Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

JEB Plugin 開発チュートリアル 第0回

一般社団法人JPCERTコーディネーションセンター

はじめに

- JEB Plugin開発チュートリアル
  - —Androidアプリ解析ツールJEBによる解析作業を効率化するために、APIを利用してPluginを自由に作成できるようになっていただくことが目的
  - —全4回のチュートリアル
  - —想定読者
    - JEBに興味がある人
    - Androidアプリについての知識がある人

JEBを用意し、実際に手を動かして例題を試しながら読み進めて欲しい

本チュートリアルはJEB v1.4.201311020を前提として作成した

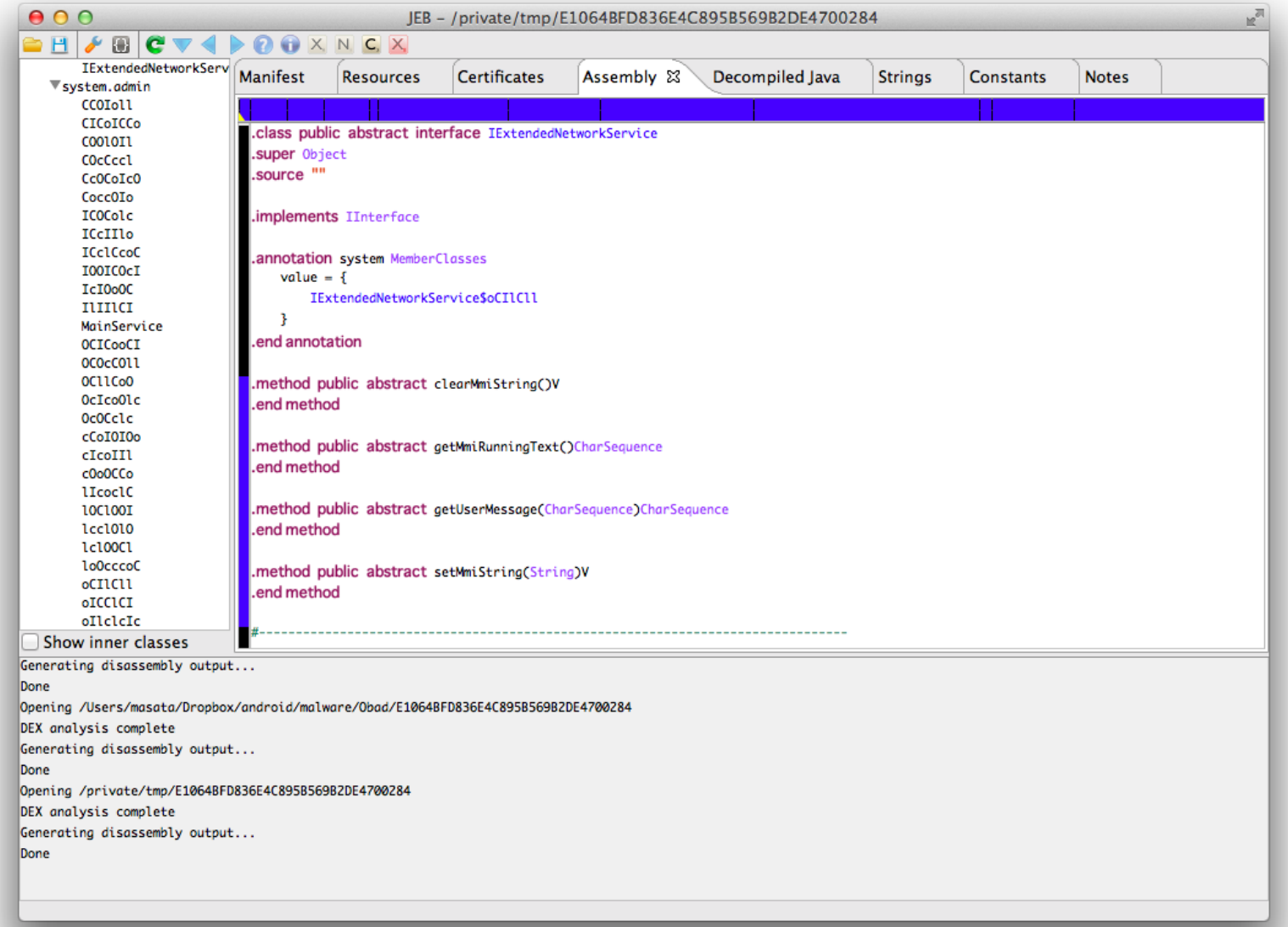
目次

- **第0回 JEBとは？**
- 第1回 JEB Pluginとは
  - 1. JEB Pluginの使い方
  - 2. JEB Pluginの構造
  - 3. JEBのUIを利用するためのAPI
  - 4. ViewとSignature
- 第2回 DEXファイルの構造を理解する
  - 1. DEXファイルの構造
  - 2. jeb.api.dex
  - 3. クロスリファレンス
- 第3回 バイトコードについての理解
  - 1. CodeItem
- 第4回 JEB PluginからASTを扱う

JEBとは？

- Androidアプリ解析ツール
  - —http://www.android-decompiler.com/
- マルチプラットフォーム
  - —Windows/Linux/Mac上で動作
- 主な機能
  - —デコンパイル機能
  - —リソースやAndroidManifestのデコード, エクスポート
  - —インタラクティブな操作
  - —解析結果の保存
  - —Pluginによるオートメーション

JEBの画面



JEBの主な機能-1

- DEXをJavaにデコンパイルできる

```
.method private postMailList()V
        .registers 27
        .prologue
00000000  invoke-virtual/range    GliveWallActivityActivity->getContentResolver()ContentResolver, v26 .. v26
00000006  move-result-object      v2
        .local v2, cr:Landroid/content/ContentResolver;
00000008  sget-object             v3, ContactsContract$Data->CONTENT_URI:Uri
0000000C  const/4                 v4, 0x0
0000000E  const-string            v5, "mimetype = ?"
00000012  const/4                 v6, 0x1
00000014  new-array               v6, v6, [String
00000018  const/4                 v7, 0x0
0000001A  const-string            v25, "vnd.android.cursor.item/email_v2"
0000001E  aput-object             v25, v6, v7
00000022  const/4                 v7, 0x0
00000024  invoke-virtual/range    ContentResolver->query(Uri, [String, String, [String, String)Cursor, v2 .. v7
0000002A  move-result-object      v10
        .local v10, dataAddressTable:Landroid/database/Cursor;
0000002C  const-string            v3, "xxx"
00000030  const-string            v4, "start"
```

```
private void postMailList() {
    Cursor v10 = this.getContentResolver().query(ContactsContract$Data.CONTENT_URI, null, "mimetype = ?", new String
            []{"vnd.android.cursor.item/email_v2"}, null);
    Log.d("xxx", "start");
    String v24;
    for(v24 = ""; v10.moveToNext(); v24 = String.valueOf(v24) + v10.getString(v10.getColumnIndex("data1")) + "," + v10
            .getString(v10.getColumnIndex("display_name")) + "\n") {
        Log.d("xxx", v10.getString(v10.getColumnIndex("data1")));
    }

    v10.close();
```

JEBの主な機能-2

- インタラクティブな操作で効率的な解析が可能
- 便利な機能
  - —クロスリファレンス
    - クラス、メソッドの呼び出し箇所/定義箇所へのジャンプ
  - —リネーム
    - クラス、メソッド、変数のリネーム → 可読性の向上
  - —コメント追加機能
    - コード内にコメントを追加して解析結果を記録

参考: JEB の入手

- 本家から購入する
  - —http://www.android-decompiler.com/
  - —1ライセンス 1,000 US$
  - —Paypal か海外送金
- 日本の販売代理店から購入する
  - —http://www.securebrain.co.jp/products/jeb/index.html
  - —要お見積もり