Hello, I'm VM, Dalvik VM!

Dainius Jocas

May 1, 2013

Table of contents

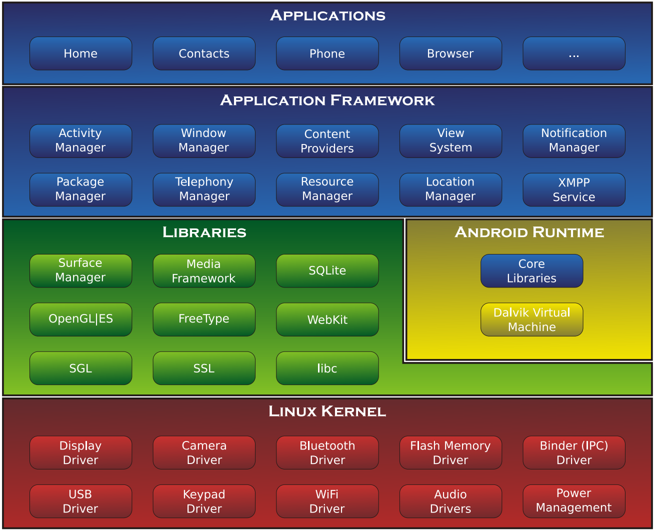
Introduction

On the way to investigate Source Code

What is a VM?

A virtual machine (VM) is a software implemented abstraction of the underlying hardware, which is presented to the application layer of the system.

Dalvik and Android



APPLICATIONS

Home

Contacts

Phone

Browser

...

APPLICATION FRAMEWORK

Activity Manager

Window Manager

Content Providers

View System

Notification Manager

Package Manager

Telephony Manager

Resource Manager

Location Manager

XMPP Service

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

Bluetooth Driver

Flash Memory Driver

Binder (IPC) Driver

USB Driver

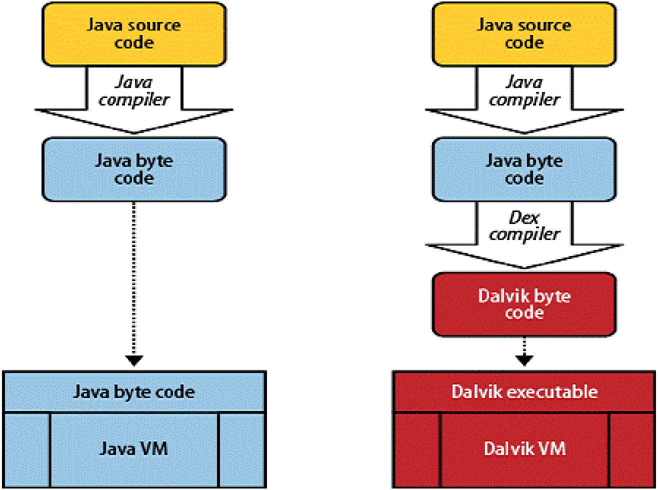
Keypad Driver

WiFi Driver

Audio Drivers

Power Management

Some picture



Dalvik VM

Definition: The Dalvik Virtual Machine is the heart of Android. It's a fast, just-in-time compiled, optimized bytecode virtual machine. Android applications are compiled to Dalvik bytecode and run on the Dalvik VM.

What it means:

- fast?
- just-in-time compiled?
- optimized bytecode?

Speed

- .dex files are smaller in size compared to .jar files.
- Dalvik is a register based VM.
- .dex produced in that way, that they have a more dense encoding.

Just-in-time compilation

- Just-in-time (JIT) compilation, also known as a dynamic translation, is a technique for improving the runtime performance of computer program based on byte code.
- Translation of interpretable bytecode into an executable machine code.
- Because Dalvik is register based VM, JIT compiler is simpler.

Optimizations on bytecode

- Constant pool references are replaced with pointers to internal data structures
- inlining of methods
- prune empty methods
- append pre-computed data
- ...

Dalvik instructions

- 01 12x MOVE vA, vB
- 16-bit instruction set.
- 226 instructions (during the optimization step new opcodes may appear).
- When used for bit values (such as integers and floating point numbers), registers are considered 32 bits wide. Adjacent register pairs are used for 64-bit values.

Android source code. Numbers

- Whole Android project: 279,843 items, totalling 7.0 GB
- Dalvik VM: 4,142 items, totalling 29.6 MB
- Dalvik VM is implemented in C, C++, Assembly, and Java

Dalvik's Toolkit

- dx – the tool that takes in class files and reformulates them for consumption in the Dalvik VM.
- dexopt – performs an abbreviated VM initialization, loads zero or more DEX files from the bootstrap class path, and then sets about verifying and optimizing whatever it can from the target DEX.
- dexdump – tool is intended to mimic "objdump" - program for displaying various information about object files.
- dexdeps – DEX external dependency dump
- ...