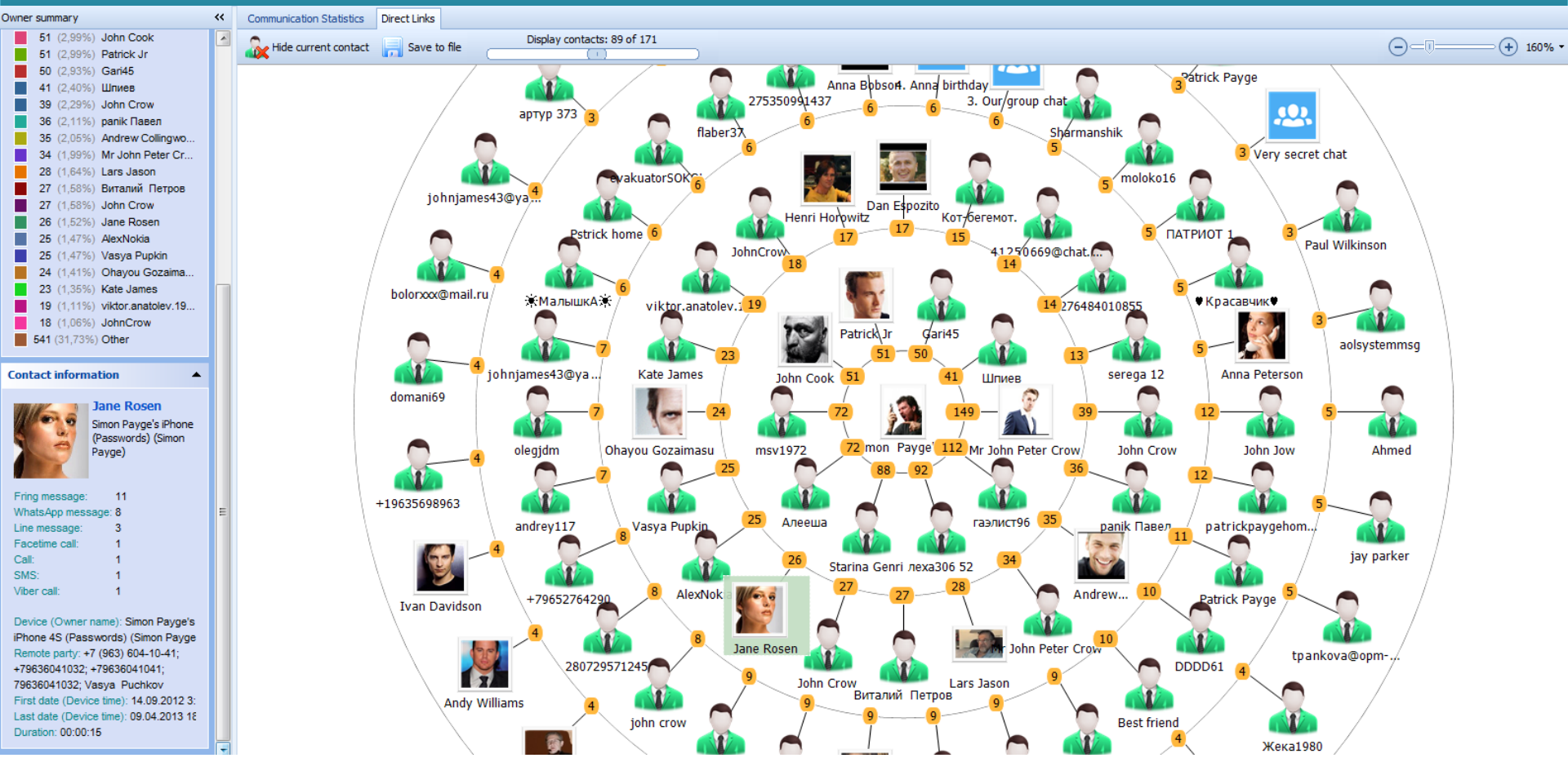
Изучение внутреннего устройства Android приложения Threema



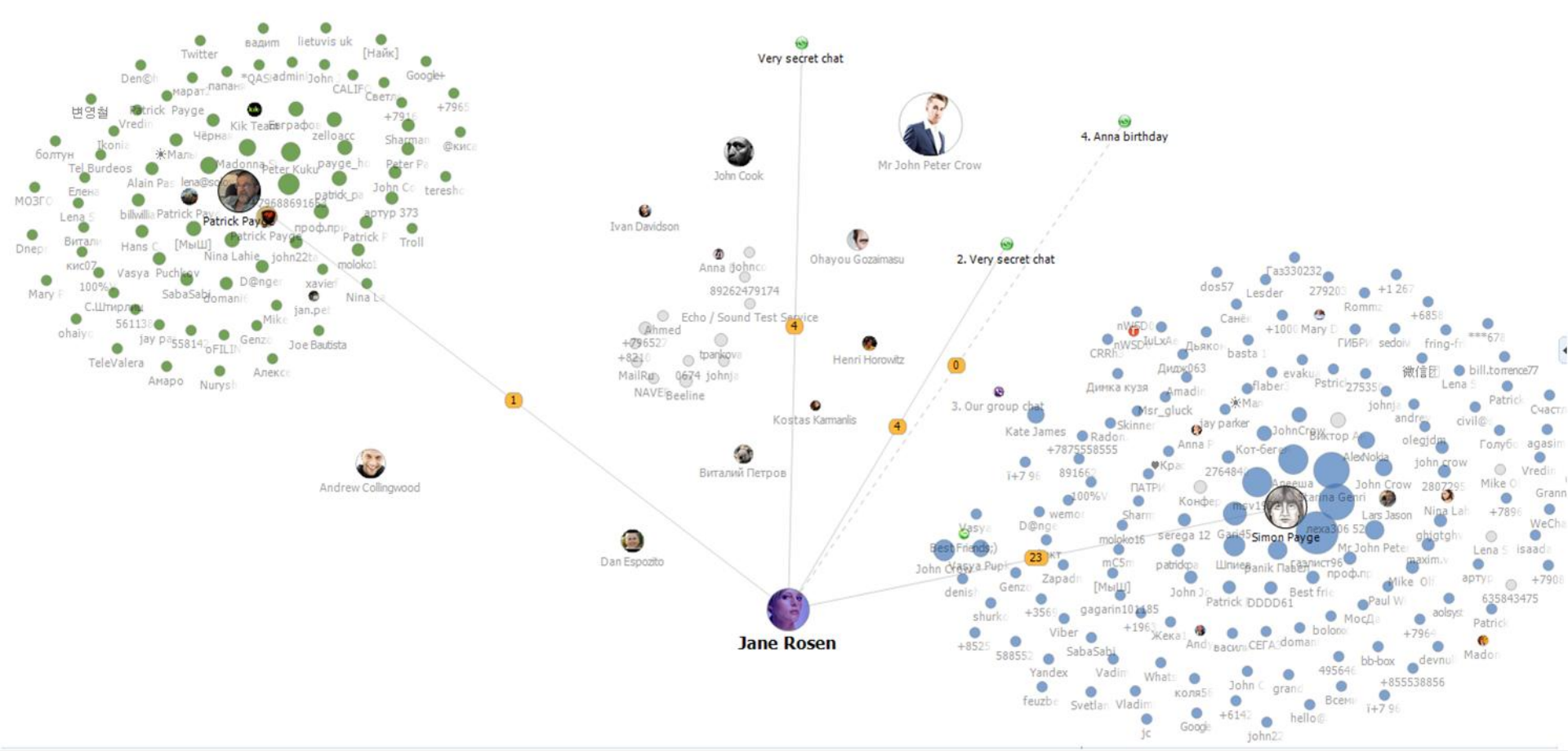
Извлечение данных из облачных хранилищ



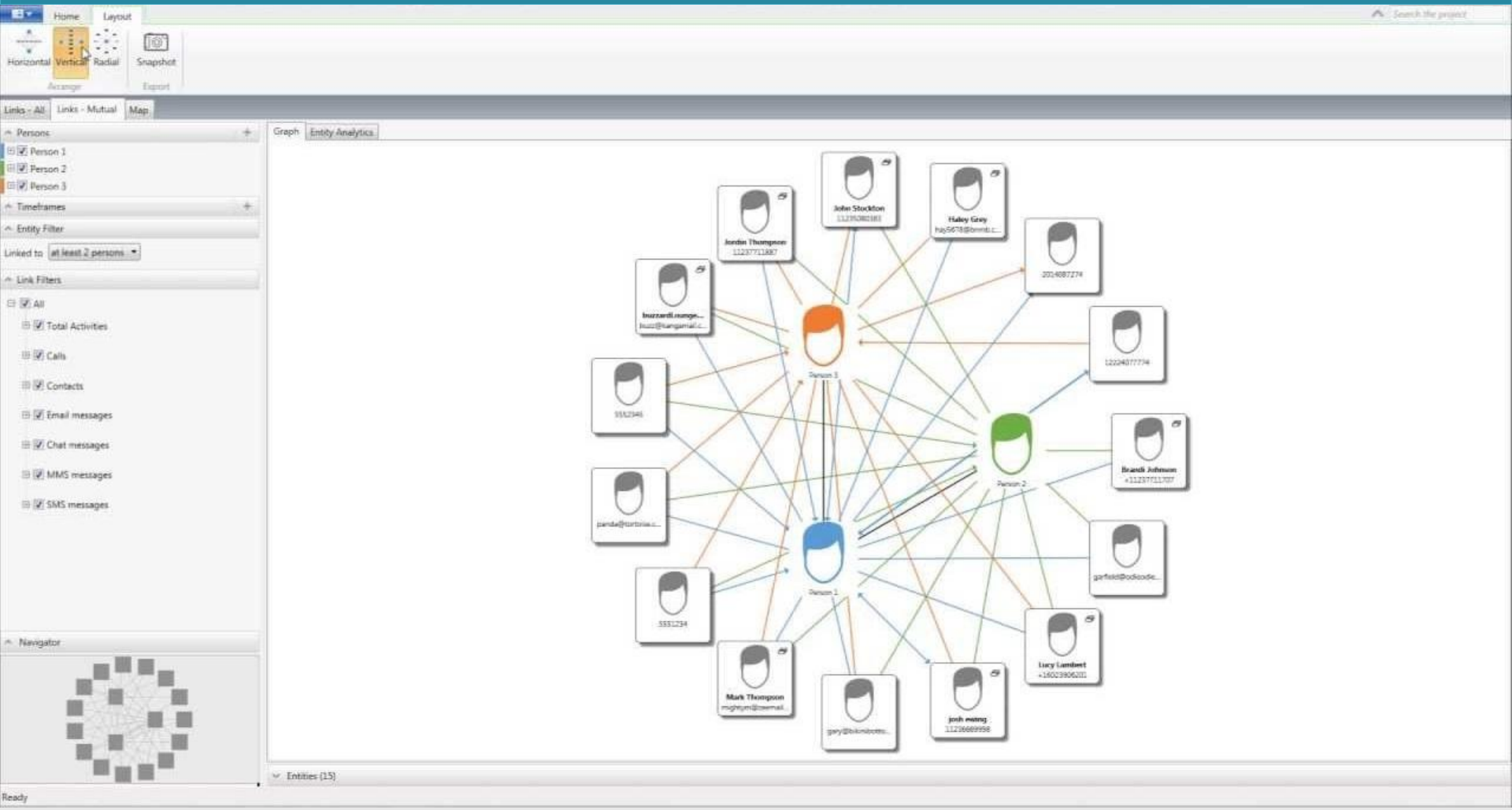
Агрегация данных из нескольких приложений



Агрегация данных из нескольких телефонов

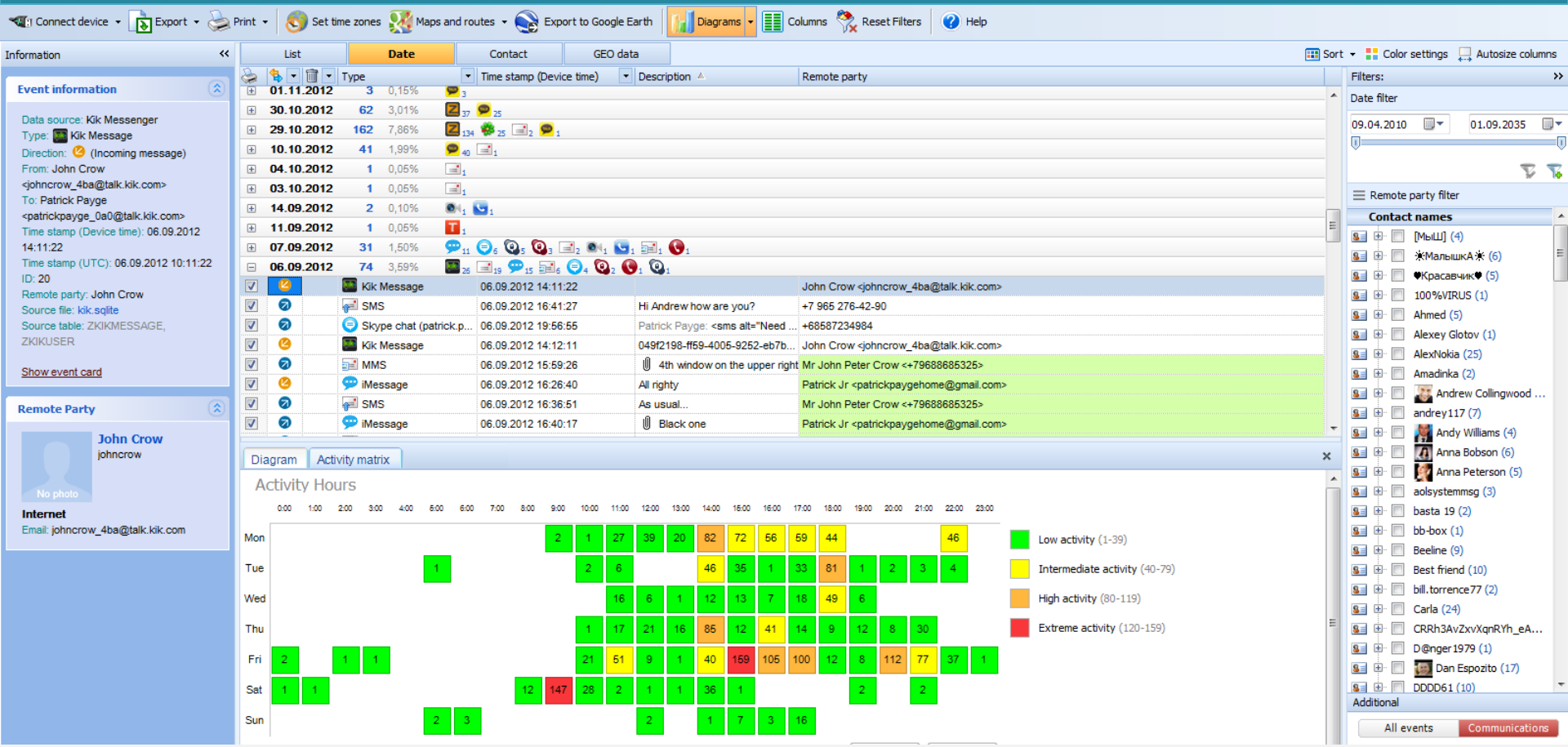


Агрегация данных из нескольких телефонов

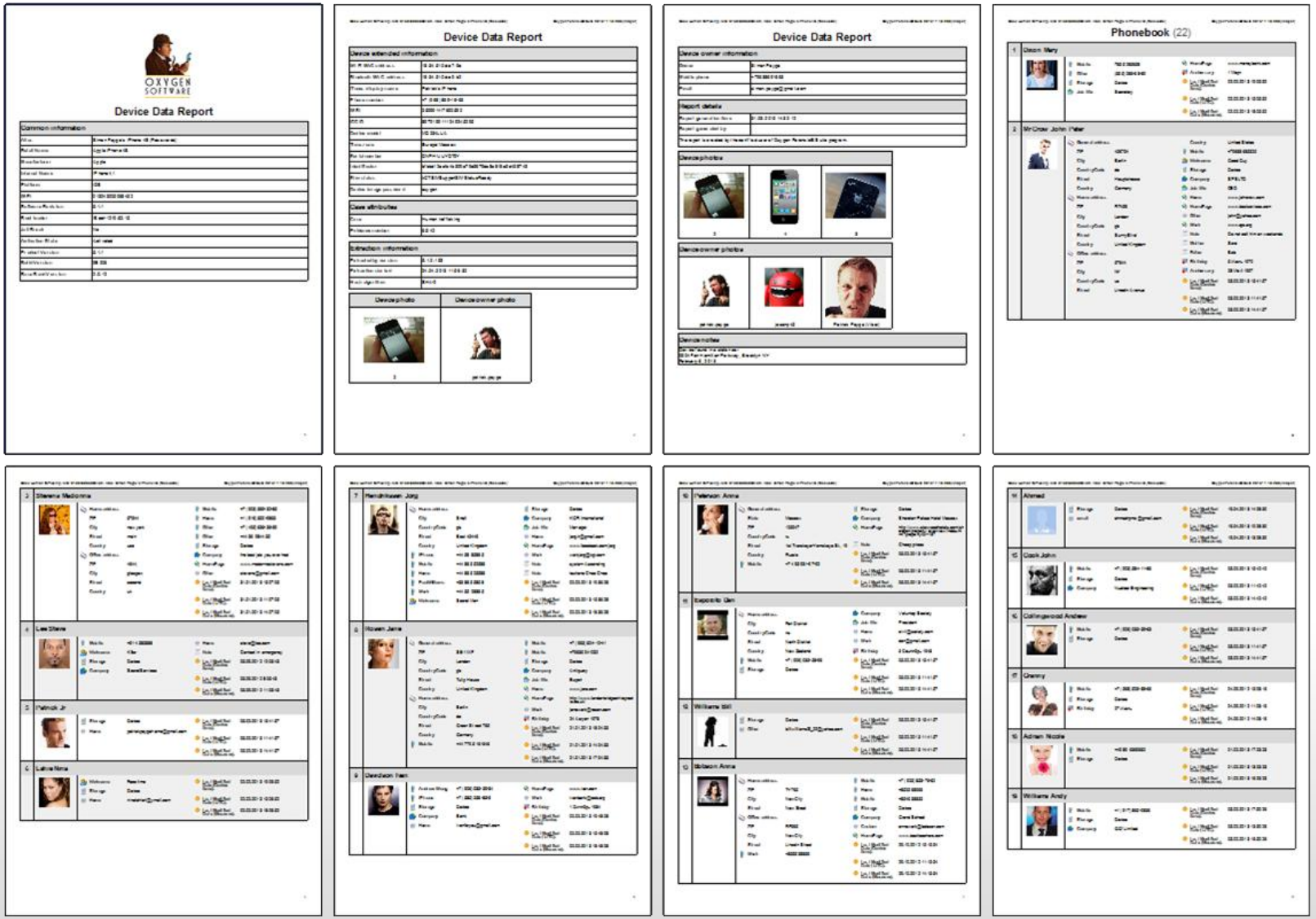


http://www.мобильный-криминалист.рф

Детализация определенного периода времени



Генерация отчета



Подводим итоги

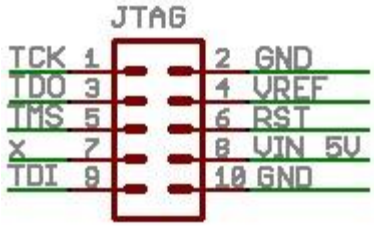
Основные этапы криминалистического анализа мобильного приложения

- 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!

OXYGEN SOFTWARE

http://www.мобильный-криминалист.рф

Вопросы???