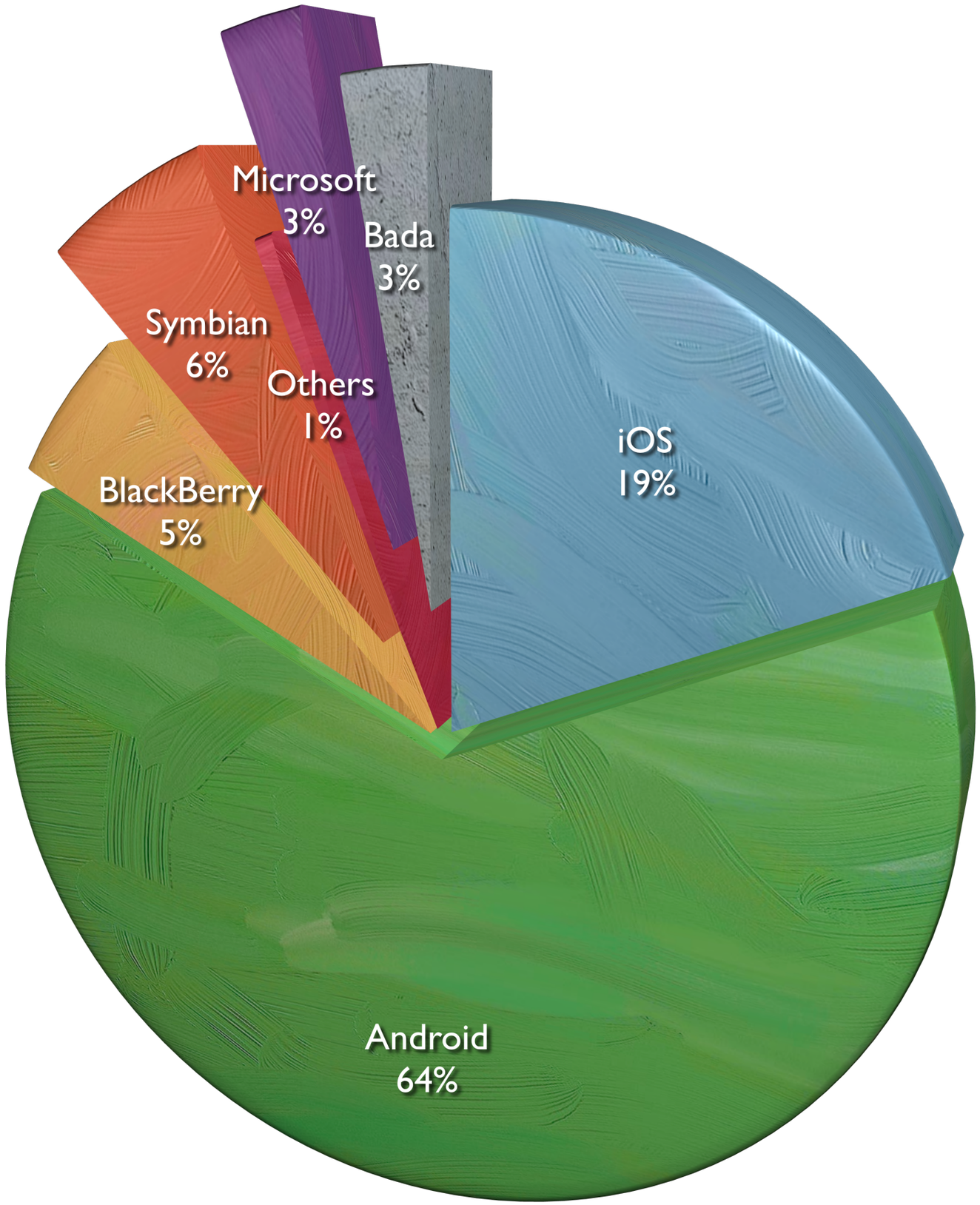
Android Forensics

Dan O'Day
Purdue Cyber Forensics Club
October 8, 2014

Retrieved from http://www.phdcomics.com/comics/archive.php?comicid=820



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

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

A

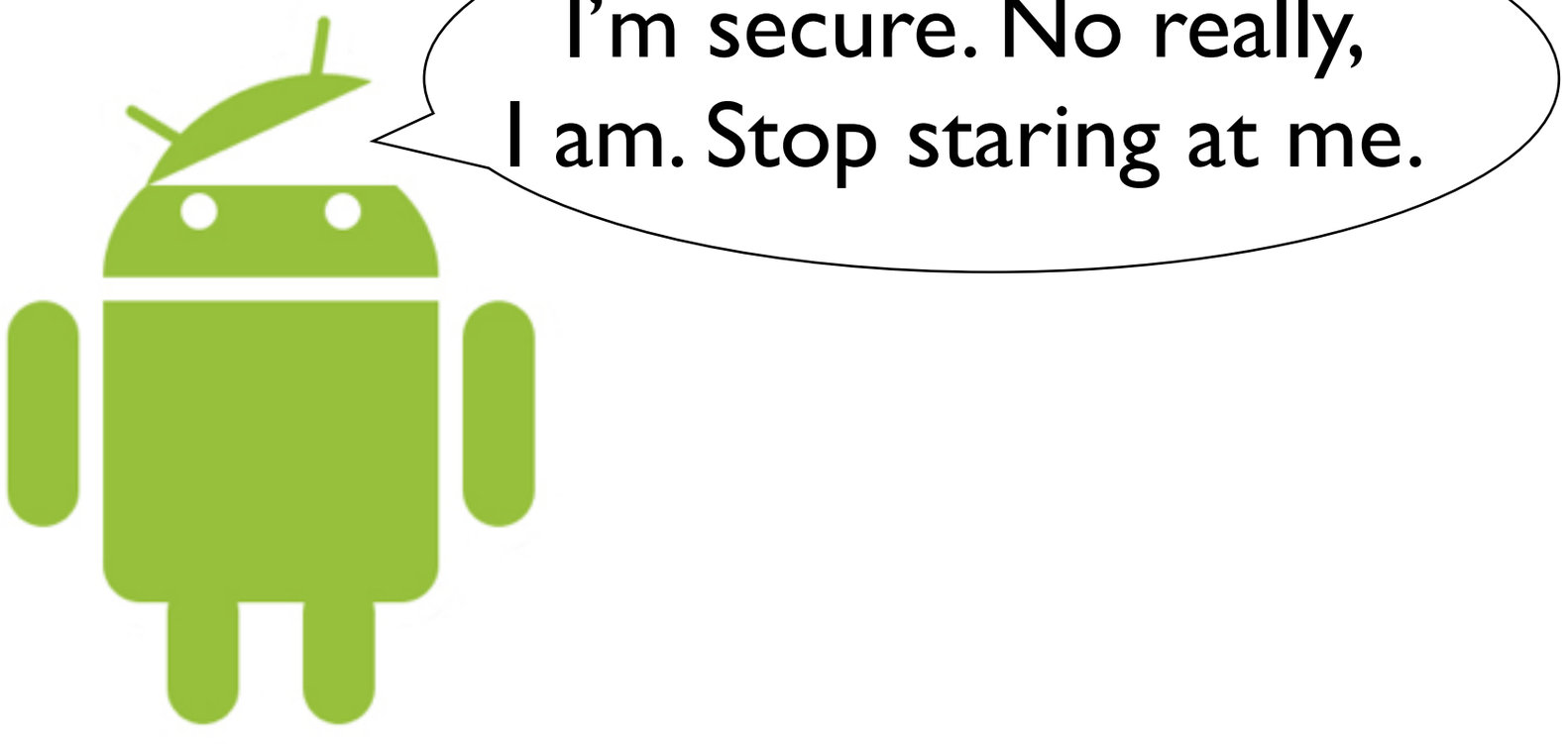
Android is responsible for **92%** of all known mobile malware. An increase from **47%** in 2012...

...a significant threat given more than

1 BILLION

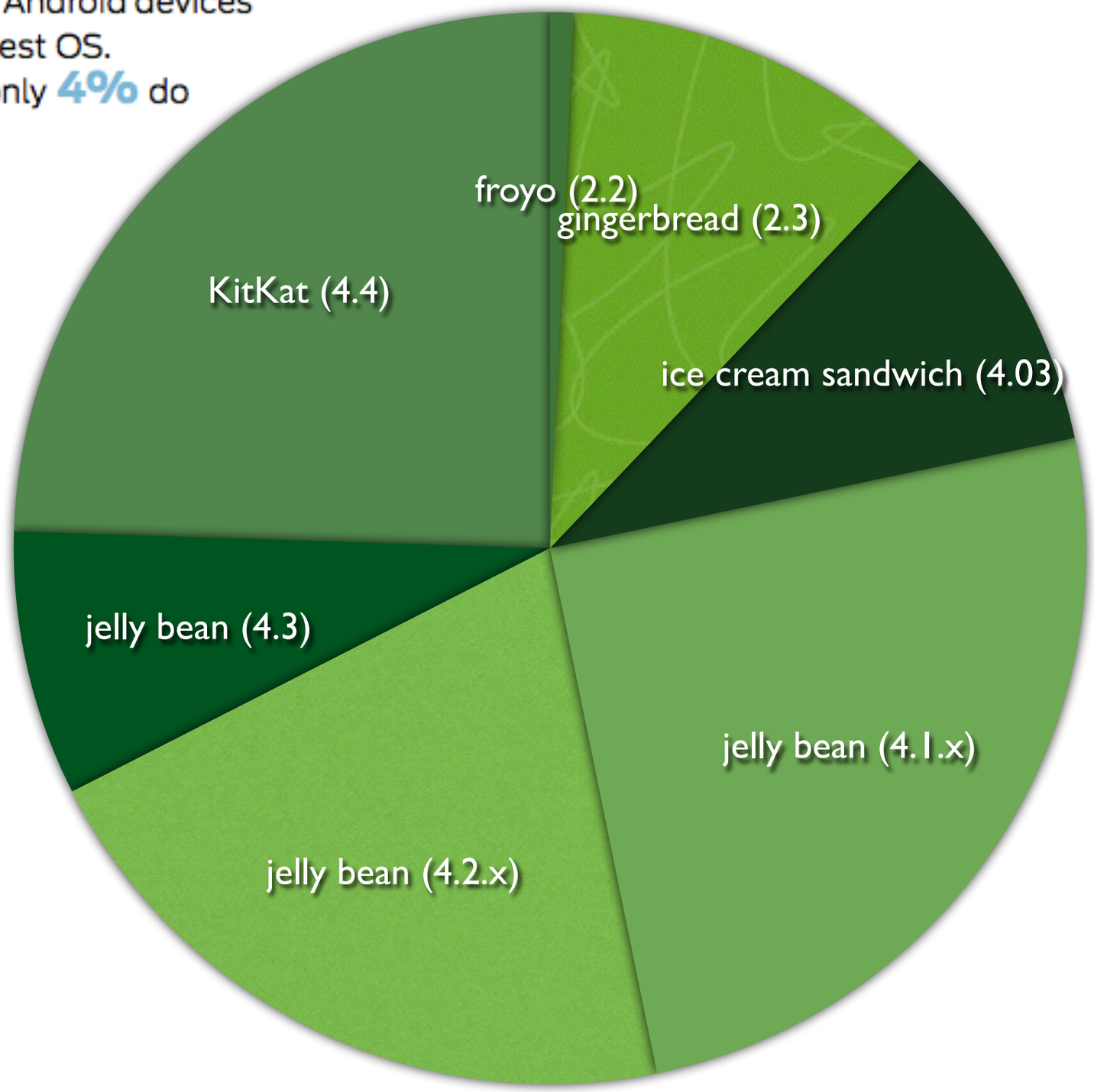
Android-based smart phones are estimated to be shipped in 2017

Source: Canalys Smart Phone Report, June 2013

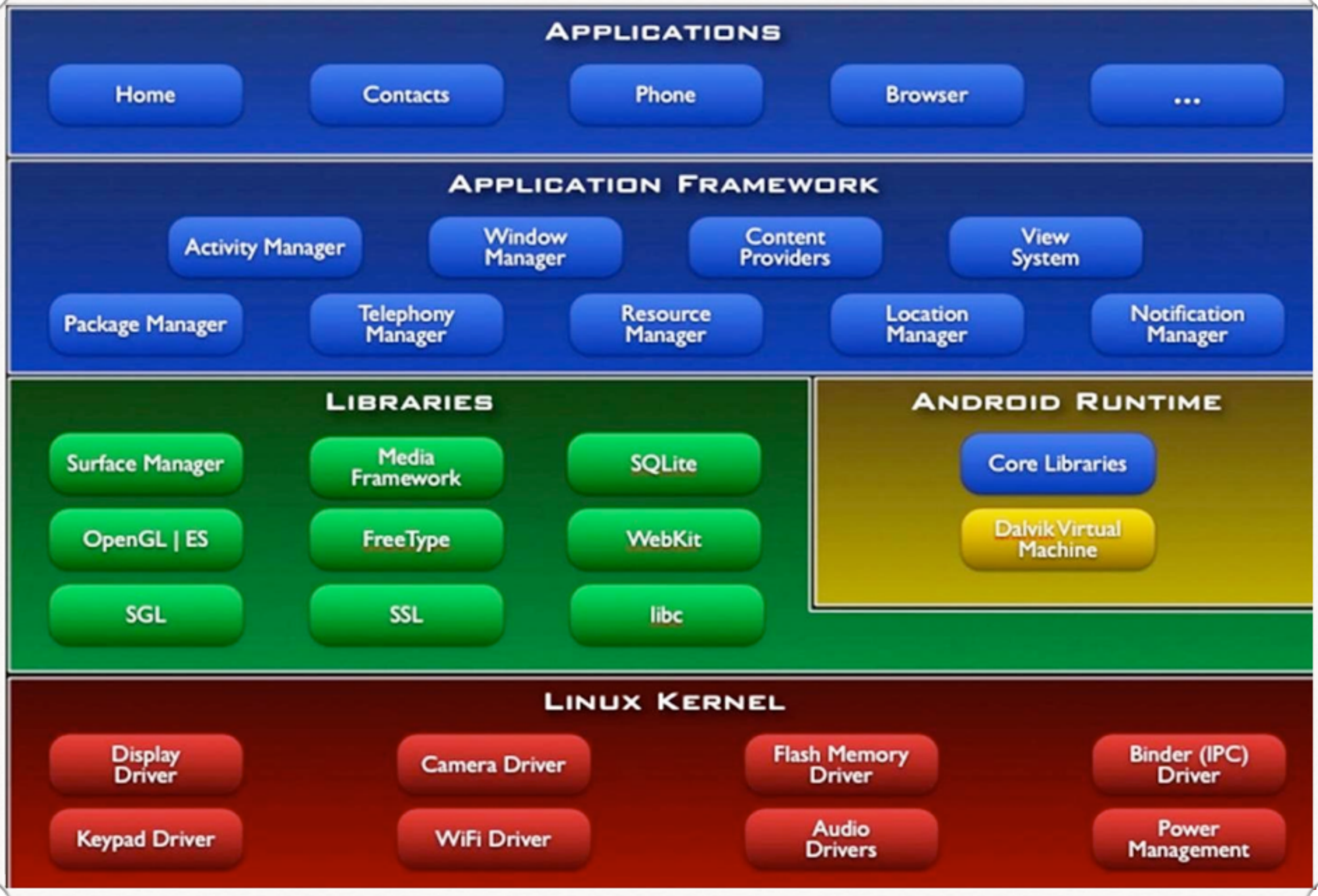


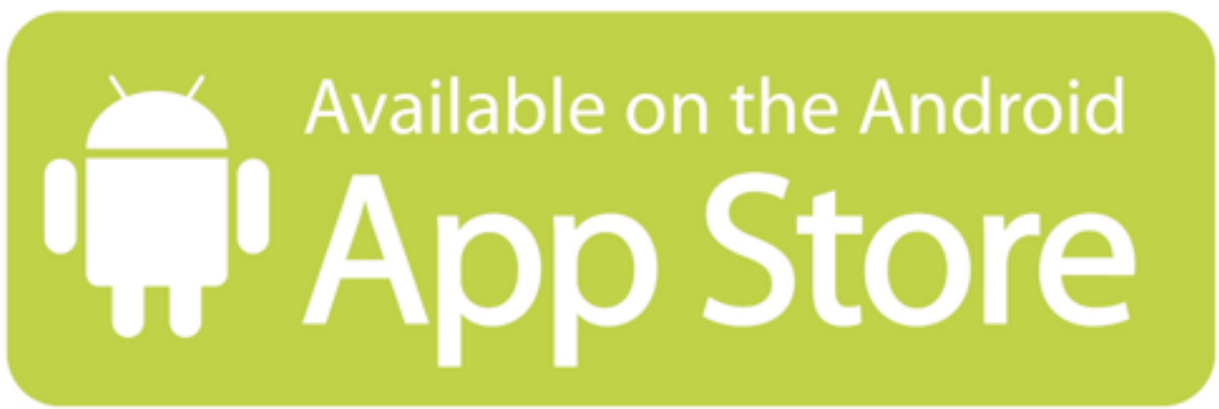
Juniper Networks. (2013). *Third Annual Mobile Threats Report*: March 2012 - March 2013.
Retrieved from http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

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



Based on Play Store statistics as of September 9, 2014

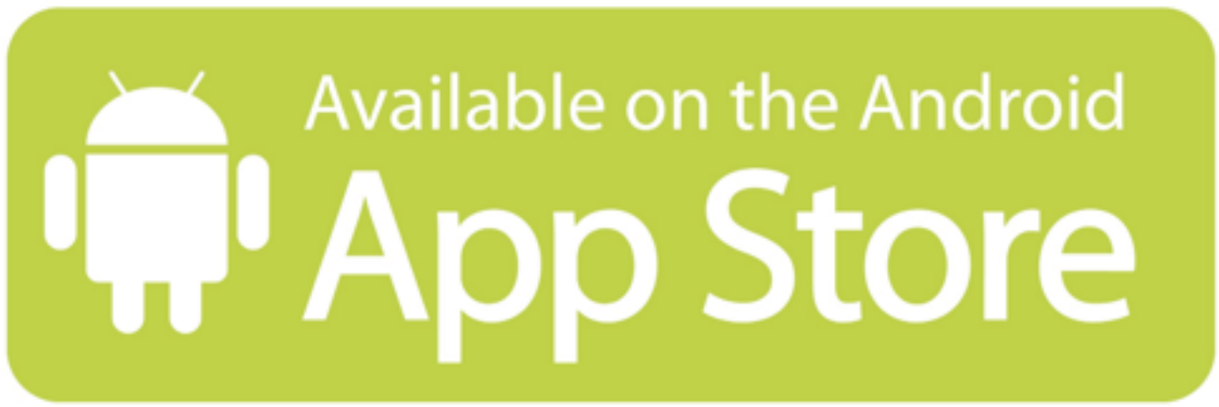

Applications
Home
Contacts
Phone
Browser
...
Application Framework
Activity Manager
Window Manager
Content Providers
View System
Package Manager
Telephony Manager
Resource Manager
Location Manager
Notification Manager
Libraries
Surface Manager
Media Framework
SQLite
OpenGL | ES
FreeType
WebKit
SGL
SSL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



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

Artifacts Commonly of

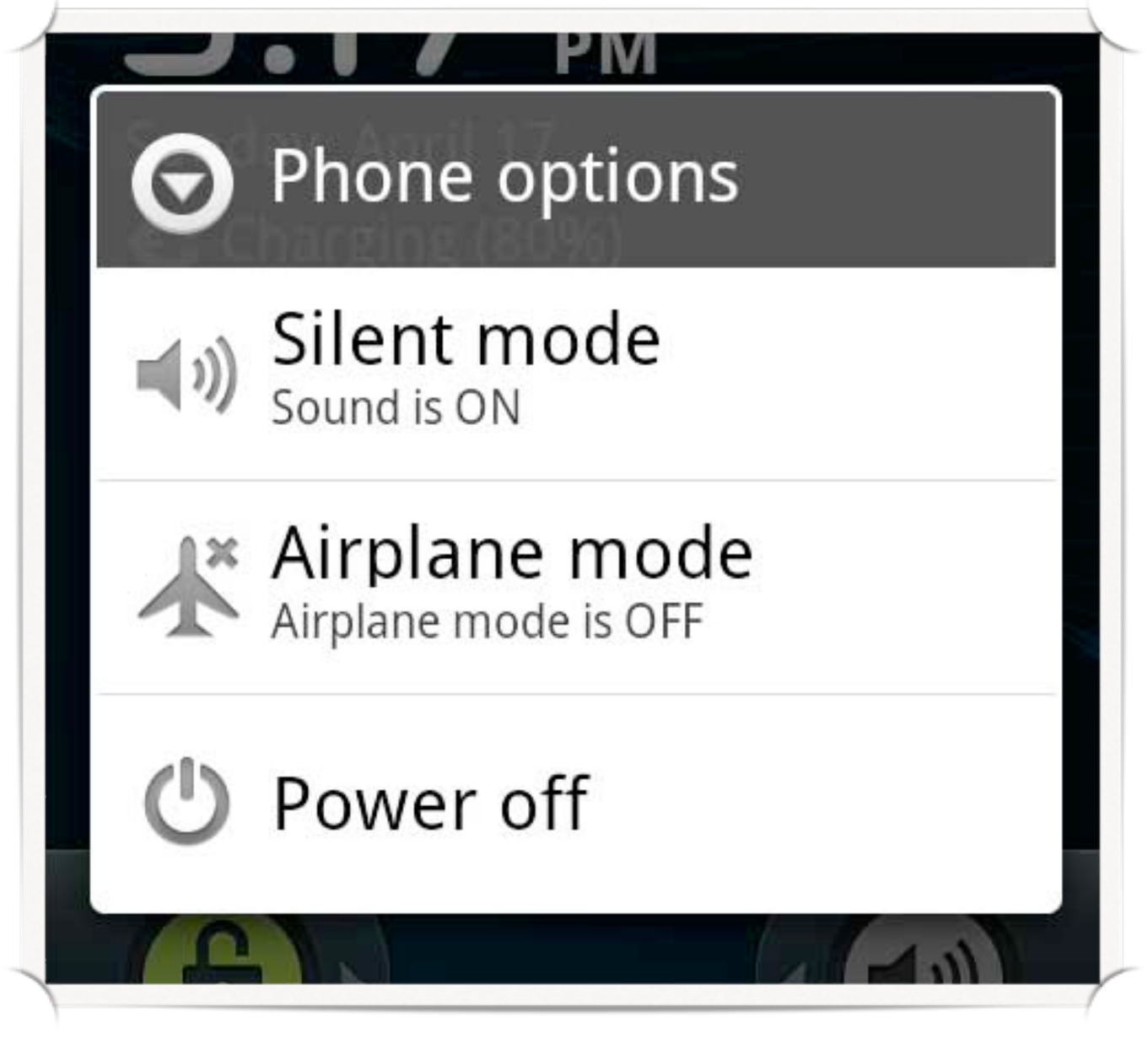
- /data partition
  - app: .apk install bundles
  - dalvik-cache: .dex files ran (compiled .apk files)
  - data: most app data, especially sqlite db's
  - misc: dhcp, bluetooth, wifi, vpn, etc.

Artifacts (continued)

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

Parsing Android

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


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


SanDisk
2GB
MADE IN CHINA

.XRY

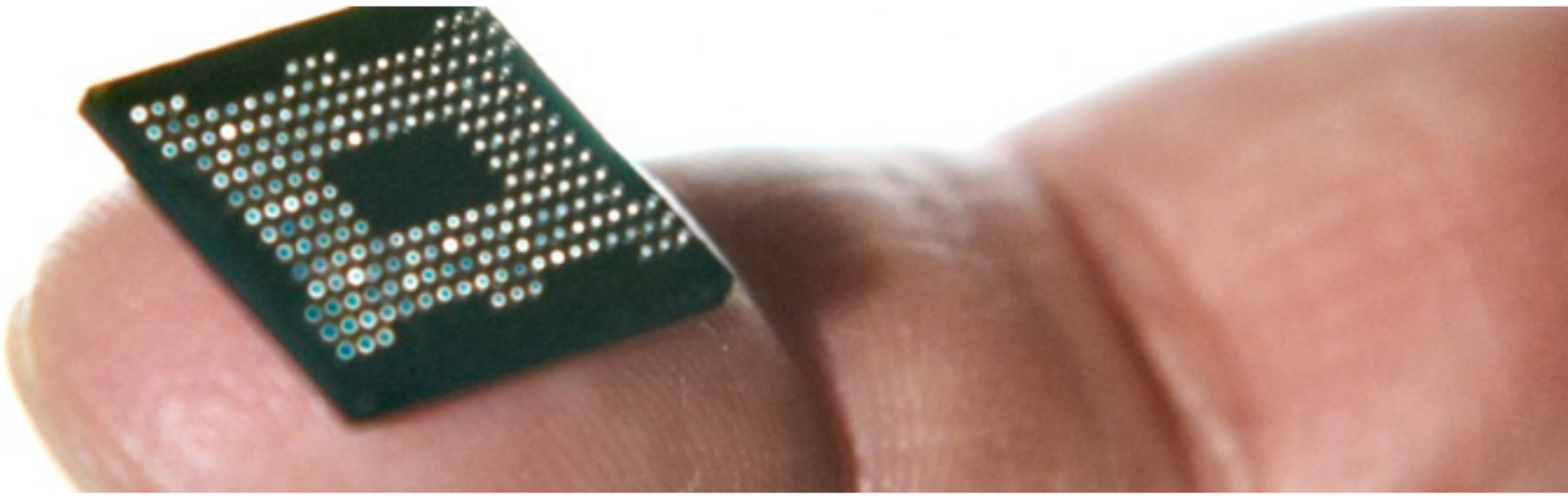
paraben
forensic tools

SECURE VIEW 3
Powered by susteen

VIAFORENSICS
advancing mobile security

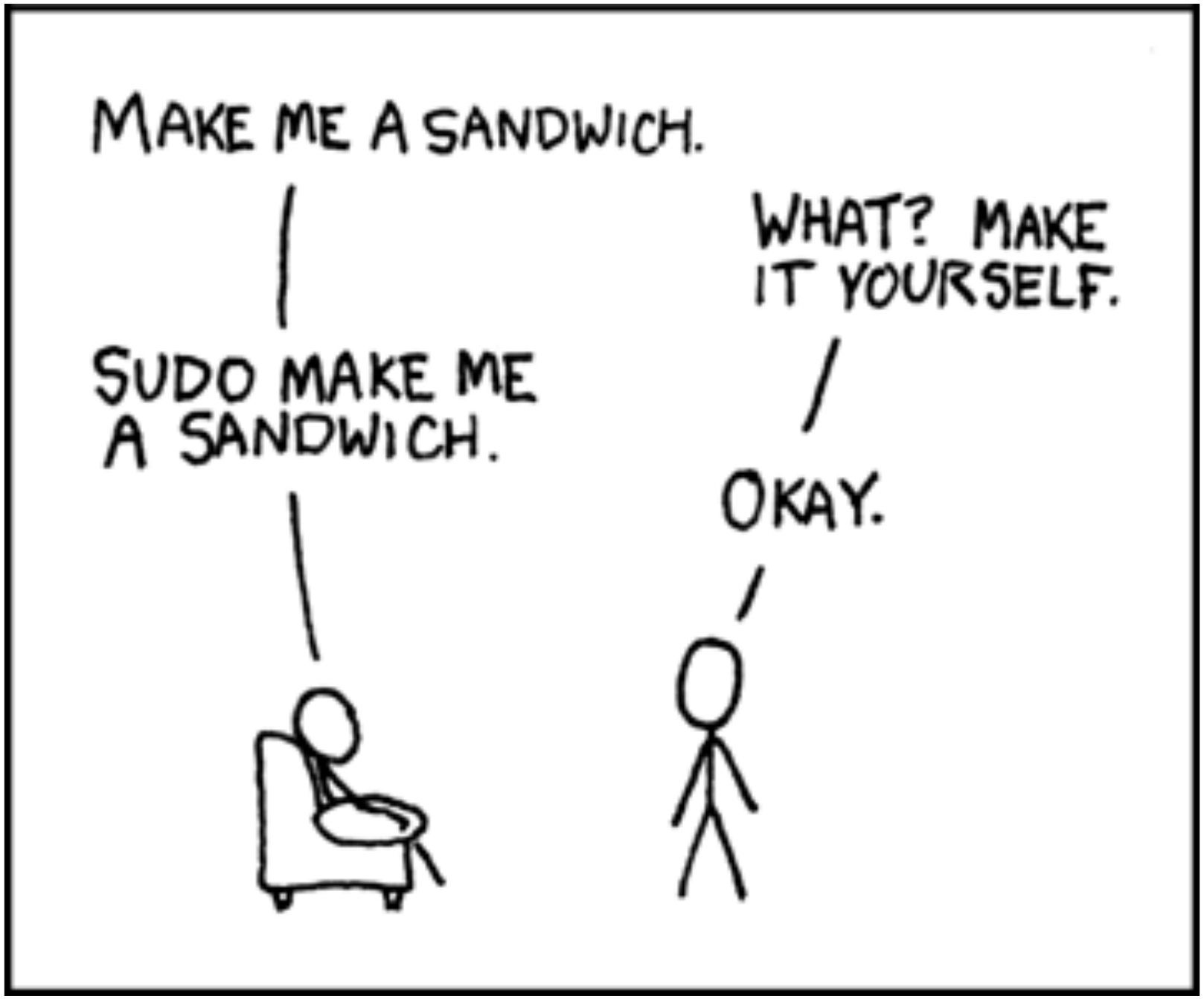

RIFF


ROCKER BOX
WWW.ROCKERDONGLE.COM



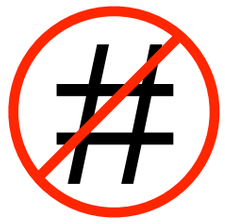
```
root@bt:~/Downloads# cd adt/sdk/platform-tools/
root@bt:~/Downloads/adt/sdk/platform-tools# ./adb devices
List of devices attached
emulator-5554   device

root@bt:~/Downloads/adt/sdk/platform-tools#
```

#


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

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

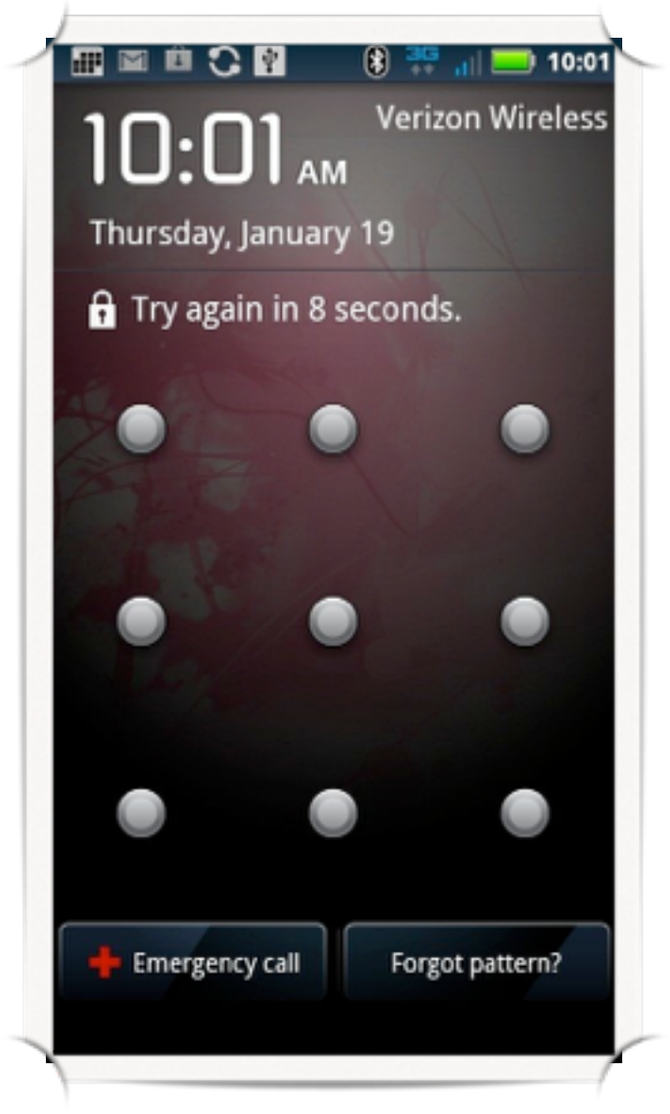
AFLogical

- 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 AFLogicaI-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

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