Android:
Modding & Hacking

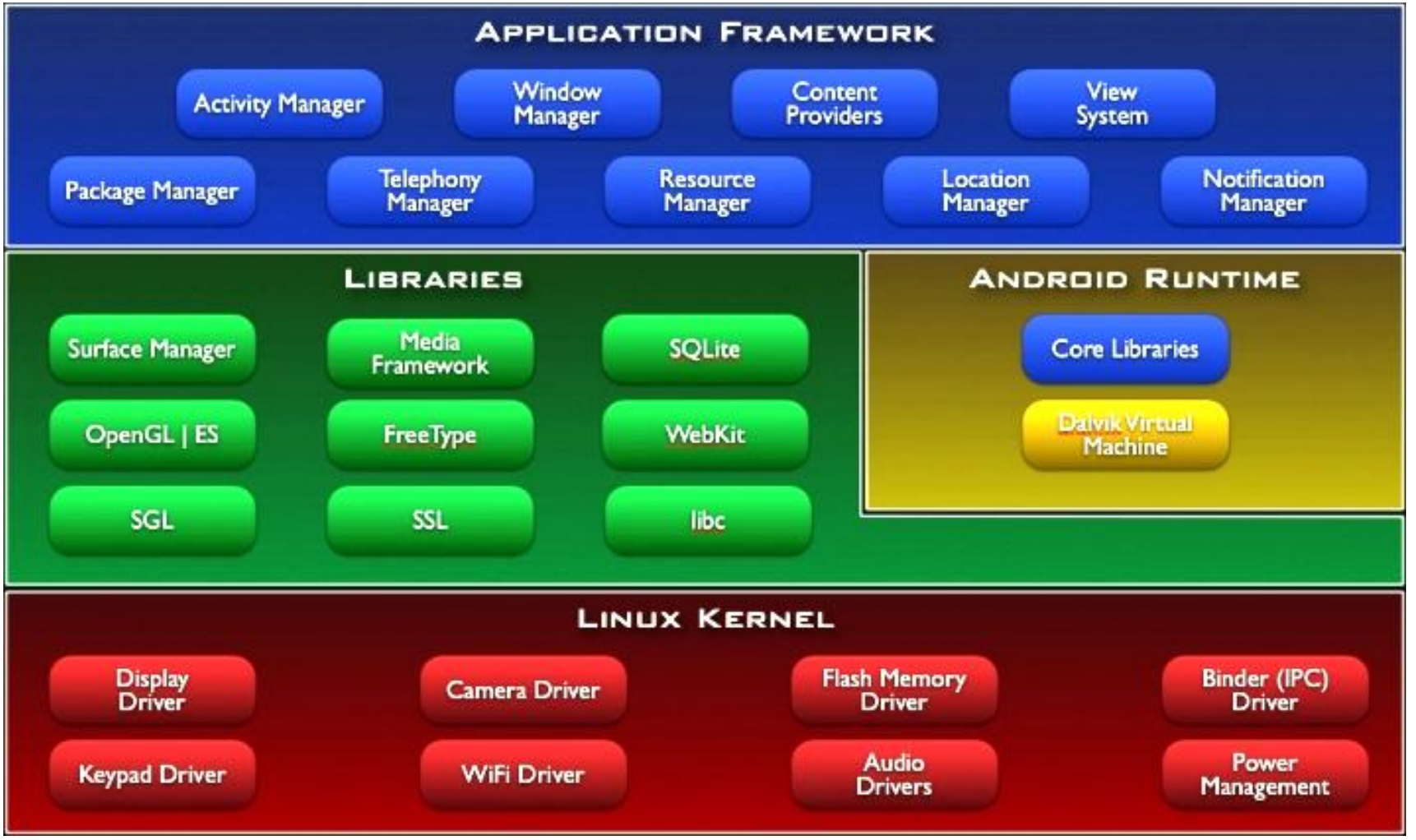
whitone
<whitone@netstudent.polito.it>
2012/12/12

What is Android?

A mobile-centric Linux distro

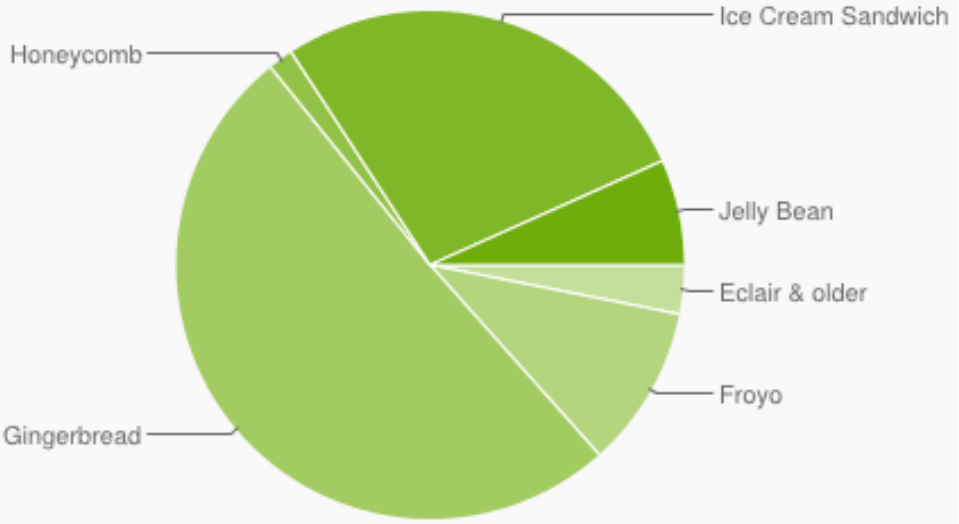
- patched Linux kernel
- Bionic Libc
- Dalvik Java VM
- App Framework

Android Architecture



Android Version Usage

Version	Codename	API	Distribution
1.5	Cupcake	3	0.1%
1.6	Donut	4	0.3%
2.1	Eclair	7	2.7%
2.2	Froyo	8	10.3%
2.3 - 2.3.2	Gingerbread	9	0.2%
2.3.3 - 2.3.7		10	50.6%
3.1	Honeycomb	12	0.4%
3.2		13	1.2%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	27.5%
4.1	Jelly Bean	16	5.9%
4.2		17	0.8%



Data collected during a 14-day period ending on December 3, 2012

Android kernel patches

low memory killer

Viking Killer

wake lock

`/sys/power/wake_lock`

early suspend

`/sys/power/request_state`

timed gpio

userspace driver

Android kernel patches

ashmem

cache

pmem

contiguous malloc

binder

IPC

ram console

`/proc/last_kmsg`

android debug bridge

Android kernel patches

... more on:

linux-kernel-source /

drivers / staging / android

Bionic Libc

embedded optimized

no fully POSIX

not compatible with GNU Libc

native programs
must linked to this library

Dalvik Java VM

register-based architecture

Java bytecode (.class)

Dalvik Executable (.dex)

low memory requirements

Android Applications

Android Packages (APK)

installation via:

- Google Play Store
- storage
(usb hd, sd, ...)
- adb

File System

/system

root of a typical linux tree

/data

apps data

/cache

apps cache

/mnt

storage

File System

in /system:

bin, etc, lib, usr

framework

application framework

app

system apps

media

bootanimation.zip

File System

... also in /system:

build.prop

fonts

roboto (android > 4.0)

xbin

optional utilities

vendor

vendor addons

File System

in /data:

app
user apps

data
user data
`com.android.providers.settings`

dalvik-cache
dex files

Android Debug Bridge

adb

install android-tools
or
android-tools-adb

Android SDK

available also for Mac and Win

Android Debug Bridge

adb shell

limited standard cmds

getprop, setprop
netcfg
input
am

busybox

Settings Database

android_metadata

language

system

volume

secure

lock

SQLite 3

Simple Boot Animation

```
# Usage: make-bootanimation image

# android destination directory
adir="/system/media"

# animation parameters
fps=10
step=5
max=100

mkdir -p bootanimation/part{0,1}

cat > bootanimation/desc.txt << EOF
$(identify -format "%[fx:w] %[fx:h]" $1) $fps
p 1 0 part0
p 0 0 part1
EOF
```

Simple Boot Animation

```
echo -n "generating animation frames: [ "
for brightness in $(seq 0 $step $max)
do
  outfile=$(printf "%03d" $brightness).png
  [ "$brightness" != "$max" ] && n=0 || n=1
  convert \
    -depth 24 \
    -type TrueColor \
    -interlace NONE \
    -modulate $brightness \
    $1 \
    PNG24:bootanimation/part$n/$outfile \
    && echo -en "\b=>"
done
echo -e "\b]"

( cd bootanimation
  zip -qr0 ../bootanimation.zip part0/ part1/ desc.txt )

adb push bootanimation.zip $adir/
```

Android Toolchain

Android NDK

```
make-standalone-toolchain.sh \
  --platform=android-14 \
  --install-dir=~/android-toolchain

PATH=~/android-toolchain/bin:$PATH
export PATH
```

$ arm-linux-androideabi- <TAB>

Useful Links

Official Android Dev

developer.android.com

XDA Developers

www.xda-developers.com

Android NDK

developer.android.com/sdk/ndk/index.html