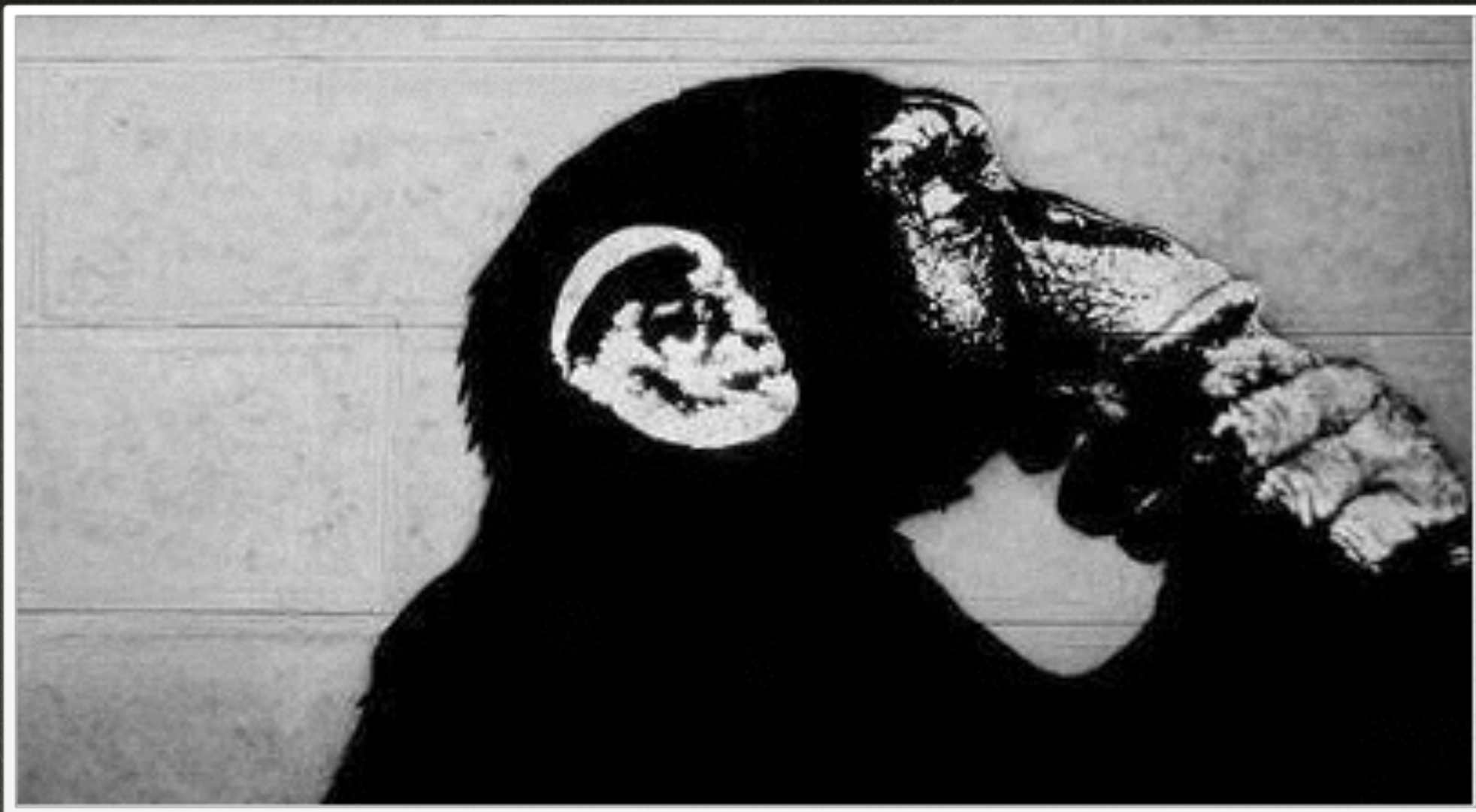


PROGRAMMING AND HACKING ANDROID

Fabrizio Cornelli
HT



FABRIZIO CORNELLI

zeno@hackingteam.com

CV

Filibusta LUG

Laurea a Crema, nel 2012

CTO, Enterprise srl

QA Manager, HT



FIRST RULE OF HT
YOU DO NO TALK ABOUT HT

]HackingTeam[

Fighting crime since 2001

Internet is wrong

Summary

Being a Developer

Being a Hacker

Android Architecture Overview

How to write an APT on Android


```
#include "Investment.h"  
#include "MyProjects/Startup/Success.h"  
#include "MyProjects/Startup/Business.h"  
  
template< typename BusinessStrategy, typename Investment >  
class Business: public BusinessStrategy  
{  
    Business( Investment& MyInvestment );  
}
```

DEVELOPER

“If it ain’t broke, don’t fix it”

Software engineer

Constructive

Programming skills

Good Practices

Design then code (and test)

RTFM

Frameworks and Libraries

Don't be the first

High level languages

Software Engineering Proverbs

The ends does not justify the mean

Choose two: good, fast, cheap

Any fool can write code that a computer can understand. Good programmers write code that humans can understand. [M. Fowler]



HACKER

“shit happens”

Hacker

Deconstructive

Reverse Engineer

Lateral Thinking

Lazy

Subvert the manual

Shortcut

Must be the first

Low level languages (C, asm)

Hacking Proverbs

the ends justify the means

a clever person solves a problem, a wise person avoids it.

Shared values

Discipline / Focus

Imagination

Farmer vs Hunter



- **farmer**
 - permanent settlements
 - tradition
 - patience
 - collaboration
- **hunter**
 - autonomy
 - innovation
 - initiative
 - indipendence

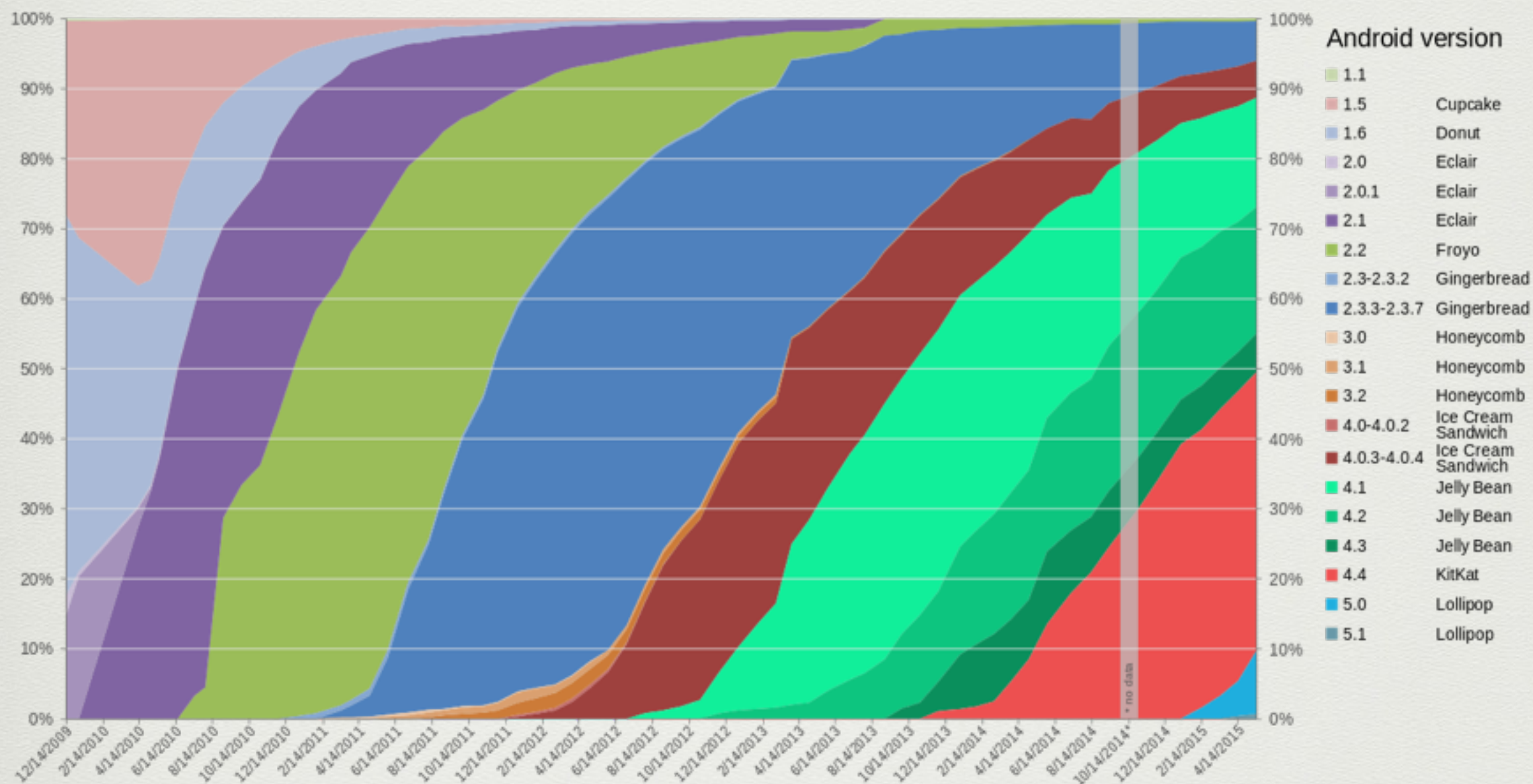
Programming

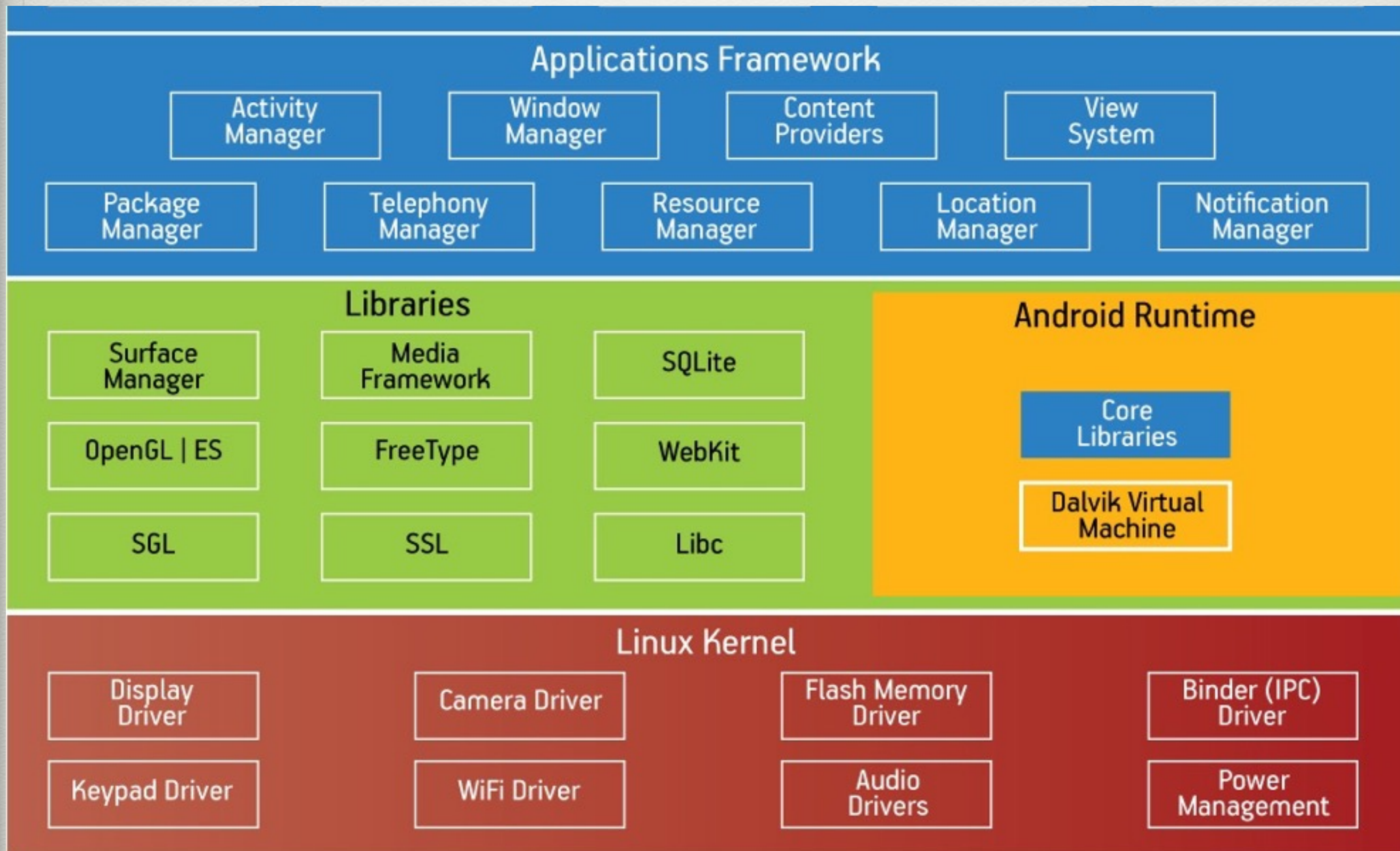
Be a hacker: get your POC

Be a developer: evolve an idea to a product



ANDROID

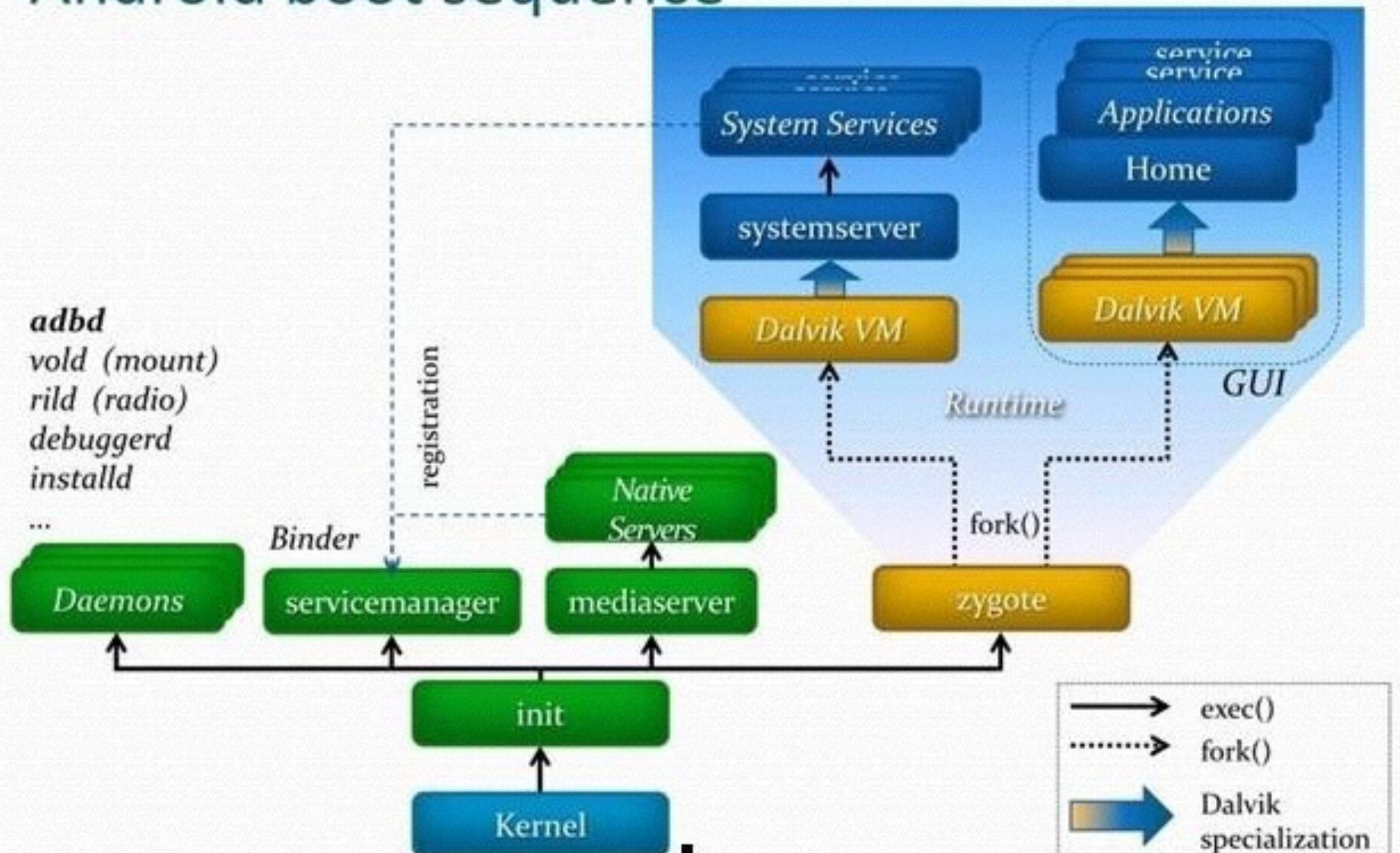




Boot

- firmware
- kernel
 - drivers
 - fs
- user space (init)
 - dalvik / ART
 - daemons
 - GC

Android boot sequence



APK

classes.dex : Code

Manifest

Resources / Assets /Licence

Libs

Signature

Dalvik

Process VM

register based

Java -> bytecode

APK

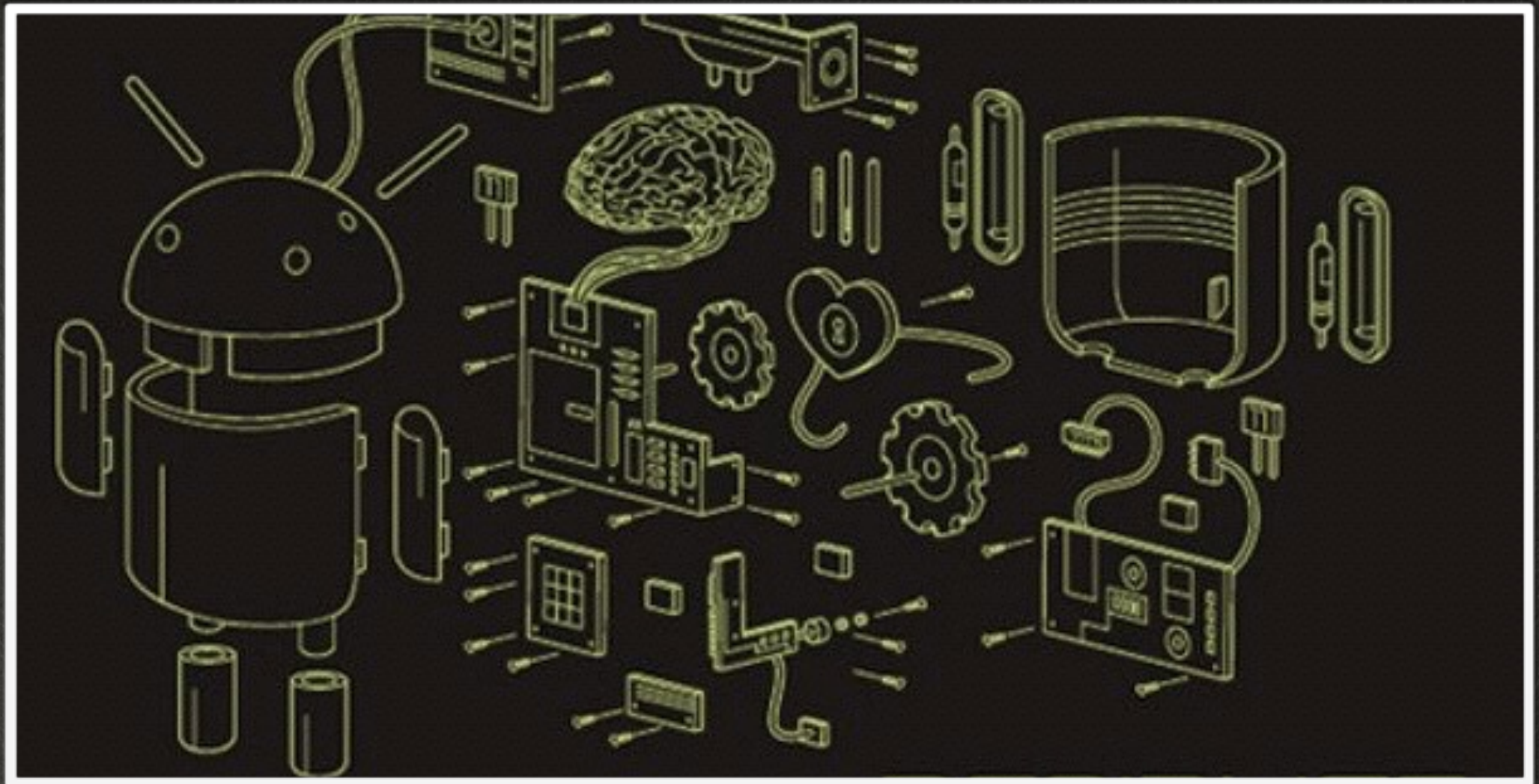
.dex -> .odex

JIT

Android Runtime (ART)

.dex -> elf

AOT Compilation



ANDROID DEVELOPMENT

Android Studio

IntelliJ Platform

IDE

gradle / ant

adb

emulator



ADB

Android Debug Bridge

Device in Debug Mode

subcommands:

shell

pull

push

install

kill-server

reboot



REVERSING

Tools

Decompilers

jd-gui

dad

jeb

Apk dissectors

androguard

apktool

Reversing Frameworks

IDA

Radare

Network analyzer

Wireshark / tcpdump

burp

apktool

decode apk

build apk

internal use of smali/baksmali

needs jarsigner

smali

```
.method public static main([Ljava/lang/String;)V
    .registers 2

    sget-object v0, Ljava/lang/System;-.>out:Ljava/io/PrintStream;

    const-string  v1, "Hello World!"

    invoke-virtual {v0, v1 }, Ljava/io/PrintStream;-.>println(Ljava/lang/String;)V

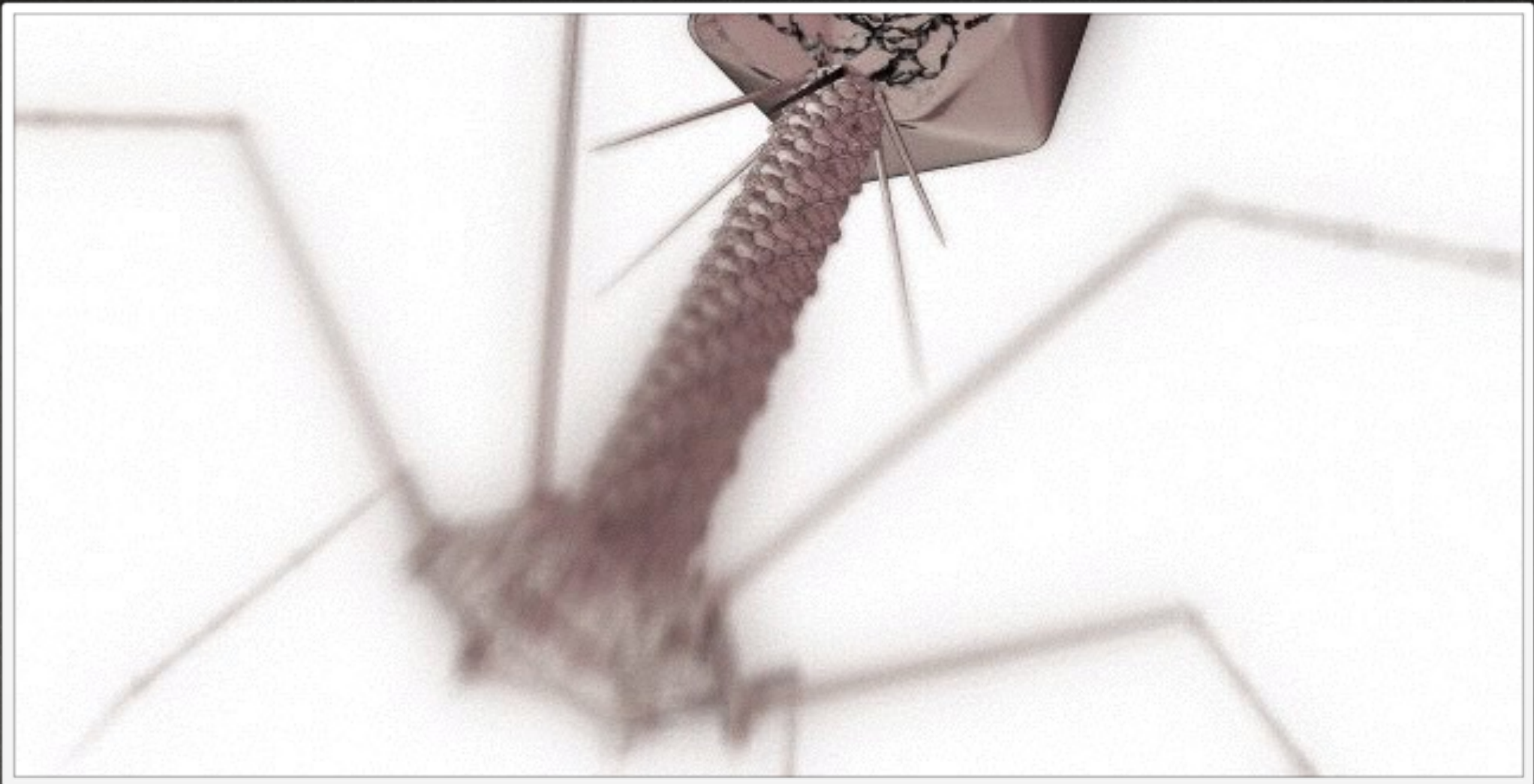
    return-void
.end method
```


learn from malware

<http://contagiominedump.blogspot.it/>

Virus Total

Androguard Database Android Malwares



APT CONCEPTS

Advanced Persistence Threats

Life cycle

Configuration

Build

Installation

Execution

Persistence

Data Exfiltration

Uninstall



HACKING ANDROID

Get the privileges

Flash the OS

Use a local to root exploit

Use a system exploit

Starting at the boot

Use the Manifest

Use the OS (root)

Get data

Use Android API

Use OS libraries

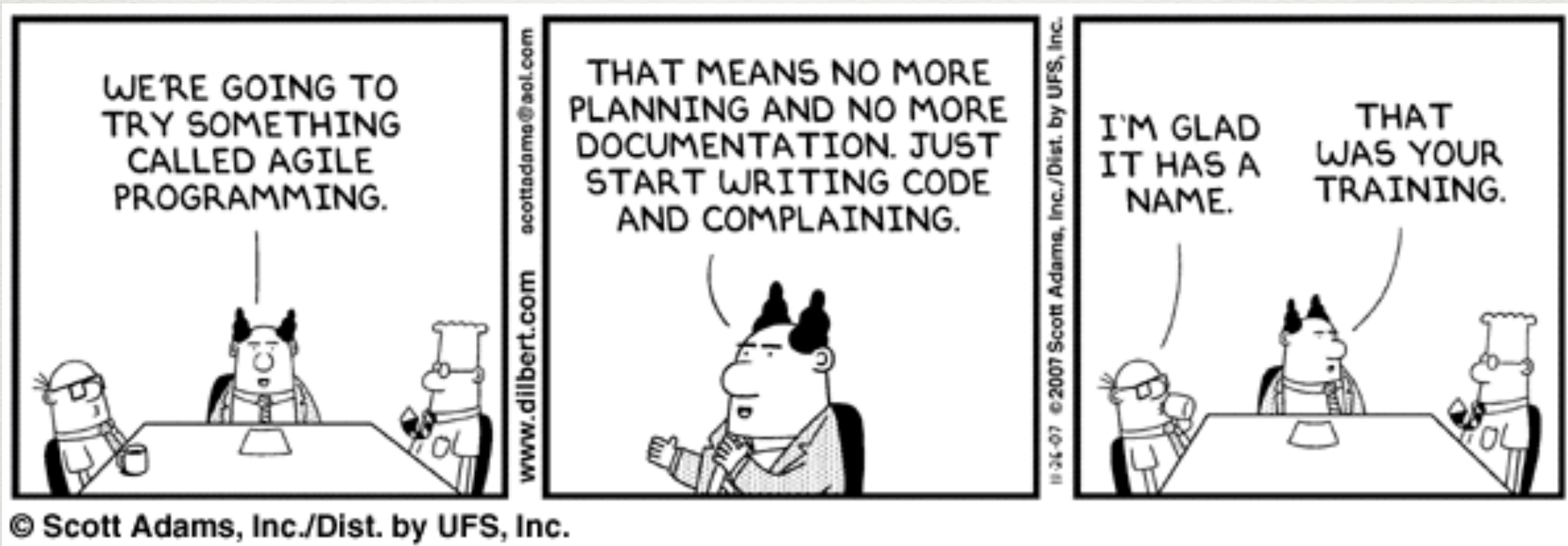
Get data reading memory (root)

Get data reading files (root)

Communication

Covered link

Use Android API



Agile programming

Protect from hackers

anti reversing tricks

polymorphic tools

encryption and obfuscation

anti virtualisation tricks

packing

virtualize

Maintain the code

Versioning

Continuous integration

Testing and code coverage

Acceptance tests

Automatic tests

Make a product

Customer support

Release policies

Marketing



LINKS

]HackingTeam[

NOW HIRING