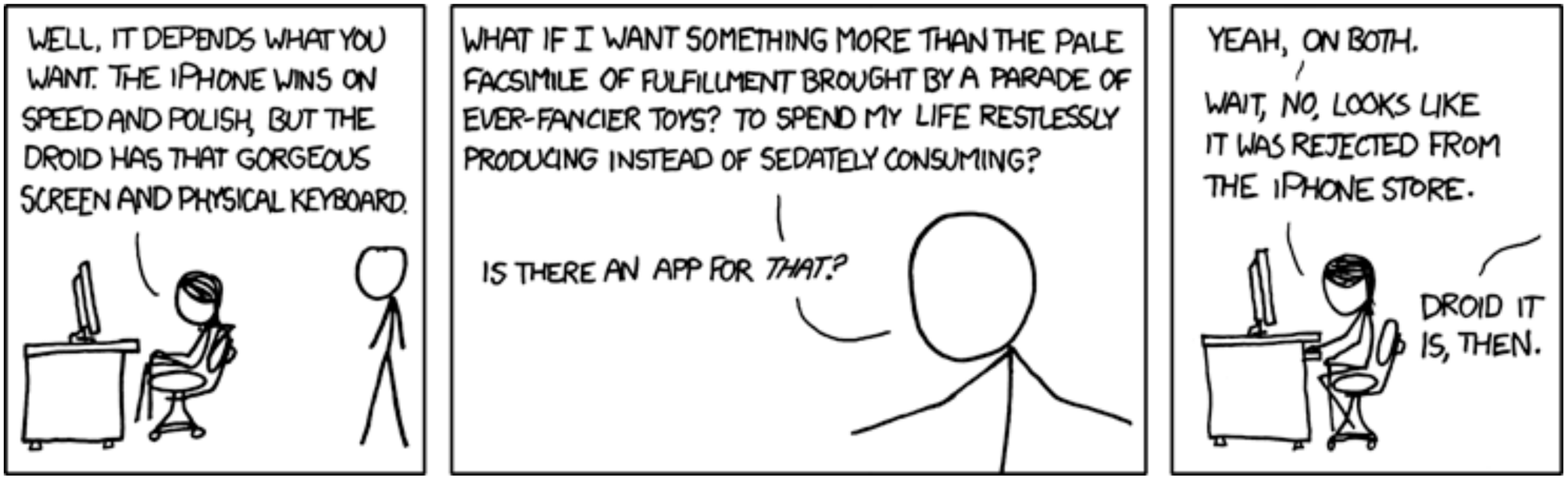


xkcd Comic. (n.d.). Retrieved from http://xkcd.com/662/

Introduction to Android Forensics

Daniel R. O'Day

Purdue University

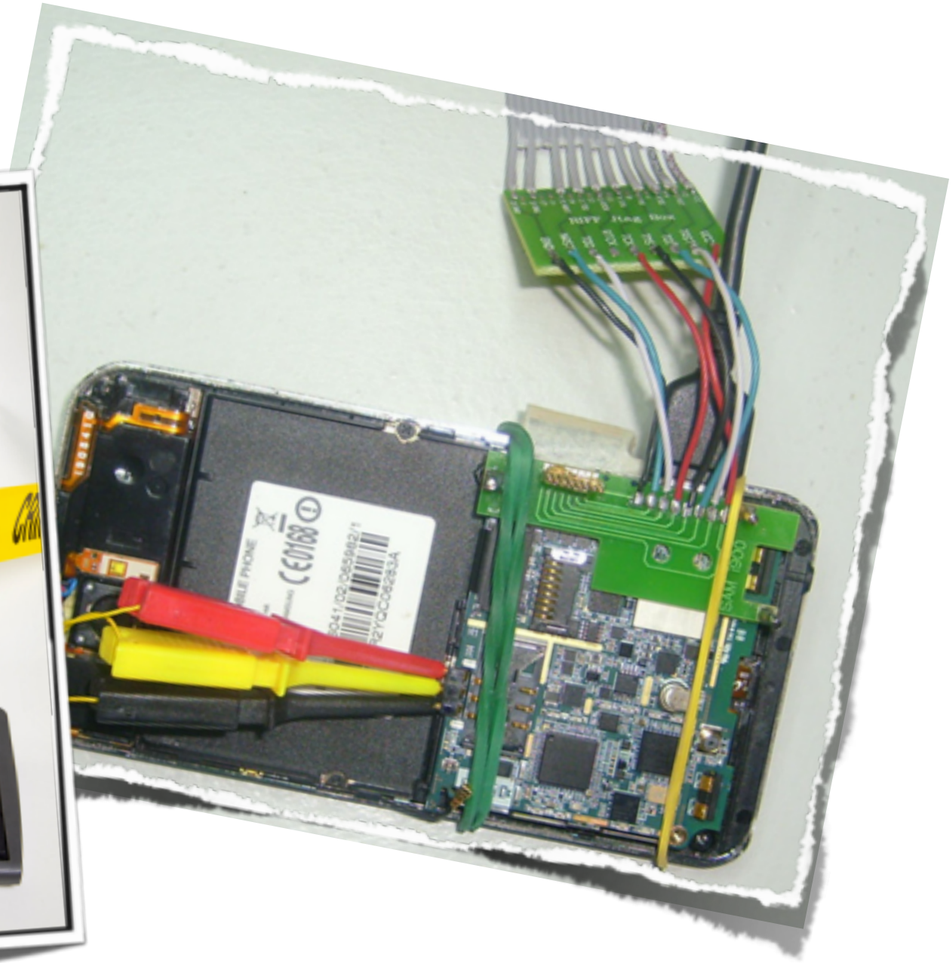
September 10, 2013

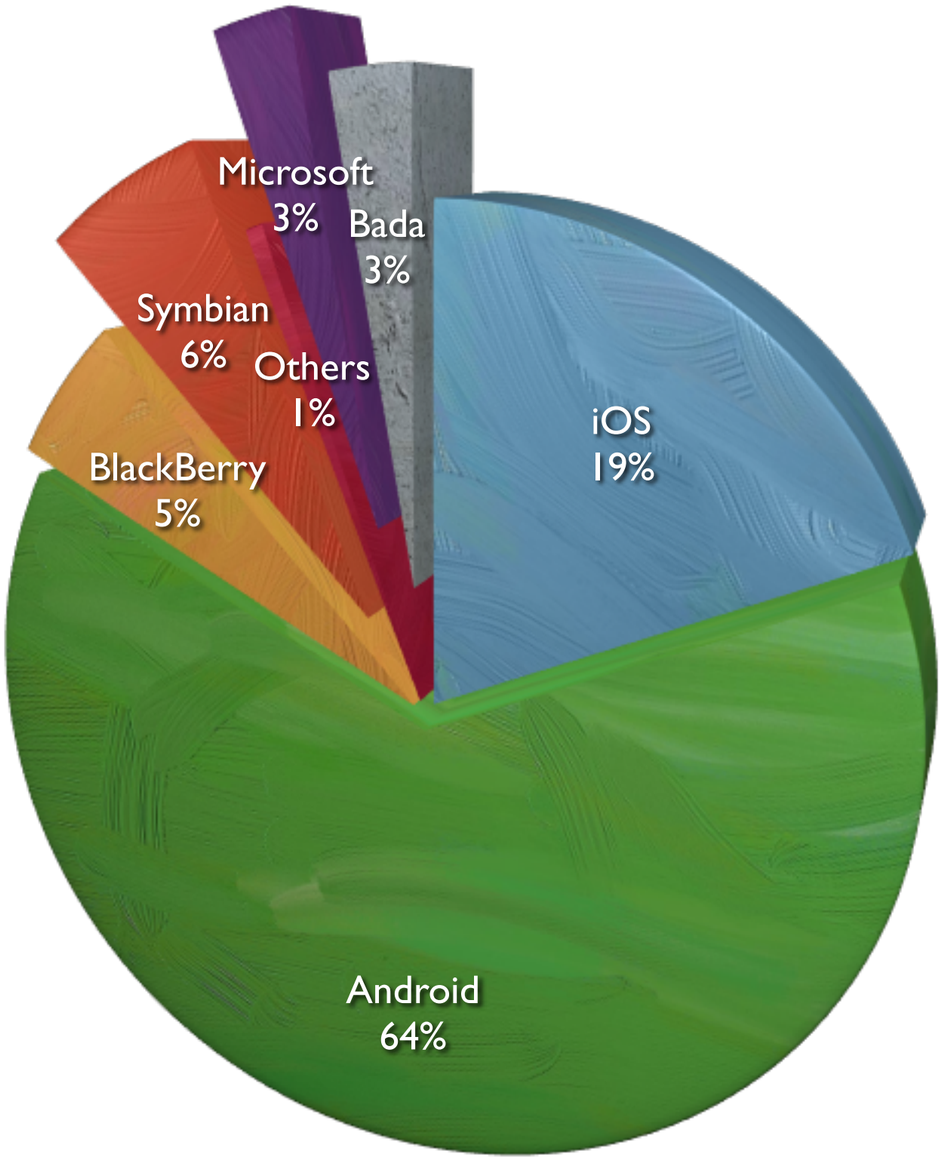
Tentative Schedule

Time	Lesson Objective
8:30 am	Introduction
8:35 am	Android OS Overview
9:00 am	Android SDK & Emulator
9:45 am	Break
10:00 am	Logical Acquisition Methods & Artifact Analysis
11:00 am	Pattern Lock Bypass

Introduction

Dan O'Day





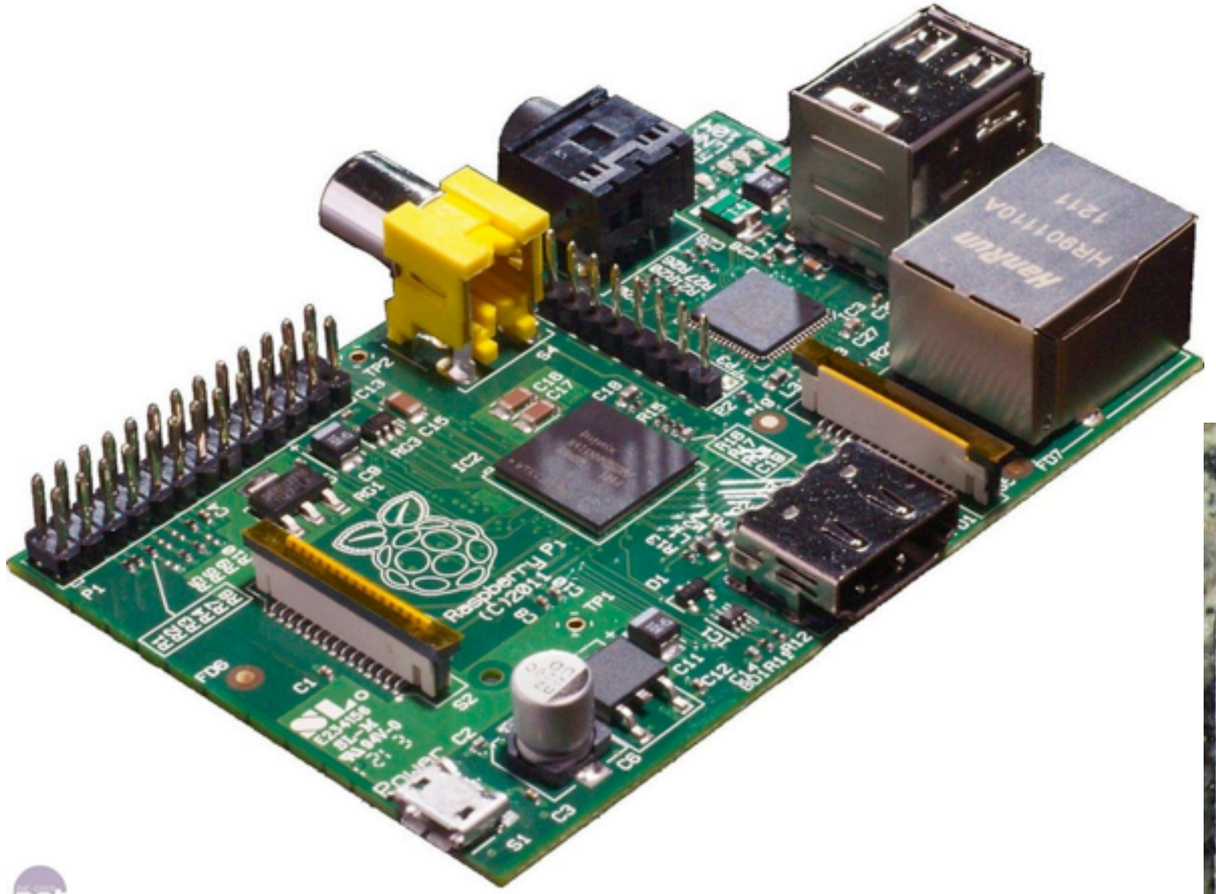
Gartner. (2013). "Gartner Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time." Retrieved from http://www.gartner.com/newsroom/id/2573415

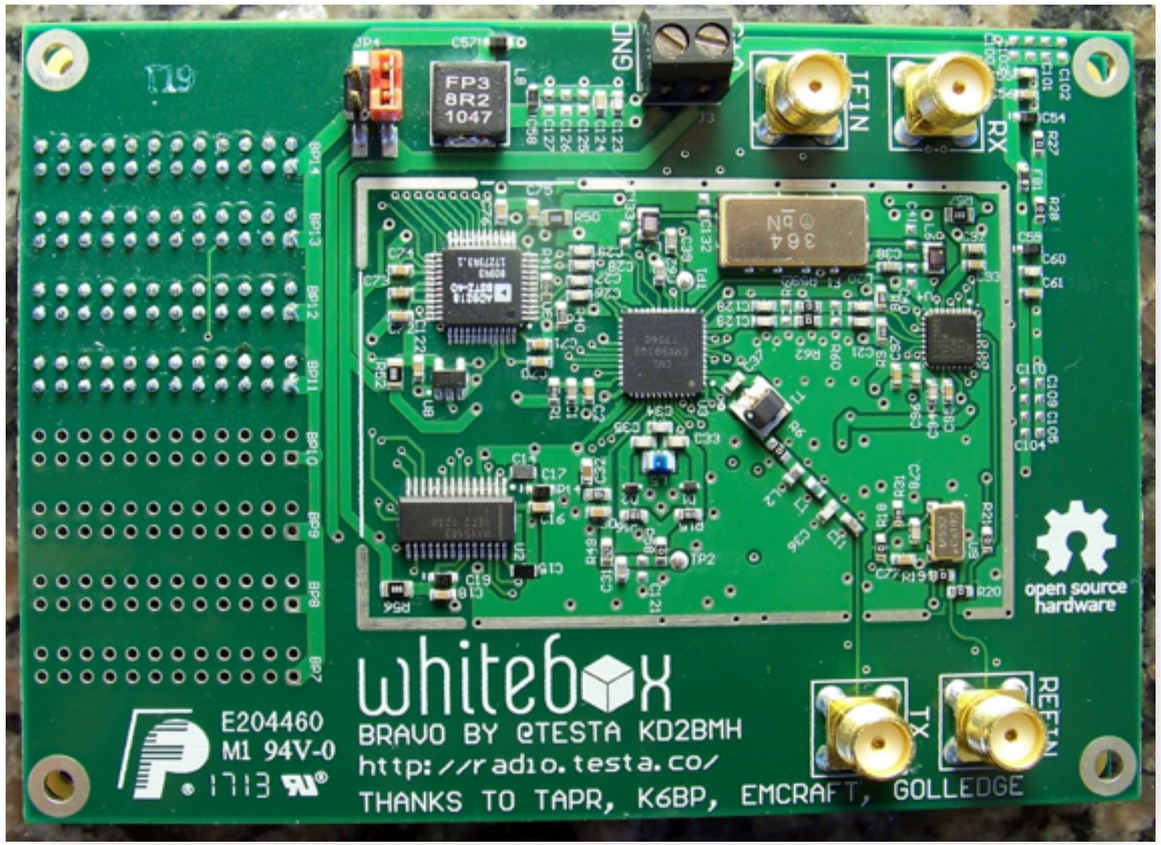
Android Overview

- 900+ million device activations (over 1.5 million activations *daily*)
- Mostly phones and tablets
- What else?

Gartner. (2013). "Gartner Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time." Retrieved from http://www.gartner.com/newsroom/id/2573415

PC Magazine. (2013). "Android Appliances at CES 2013." Retrieved from http://www.pcmag.com/article2/0,2817,2414179,00.asp




GND
IFIN
RX
TX
REFIN
FP3
8R2
1047
whitebox
BRAVO BY @TESTA KD2BMH
http://radio.testa.co/
THANKS TO TAPR, K6BP, EMCRAFT, GOLLEDGE
E204460
M1 94V-0
open source
hardware

- No central point of failure
- No single industry player can control the innovations of others
- Widest implementation possible

Android is responsible for **92%** of all known mobile malware. An increase from **47%** in 2012...

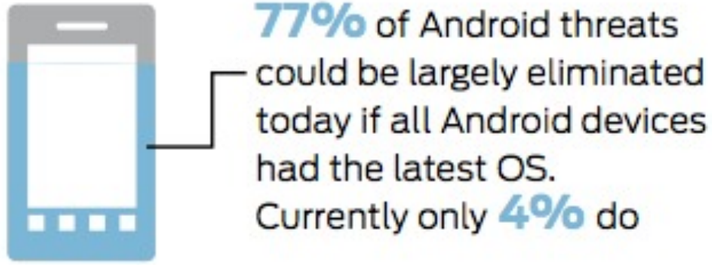
...a significant threat given more than

1 BILLION

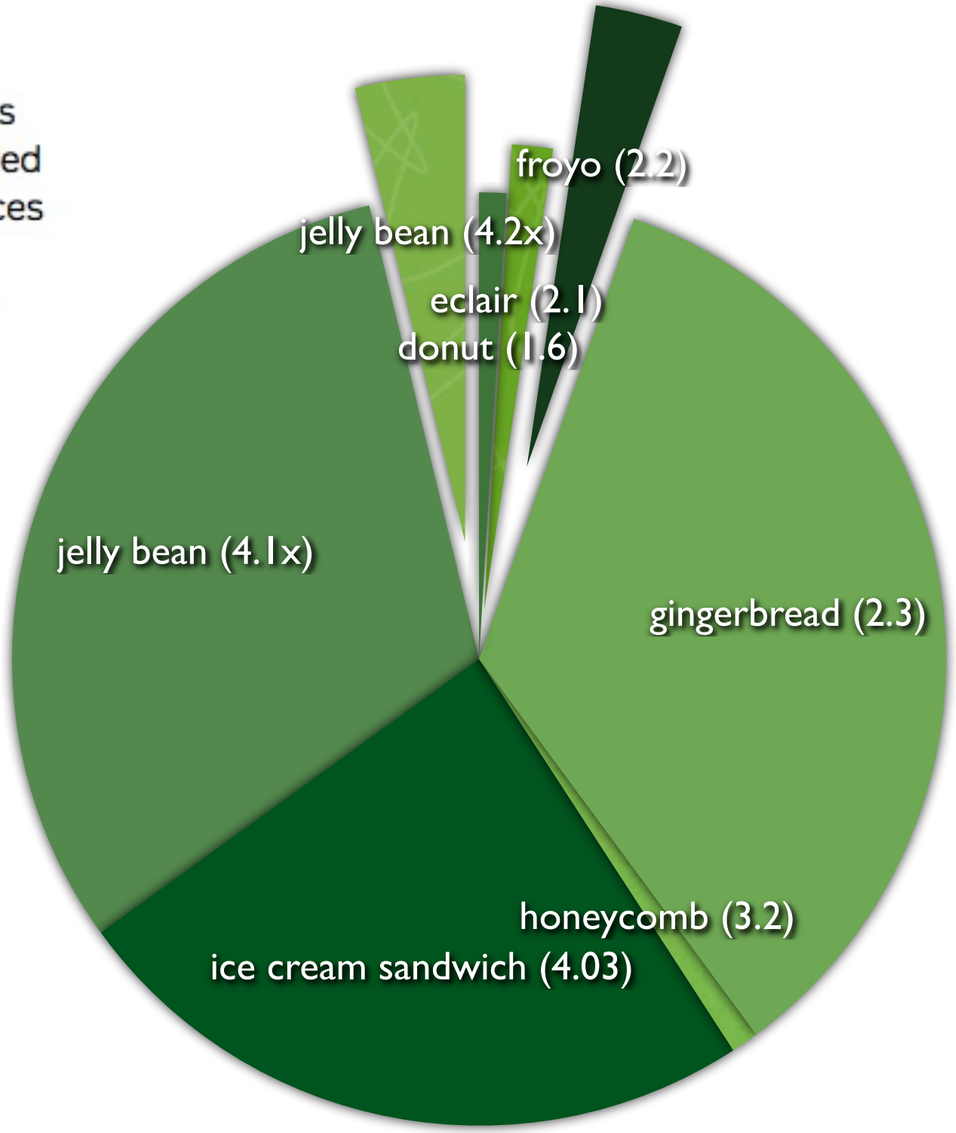
Android-based smart phones are estimated to be shipped in 2017

Source: Canalys Smart Phone Report, June 2013

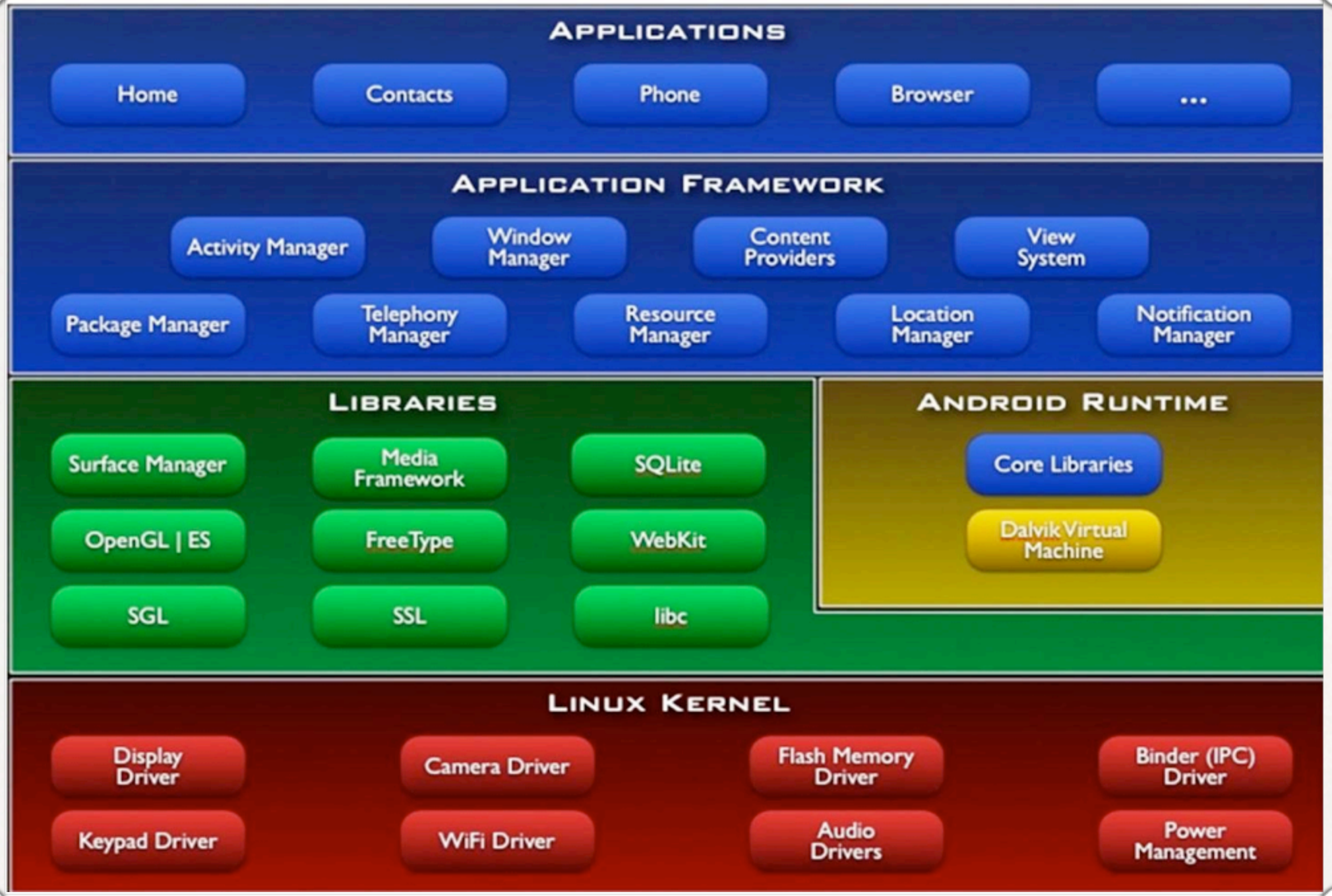
Juniper Networks. (2013). *Third Annual Mobile Threats Report*: March 2012 - March 2013.
Retrieved from http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

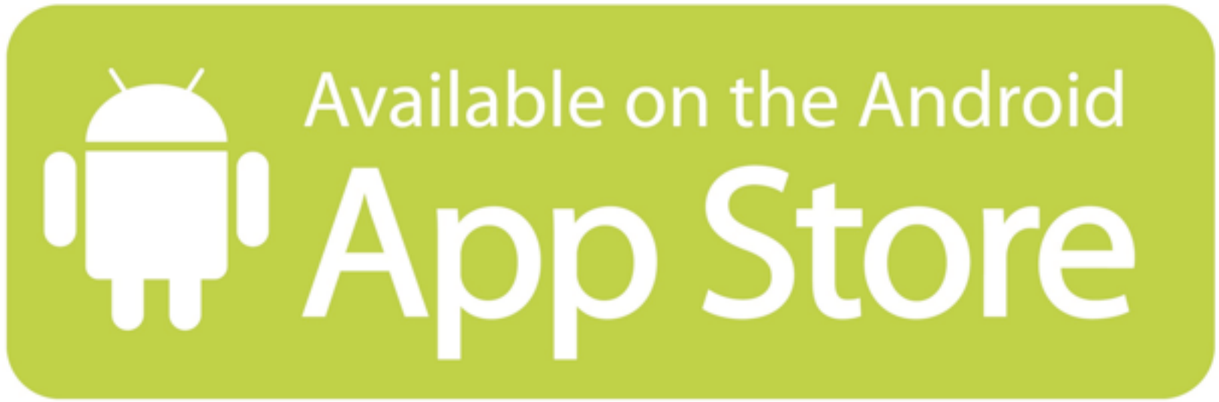


77% of Android threats could be largely eliminated today if all Android devices had the latest OS. Currently only **4%** do



Juniper Networks. (2013). *Third Annual Mobile Threats Report*: March 2012 - March 2013.
Retrieved from http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

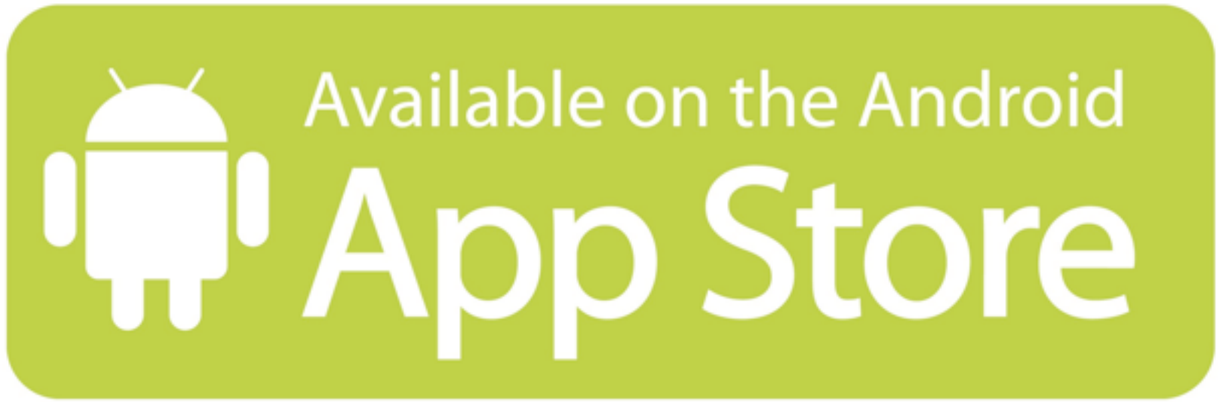

Applications
Home
Contacts
Phone
Browser
...
Application Framework
Activity Manager
Window Manager
Content Providers
View System
Package Manager
Telephony Manager
Resource Manager
Location Manager
Notification Manager
Libraries
Surface Manager
Media Framework
SQLite
OpenGL | ES
FreeType
WebKit
SGL
SSL
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



App → unique UID/GUID/process

→ Dalvik VM instance

→ data storage



Four types of data storage available to developers

1. Preferences (key/value)
2. Files
3. SQLite databases
4. Cloud

NAND Flash Memory

- Access via a page
- Limited P/E cycles
- Page must be erased before writing (writes all 1's)
- Page only written once, no update without erase

NAND Flash Erase/Write

- Entire block is written with 1's when erased
- The only way 0 can be changed to 1
- So when written to (not erased), it only changes the 1 bit to a 0
- Lots of latent data can be found

Android File Systems

- YAFFS/2 (optimal FS for NAND chips - optimally handled variable page sizes, OOB areas, wear leveling, and strict write requirements; primarily used through 2.2/Froyo)
- Ext3/4 (2.3/Gingerbread and most thereafter)
- V/FAT/32 (SD Cards)
- Can run different FS's on different partitions

Artifacts Commonly of Interest

- /data partition
  - app: .apk install bundles
  - dalvik-cache: .dex files ran (compiled .apk files)
  - data: most app data, especially sqlite db's
  - misc: dhcp, bluetooth, wifi, vpn, etc.
  - system: installed app list (packages.xml), users, locked screen security

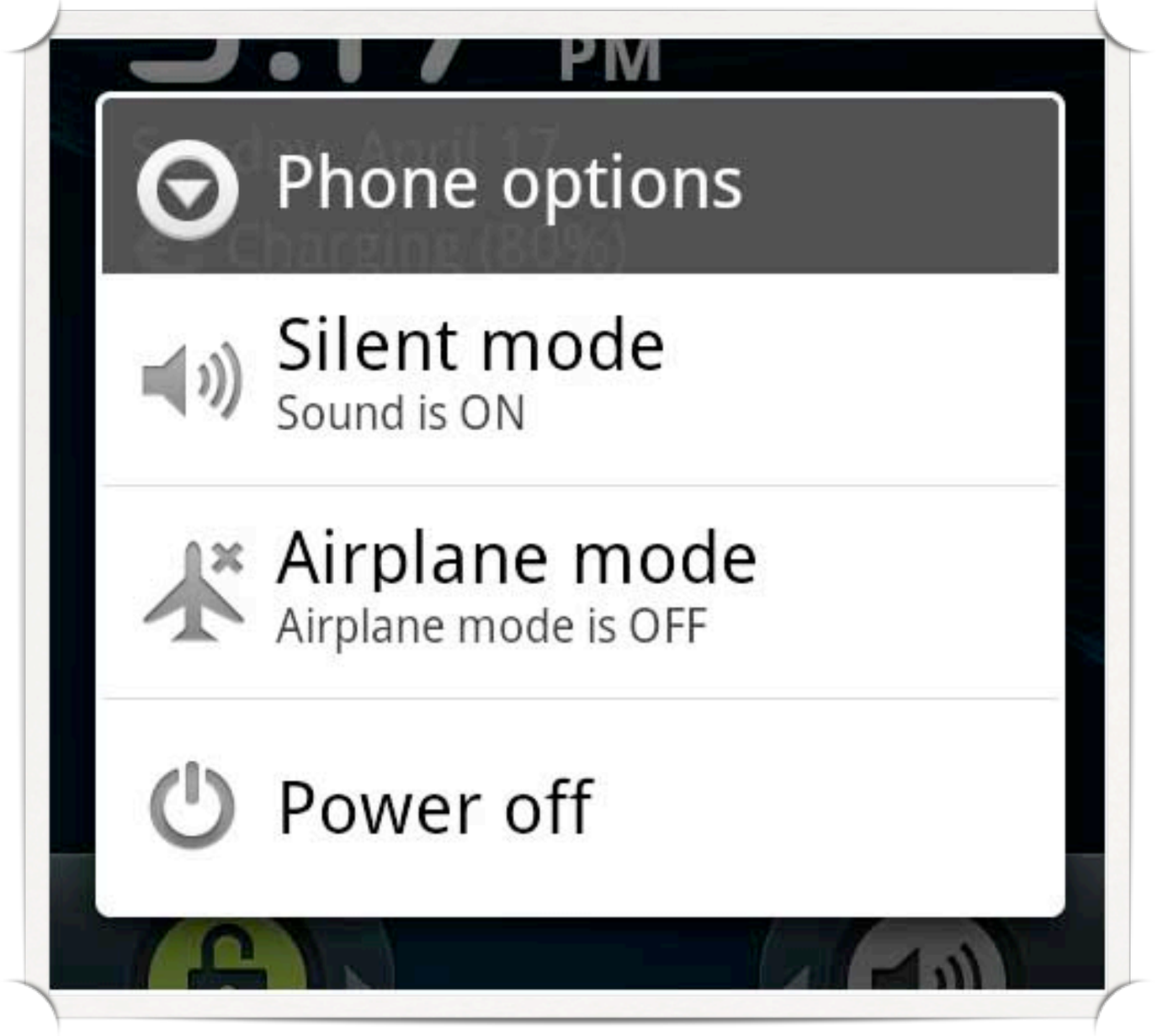
Artifacts (continued)

- /cache partition
  - OTA updates
  - Web-based cached data (browser, gmail, etc.)
- Lots more - poke around and find them

Parsing Android Timestamps

- Unix epoch (January 1, 1970) in *milli*seconds
- Divide standard Unix time by 1000 and convert
- date -d @1234567890
- select datetime(timestamp/1000) as convertedtime from table;

Analysis Methods


PM
Phone options
Silent mode
Sound is ON
Airplane mode
Airplane mode is OFF
Power off


SanDisk
2GB
MADE IN CHINA

.XRY

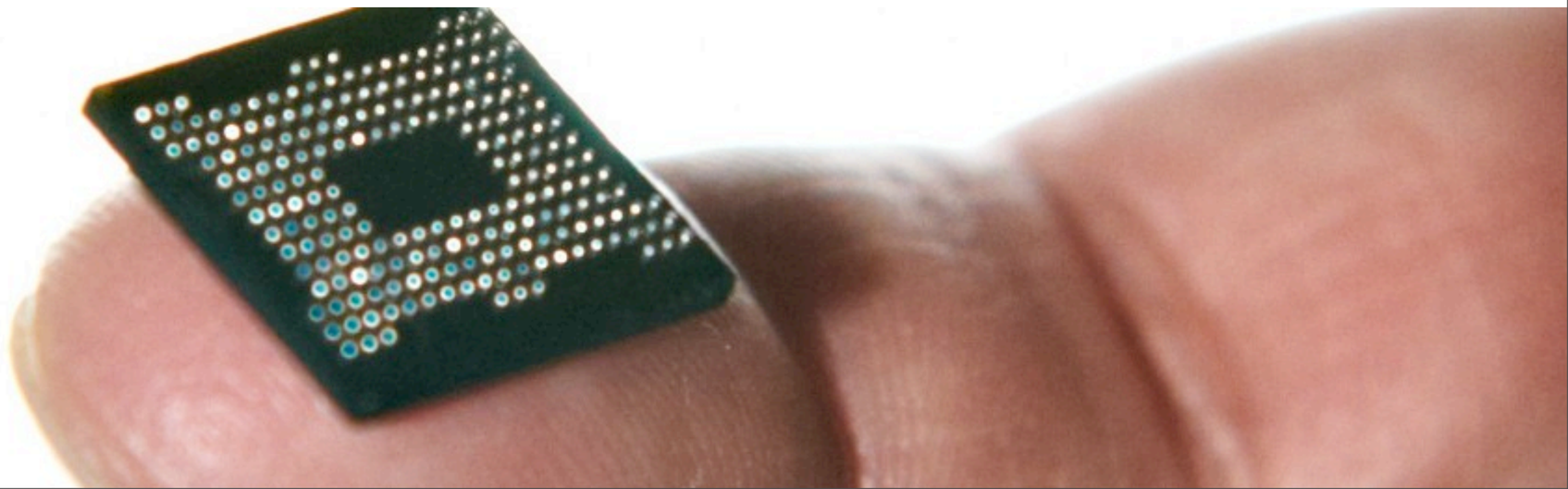
paraben
forensic tools

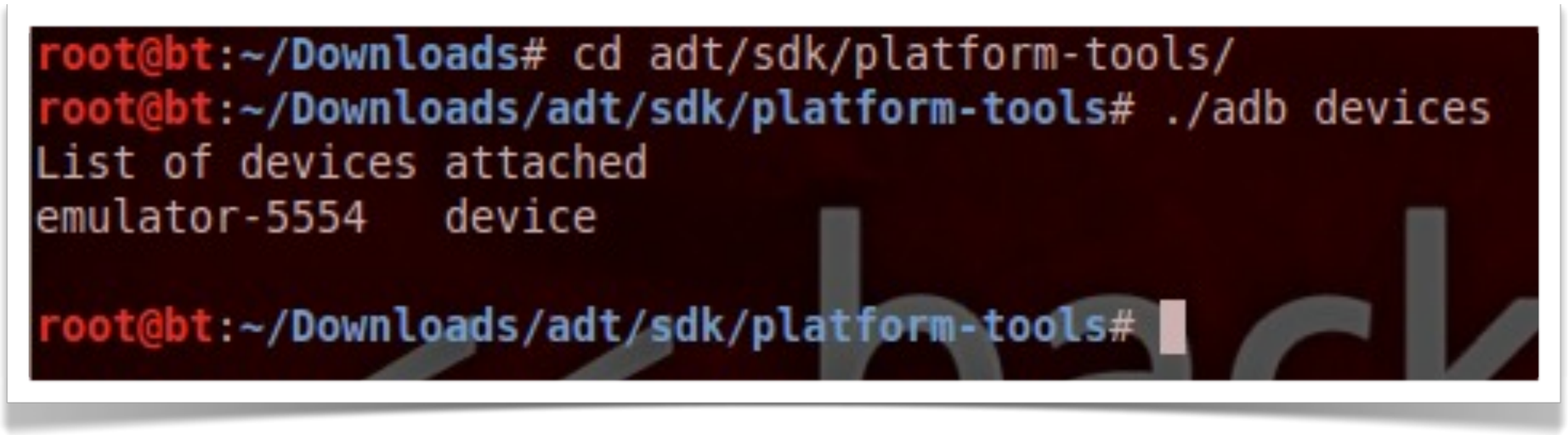
SECURE VIEW 3
Powered by susteen

VIAFORENSICS
advancing mobile security

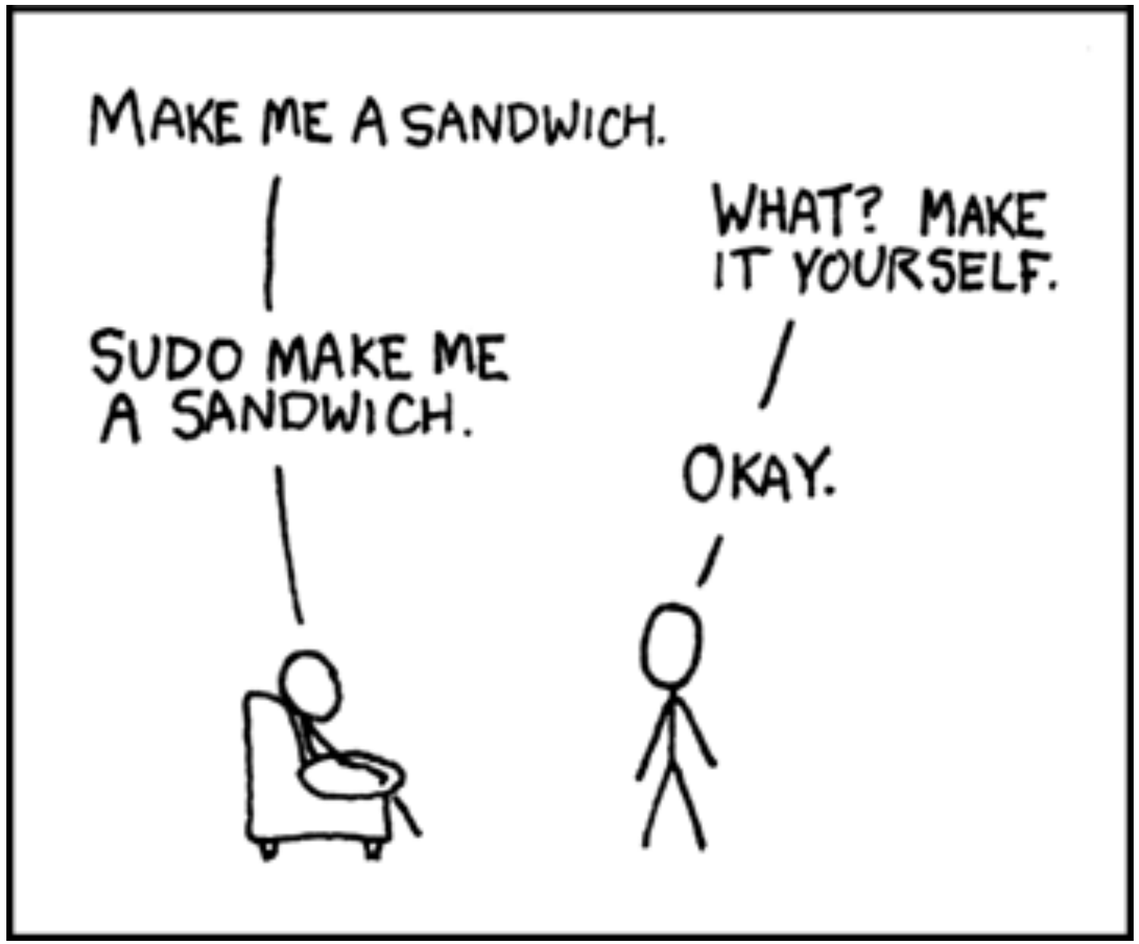
Oxygen Forensic
Suite


ROCKER BOX
WWW.ROCKERDONGLE.COM




root@bt:~/Downloads# cd adt/sdk/platform-tools/
root@bt:~/Downloads/adt/sdk/platform-tools# ./adb devices
List of devices attached
emulator-5554   device
root@bt:~/Downloads/adt/sdk/platform-tools#

#


MAKE ME A SANDWICH.
WHAT? MAKE IT YOURSELF.
SUDO MAKE ME A SANDWICH.
OKAY.

# #

- USB debugging
  - Rage against the cage
  - psneuter
  - gingerbreak
  - zergrush
  - tacoroot
- 12m
- debugfs
- One click root solutions

- Logical forensic applications (many COTS)
  - AFLogicalOSE.apk (F/OSS)
  - Uses ContentResolver object to get data from ContentProviders
  - Writes data to CSV files on SD card

Android SDK & Emulator

- API libraries and tools for app development
- Java headache (aspirin below):
  - License issues between Ubuntu and Oracle, so no supported Java releases (including JDK and JRE which we need)
  - Ubuntu officially supports OpenJDK and OpenJRE (already installed on BT5)

ADT

- ADT bundle at http://developer.android.com/sdk/index.html
- Unzip/untar, go to sdk/tools directory
- ./android update sdk

Emulator

- Android SDK Manager
  - Tools > Manage AVDs
  - Create test device
  - Run test device: ./emulator @TestDeviceName
  - Very buggy, especially first time test device is run
  - Make artifacts


break

Examine Artifacts

- Inside ADT bundle, navigate to sdk/platform-tools directory (new Terminal window)
- ./adb devices (don't forget USB debugging)
- ./adb shell
- Examine artifacts

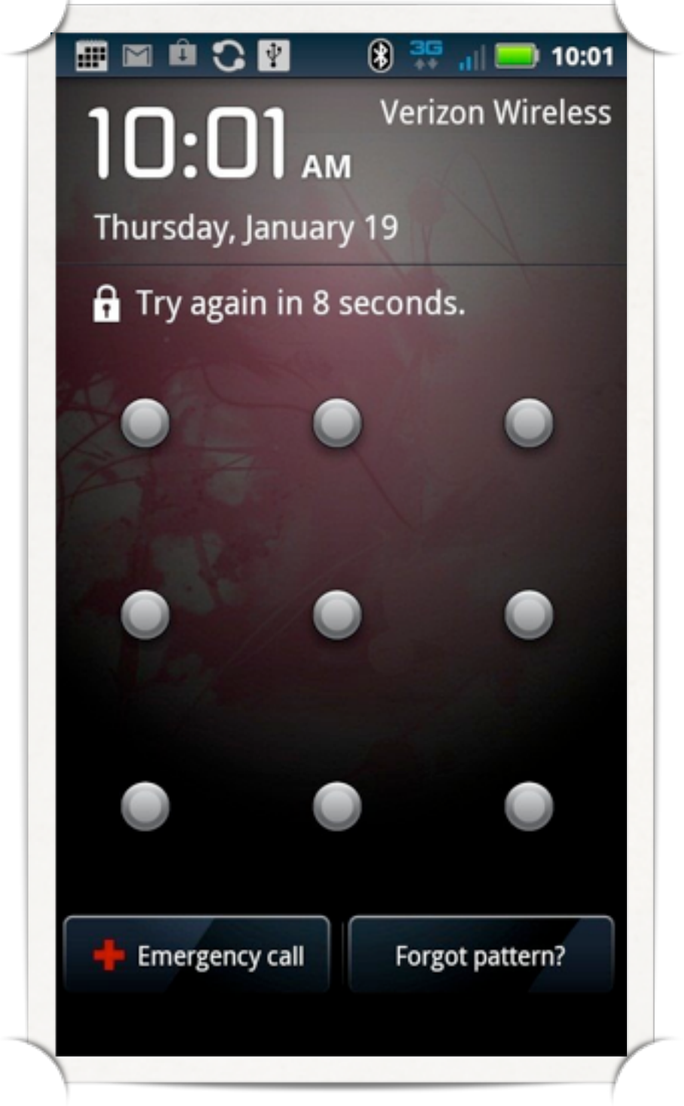
AFLogical

- F/OSS available at: https://github.com/viaforensics/android-forensics/downloads
- License covers academic use, expanded use must get permission from viaForensics
- Replace user SD card with examiner SD card
- ./adb install AFLogical-OSE.apk
- Run on device by opening app

AFLogical (continued)

- Capture desired artifacts (open source edition has limited options)
- Retrieve from SD card (/sdcard/forensics directory)
- ./adb pull /sdcard/forensics ~/Desktop/wherever
- ./adb uninstall com.viaforensics.android.aflogical_ose
- Batch parse Android timestamps in AFLogical CSV output with http://digital0day.googlecode.com/files/pdtime.py

Bypass Pattern Lock



Pattern Lock

- Set pattern lock
- ./adb pull /data/system/gesture.key
- Obtain script from https://github.com/sch3m4/androidpatternlock
- python crack.pattern.py gesture.key