Android Programming and Security

Dependable and Secure Systems

Andrea Saracino

andrea.saracino@iet.unipi.it

Outlook (1)

- The Android Open Source Project
  - Philosophy

Outlook (2)

- Part I: Android System and Applications
  - Android Framework

  - Android Applications
  - Google Play

Outlook (3)

- Part II: Android Security
  - Native Mechanisms
  - Attacks
  - Innovative Solutions

Part I

- Android System and Applications

The Android Open Source Project (AOSP)

- What is Android?
  - A mobile OS? **No**
  - A framework for mobile devices **Maybe**
- Android is an **Open Source** Project held by the Open Handset Alliance.

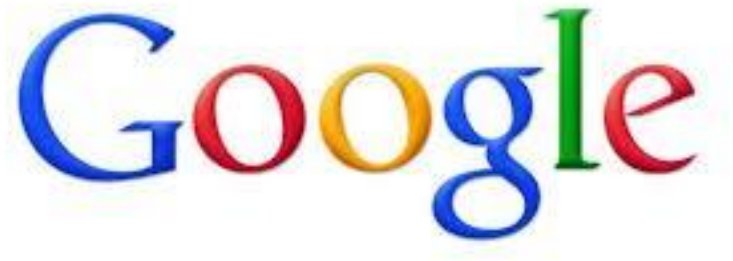
Open Handset Alliance

- Consortium of Enterprises that work in the field of mobile communications.
  - Service Provider
  - Hardware Manifacturer
  - Smartphone Producer
  - Software developer
  - …

GARMIN
FIH
DELL
ASUS
Rock Solid · Heart Touching
ALCATEL mobile phones
acer
MOTOROLA
LG
lenovo 联想移动
KYOCERA
HUAWEI
htc smart mobility
ZTE中兴
TOSHIBA
Sony Ericsson
SHARP
SAMSUNG
NEC
NUANCE
myriad
Living Image
Google
ebY
Ascender Corporation
VisualOn
SVOX
SONiVOX sound that rocks.
skypop.
pv
OMRON
tat
embinux
sasken
noser
BORQS
Aplix Corporation
中国电信 CHINA TELECOM
中国移动通信 CHINA MOBILE
Bouygues Telecom
WIPRO Applying Thought
WIND RIVER
TELECA
T··Mobile·
Sprint
SoftBank
NTT docomo
Designing The Future KDDI
China unicom 中国联通
ARM
Audience
AKM
vodafone
Telefonica
TELECOM ITALIA
gemalto security to be free
freescale semiconductor
CYPRESS PERFORM
csr
BROADCOM.
ATHEROS
RENESAS Renesas Electronics
QUALCOMM
NVIDIA.
MIPS TECHNOLOGIES
MARVELL
intel
Ascender Corporation
VIA Telecom
TEXAS INSTRUMENTS
Synaptics
ST ERICSSON
NXP SOFTWARE
L&T Infotech
MOTOYA
Audience
MEDIATE
CCI

Open Handset Alliance

- The Open Handset Alliance is led by one company:



Android Philosophy

- Open Source:
  - All of Android source code is available and can be downloaded and modified.
  - Improvement can be uploaded as system patches.
  - Patches pass through a long review process.

Android Devices

- Android has been designed for three type of devices:
  - Smartphones
  - Tablets
  - Embedded Systems.

Versions and Distributions

- **Apple Pie** (Android 1.0) Developed for HTC Dream.
- **Cupcake** (Android 1.5) Several Graphic improvements.
- **Donut** and **Eclair**(Android 1.6 – 2.1).
- **Froyo**(Android 2.2) First version with a large distribution.
- **Gingerbread** (Android 2.3 – 2.6) Installed on several smartphone in particular: Samsung Galaxy, Galaxy S and Galaxy S2.
- **Honeycomb** (Android 3.0) Distribution for tablets only.
- **Ice Cream Sandwich** (Android 4.0) For tablets and smartphone. Large distribution, used on Samsung Galaxy Nexus.
- **Jelly Bean** (Android 4.1 – 4.2) The latest release for smartphone and tablets.

Android Full Code

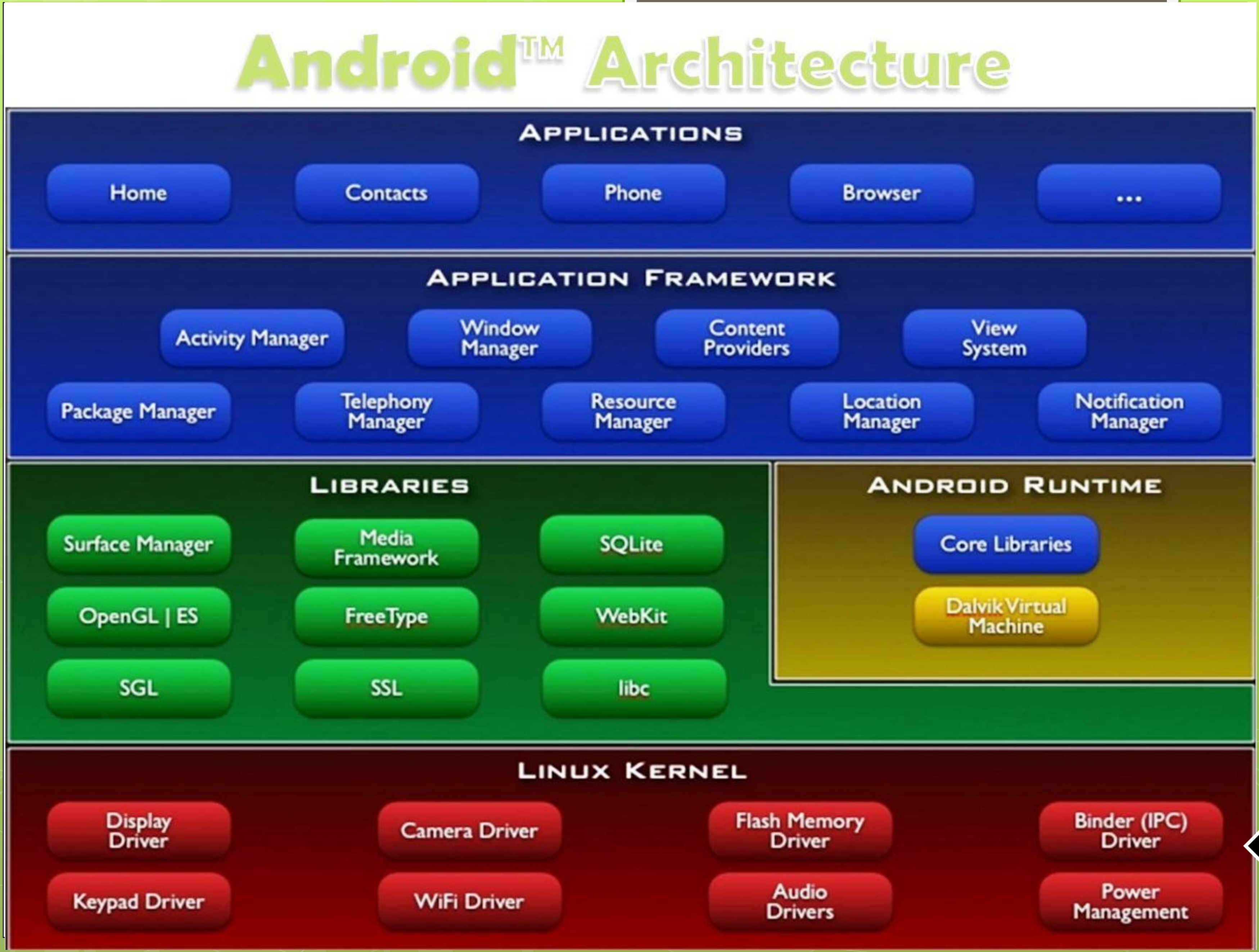
- The full code of Android is available at www.source.android.com as a **git** repository.
- Requires more than 10 GBs of mass storage and a swap of 20 GBs to be compiled.
- *Note: The source download is approximately 8.5GB in size. You will need over 30GB free to complete a single build, and up to 100GB (or more) for a full set of builds.*
- There is a version for smartphone (Maguro), one for Emulator (Goldfish) and one for embedded devices (Panda).

ROMs (1)

- The ROM is an Android Image (few MBs) of the OS that is installed on a device.
- Manufacturers ROM
  - Smartphone manufacturers equip their devices with custom ROMs.
  - Inclusion of manufacturer software (Samsung Kies…)
  - Some limitations on functionalities (Tethering).

ROMs (2)

- Custom ROM
  - ROMs modified by third party developers.
  - Inclusion of additional features.
  - No limitations on functionalities.
- Original ROMs
  - Installed on **Nexus** devices, which are devices produced by manufacturer under the guidance of Google.



Android™ Architecture

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

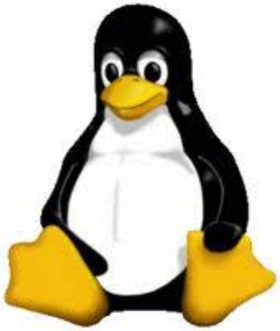
- Core Libraries
- Dalvik Virtual Machine

Linux Kernel

- Display Driver
- Camera Driver
- Flash Memory Driver
- Binder (IPC) Driver
- Keypad Driver
- WiFi Driver
- Audio Drivers
- Power Management

Kernel(1)

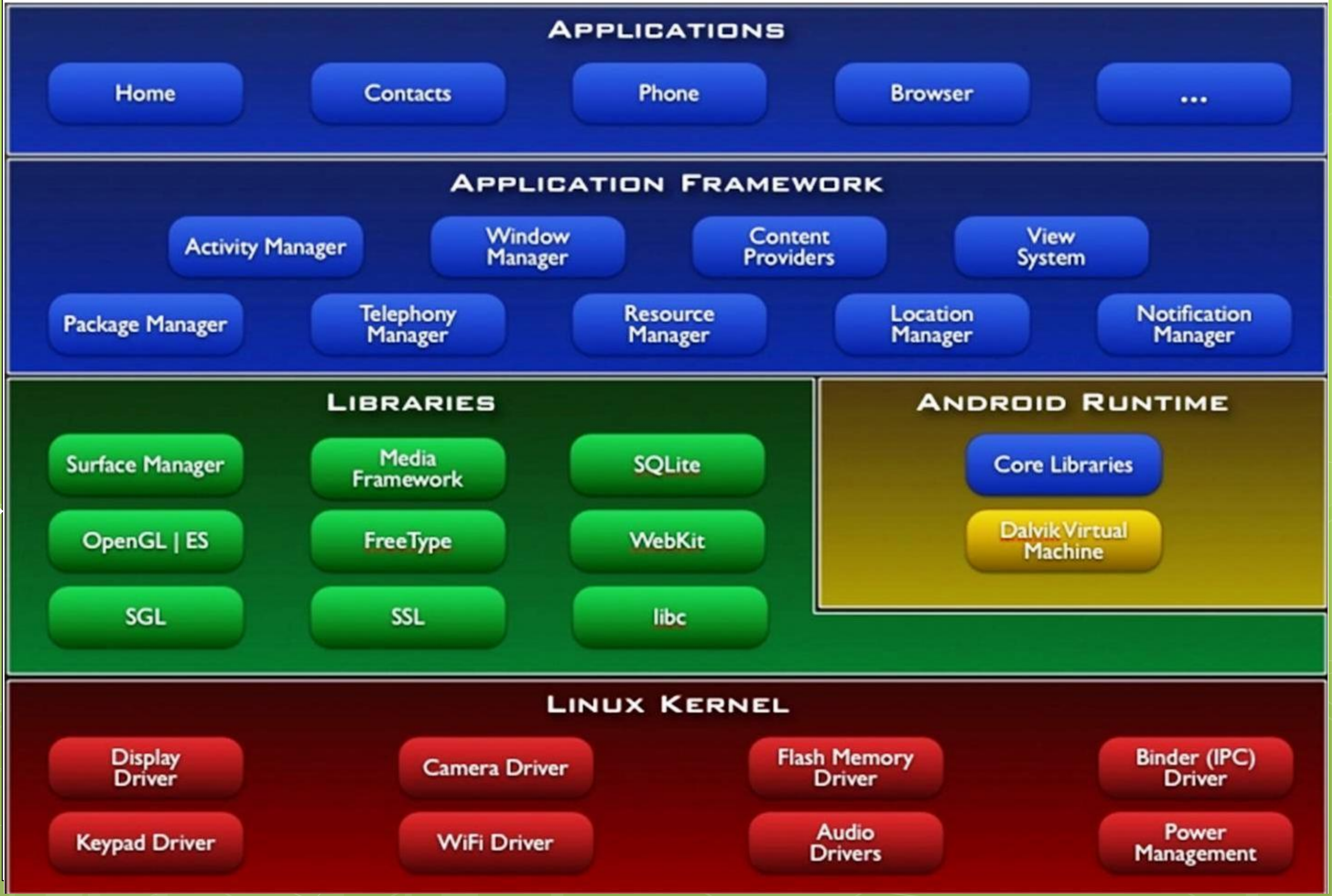
- The Android framework runs on top of a Linux Kernel.
  - Shell available.
  - Some commands are not available.
  - Some modules are not compiled.
  - In particular it is not possible:
    - To copy a file.
    - To create or modify users.
    - Become Super-User.



Kernel(2)

- Kernel Tasks:
  - Handles Inter Process Communication (IPC).
    - Processes cannot communicate directly.
  - Handles Inter Component Communication (ICC).
    - Hardware and Connection Interfaces.
  - Executes all of the low-level tasks.
  - Enforces Security.

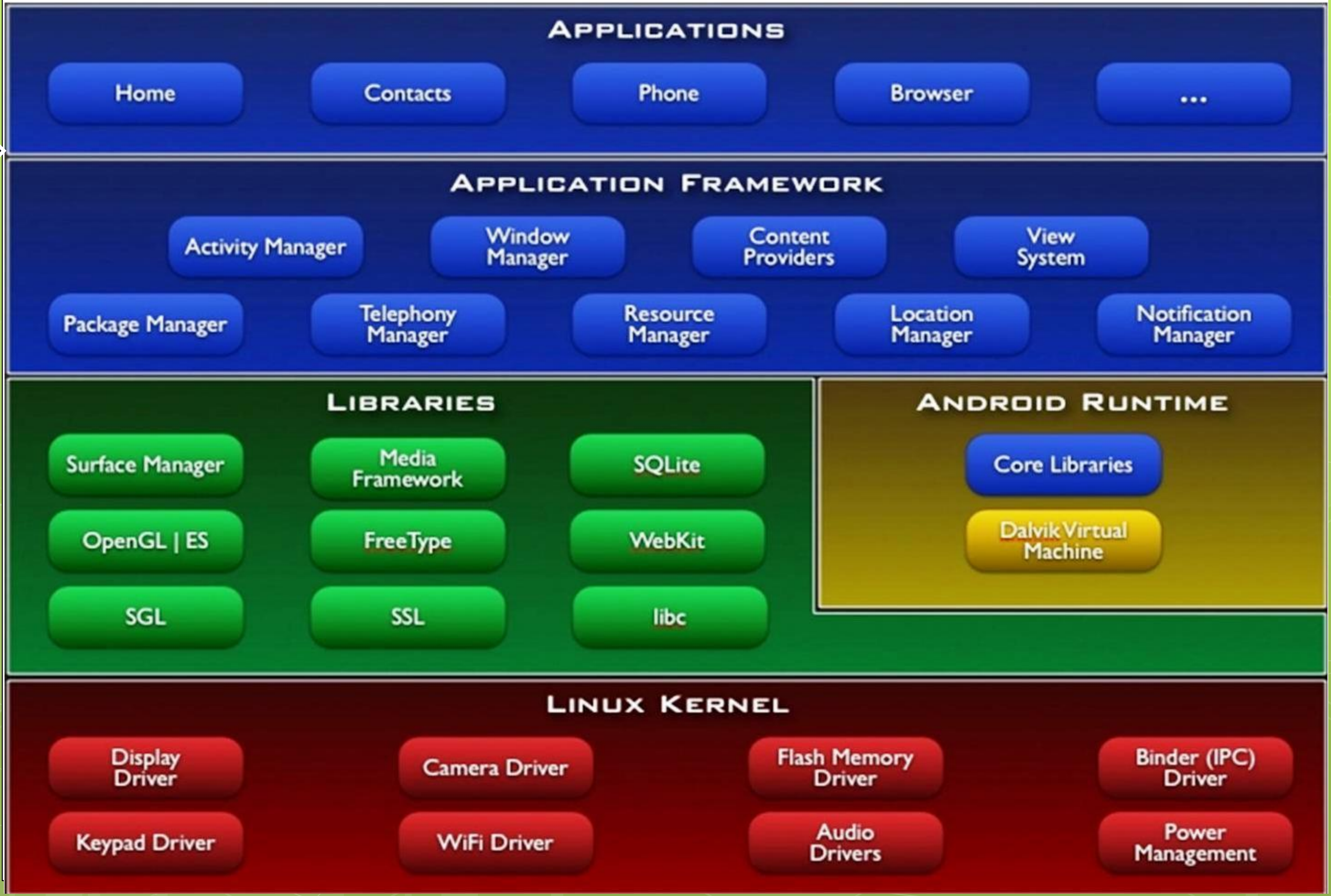
Android™ Architecture



Libraries

- Libraries written in C/C++.
  - They work as support for high performance and real time tasks (OpenGL).
  - Security (SSL).
  - Communication (Socket).
  - Database interaction (SQLite)
  - …

Android™ Architecture



Application Level

- The application level of Android is entirely based on Java.
  - Android uses a slightly modified version of Java.
    - Clash between Google and Oracle.
- Android applications are programmed in Java.

Why Java?

- Open Source Language.
- Highly portable.
- Object-Oriented and extremely expressive.
- Use of Virtual Machine.
  - The Java Virtual Machine is an environment in which Java applications run.
  - Ensures portability and security.

Android Applications (App)

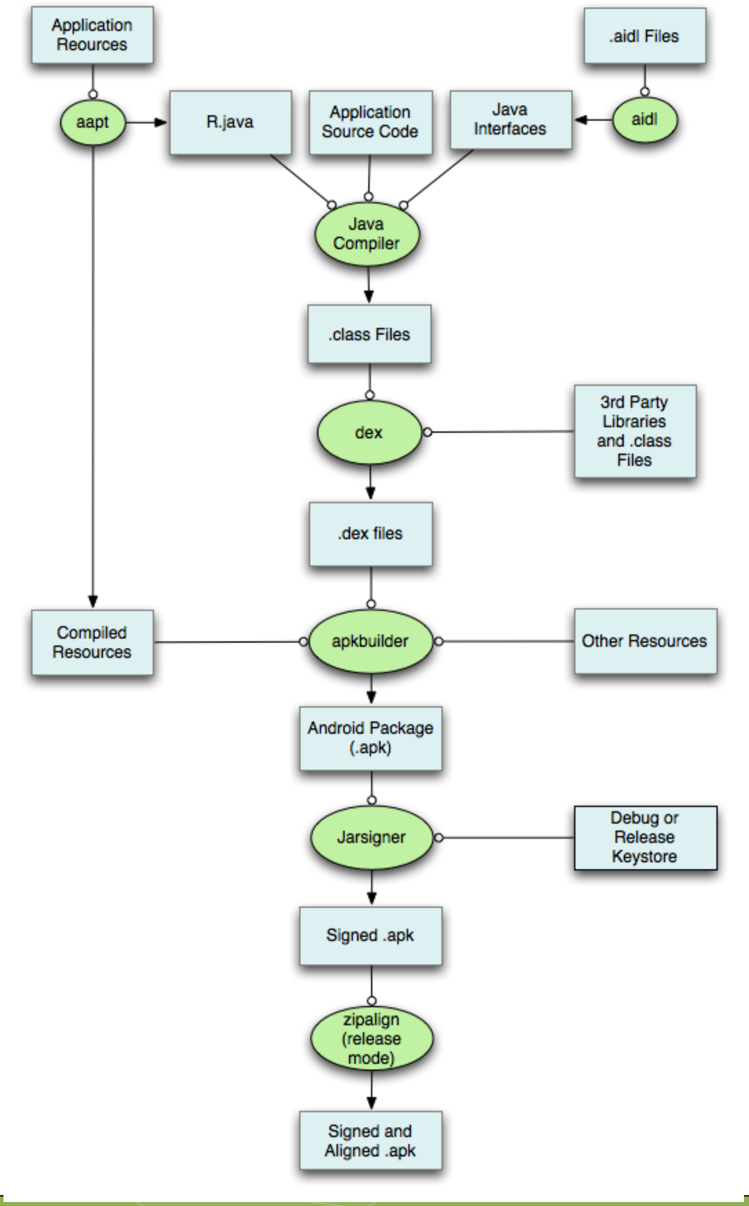
- Android applications come as a unique file directly installed on the device.
- Application PacKage (**APK**) are a bundle of file that contains both executables and static resources.
- Android applications are developed in Java.
- They are distributed through marketplace.

Installing

- How to install an app?
- There are three methods:

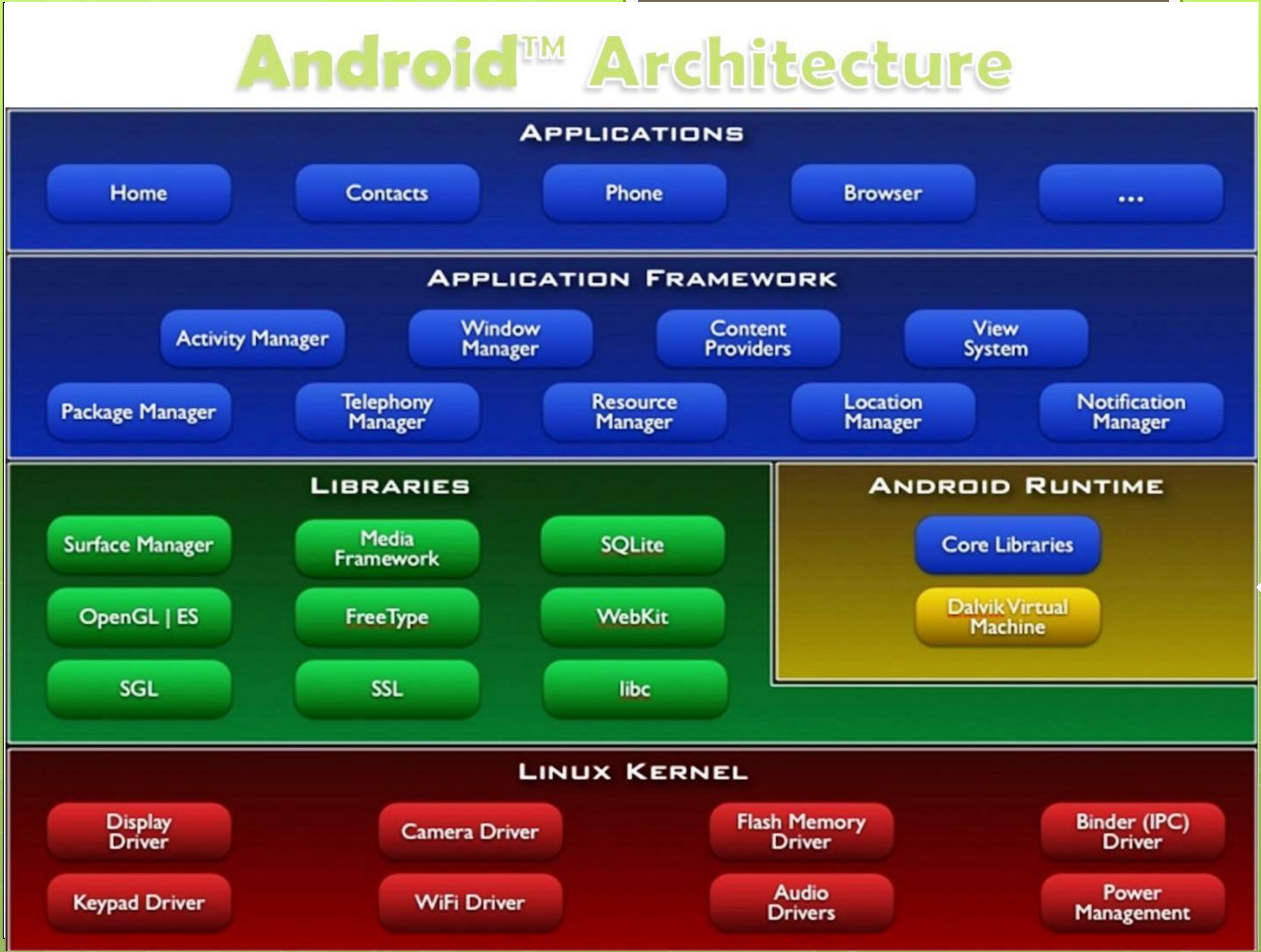
1. Market Installer: Use an application like Play to browse choose and Install Apps
2. File Browser: Put the app on the device memory and install it with a file browser .
3. Use the Android Debug Bridge (ADB).

Building (1)


Application Reources
.aidl Files
aapt
R.java
Application Source Code
Java Interfaces
aidl
Java Compiler
.class Files
dex
3rd Party Libraries and .class Files
.dex files
Compiled Resources
apkbuilder
Other Resources
Android Package (.apk)
Jarsigner
Debug or Release Keystore
Signed .apk
zipalign (release mode)
Signed and Aligned .apk

Building (2)

1. Interfaces, resources and source code are compiled by a classical java compiler.
2. Class files are **dexed**. The result is a **dex** (Dalvik EXecutable) file, an optimized version of bytecode.
3. Executable are merged with static resources to create an apk file.
4. The apk is signed to ensure integrity.
5. Further optimization through zip align.



Android™ Architecture

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

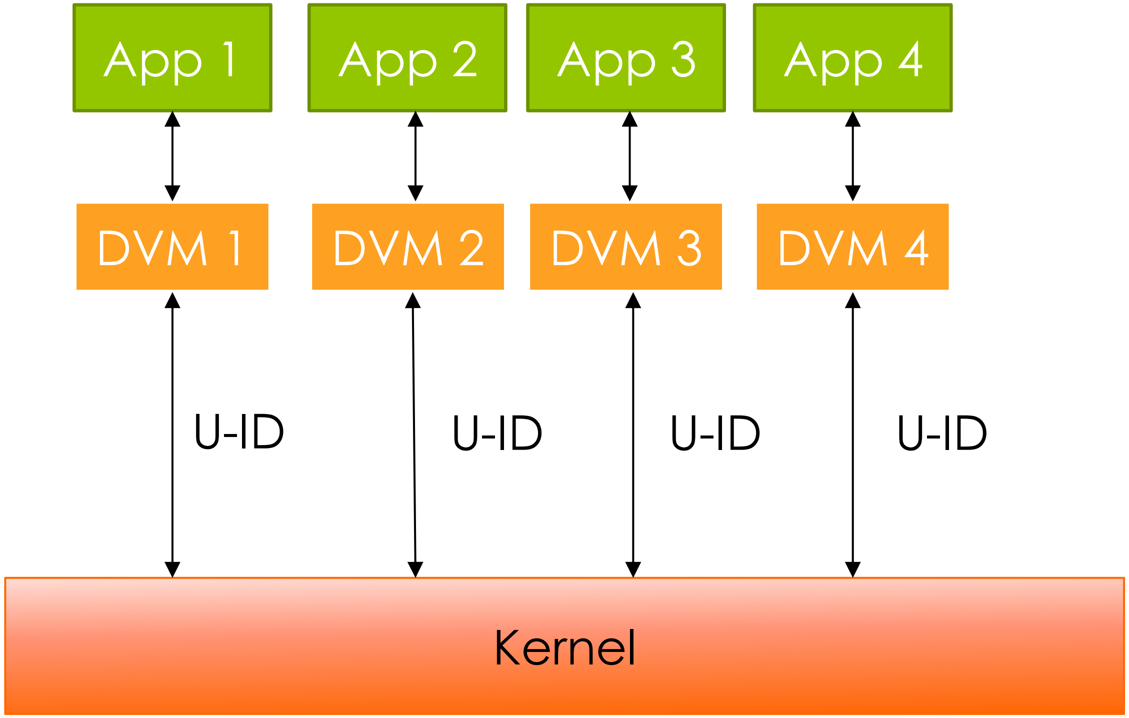
LINUX KERNEL

Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Android Runtime

- In Android applications run on a modified version of the JVM.
- Dalvik Virtual Machine (DVM) is faster and lighter than the classical JVM.
    - Suitable for mobile devices.

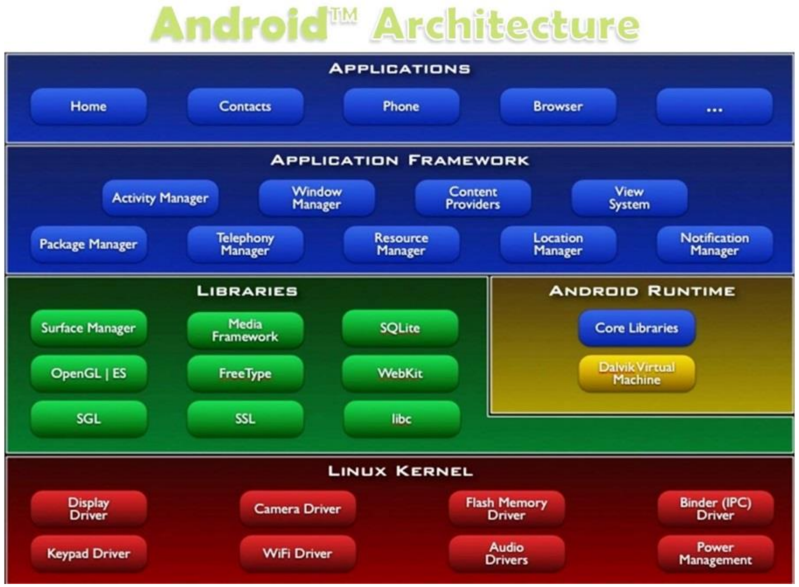
App Execution (1)



App Execution (2)

- Android applications run in the Dalvik Virtual machine. For each running application a different DVM is instantiated.
- The DVM interacts with the underlying Linux kernel.
- Every DVM has a Linux UID. Thus every Android application is considered a different Linux user.
  - The Linux UID is assigned to an application at install time and is not changed until the app is not uninstalled.

Device Side Components



Android™ Architecture

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

Developer Side Components

Standard Development Kit (SDK)

- The Android SDK is a bundle of all the software and tools necessaries to develop, debug and test Android applications.
  - **APK Builder:** Creates ready-to-install applications from code
  - **Android Debug Bridge:** Allow the USB connection and management of an Android device.
  - **Emulator:** Android device emulator.
  - **Android Developer Tool (ADT):** Plugin for the Eclipse IDE.
  - **Fastboot:** Boot a connected device in different modes.
  - **Mksdcard:** Used to create a virtual SDCard**.**

Get it!!

http://developer.android.com/sdk/index.html

Checklist

- Java Runtime Environment installed?
- Java Environment variables correctly set?
- PATH Environment variables correctly set?

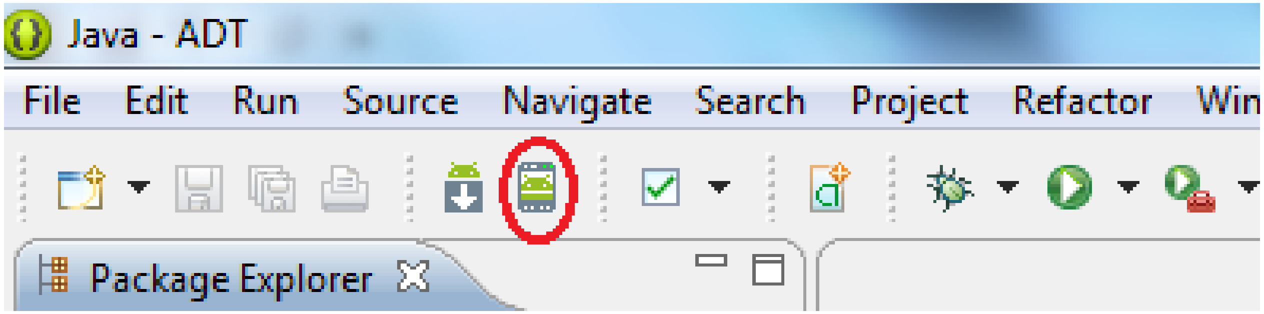
ADT

- Plugin for Eclipse to develop Android applications.

- Includes DDMS to interact with other tools of the Android SDK.

Emulator

- An Android device emulator with (almost) all the functionalities of a real smartphone..
- Virtual devices are created through the Virtual Device Manager.



Android Debug Bridge (1)

- Used to connect and interact with an Android device.
- Some options:
  - adb shell: open a linux shell on the device.
  - adb push/pull: push or pull a file onto/from device.
  - adb install: installs an application on the device.

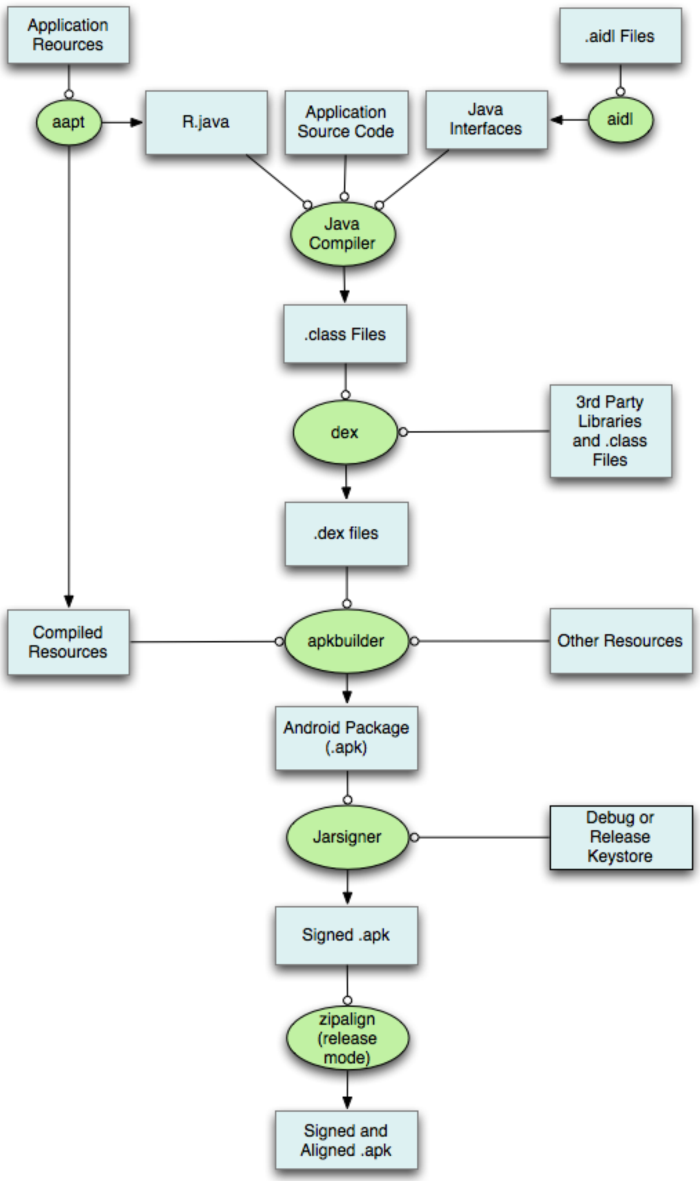
Android Debug Bridge (2)

- Other ADB commands:
  - adb reboot: reboots the connected device.
  - adb devices: lists the connected devices.
  - adb logcat: show the device logcat, used for debugging.
  - …

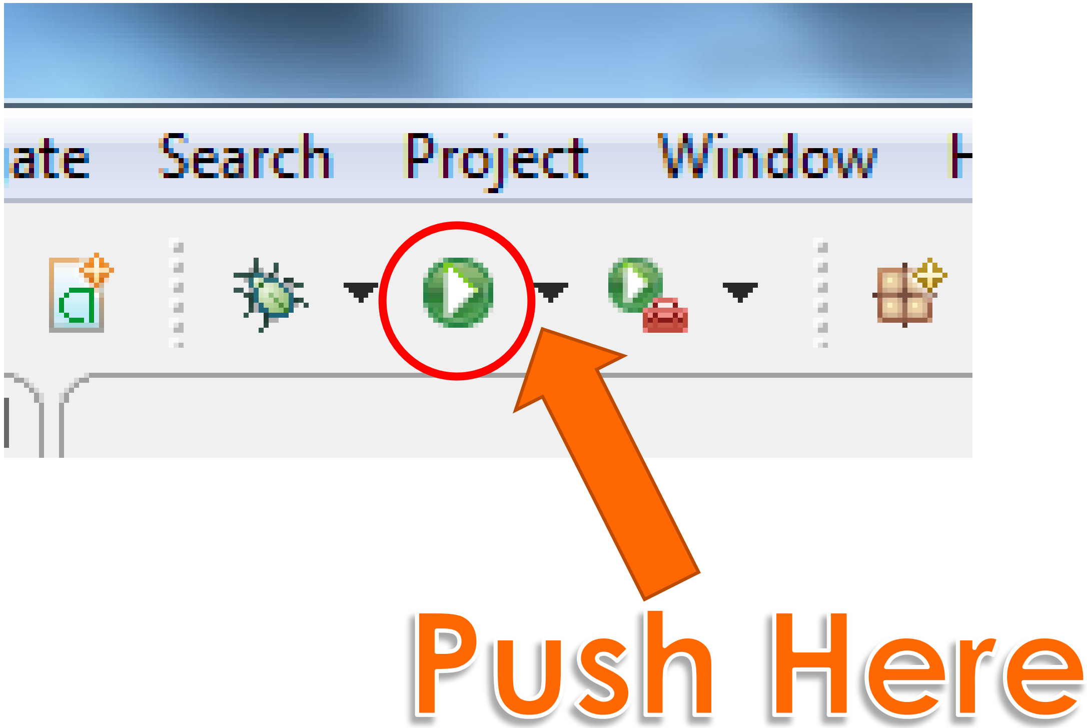
App Developer

- Since the Android SDK can be downloaded for free, virtually anyone can be an app developer.
- We can roughly divide developers in 3 categories:
  - Enthusiast Developers.
  - Professional Developers.
  - Google

Building


Application Reources
.aidl Files
aapt
R.java
Application Source Code
Java Interfaces
aidl
Java Compiler
.class Files
dex
3rd Party Libraries and .class Files
.dex files
Compiled Resources
apkbuilder
Other Resources
Android Package (.apk)
Jarsigner
Debug or Release Keystore
Signed .apk
zipalign (release mode)
Signed and Aligned .apk

Building (with Eclipse)



Programming

- Hello World!
- Create a new project in Eclipse and call it: HelloWorld.
- When ready, build the project.

Application Project (1)

- Folders:
  - **src**: contains the source code written by the developer.
  - **gen**: auto-generated files. These files should not be manually modified.
  - **assets**: all non-pictures resources used by an application should be put here.
  - **bin**: automatically generated executable and files.
  - **libs**: external libraries.
  - **res**: icons, pictures and xml files to describe layouts and fixed values.

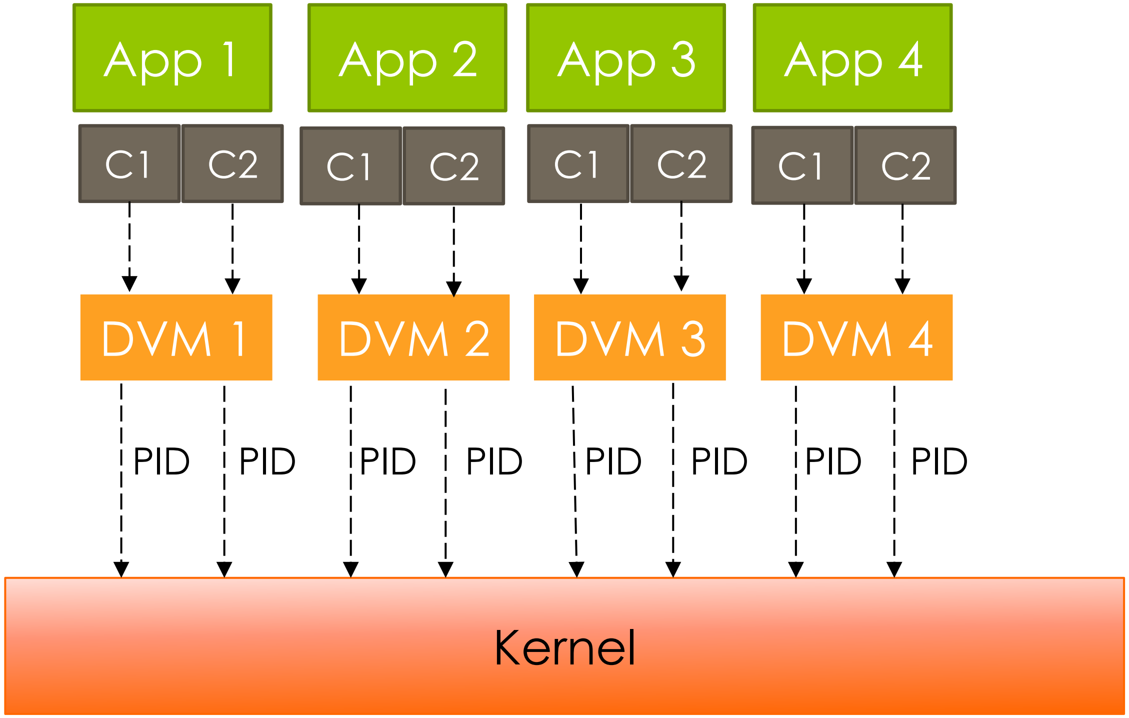
Application Project (2)

- Android Manifest
  - XML file that describes an application.
  - Contains info on developer and version.
  - Lists all the **application components**.
  - Lists all the resource accessed by the application (permissions).
  - Lists all functionalities offered to other applications (intent filter).

Application Components

- Android applications have 5 main components:
  - Activity
  - Service
  - Intent
  - Content Provider
  - Broadcast Receiver

App Execution (3)



App Execution (4)

- An Android application may launch, through the DVM, different processes.
- Generally an application with several components launches a process for each running component. The user of this processes is the one assigned to the application.