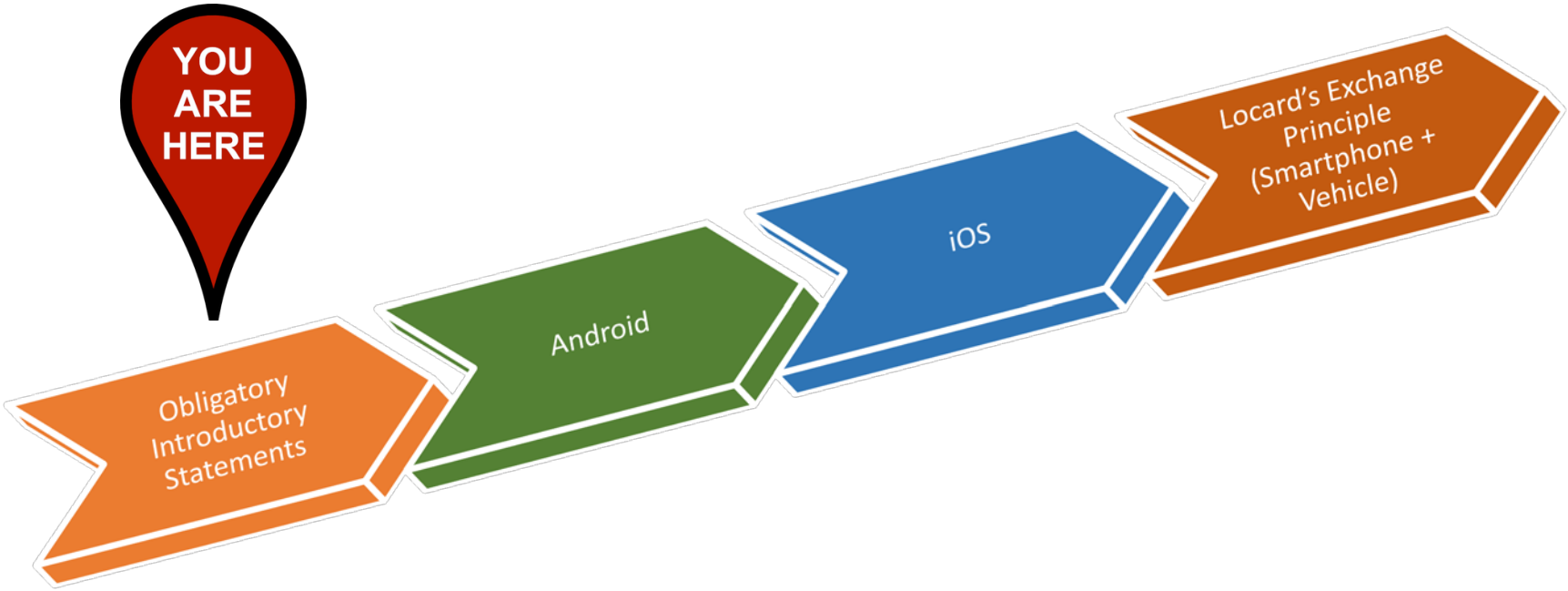
Intro to smartphone forensics

Dan O'Day

Chicago Chapter ACM

September 13, 2017

pwd


YOU ARE HERE
Obligatory Introductory Statements
Android
iOS
Locard's Exchange Principle (Smartphone + Vehicle)

whoami

- KPMG Cyber Security Services => Cyber Response consulting
- Previously:
  - Federal law enforcement
  - Military
  - Instructor (academic and corporate)
- Husband, dad, coder, discusser of interesting things

Disclaimers

This presentation was prepared by Dan O'Day in his personal capacity. The opinions expressed in this presentation are the author's own and do not reflect the view(s) of KPMG.

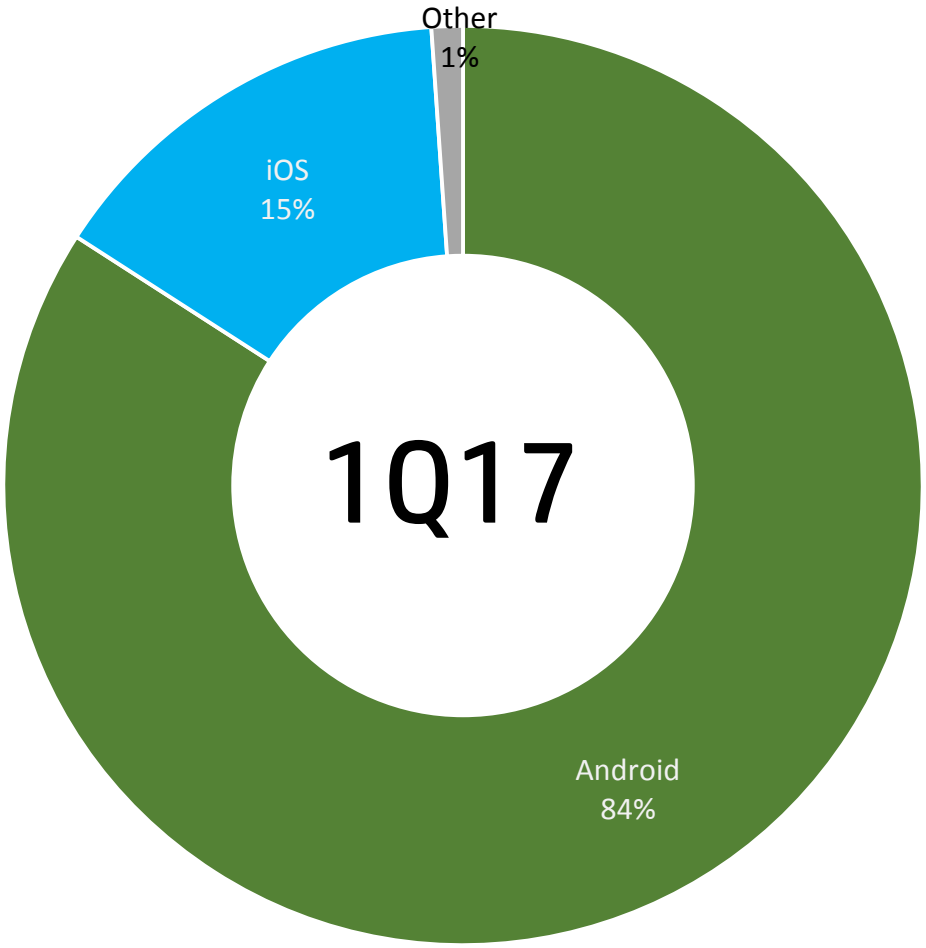
The contents of this presentation are for informational purposes only and are not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem.

Dan O'Day makes no representations as to the accuracy, completeness, currentness, suitability, or validity of any information in this presentation. All information is provided on an as-is basis.

(De)Limitations

- Not enough time to do in-depth tutorial (~4 hours for my full iPhone preservation training – *rushed*)
- This presentation is a mile wide and an inch deep (see http://abstrusegoose.com/272 - *warning*: contains swears)
  - *But* I've tried to create pointers to where you can learn more, and I'm happy to answer questions and correspond

Global mobile OS market share



Retrieved from https://www.gartner.com/newsroom/id/3725117

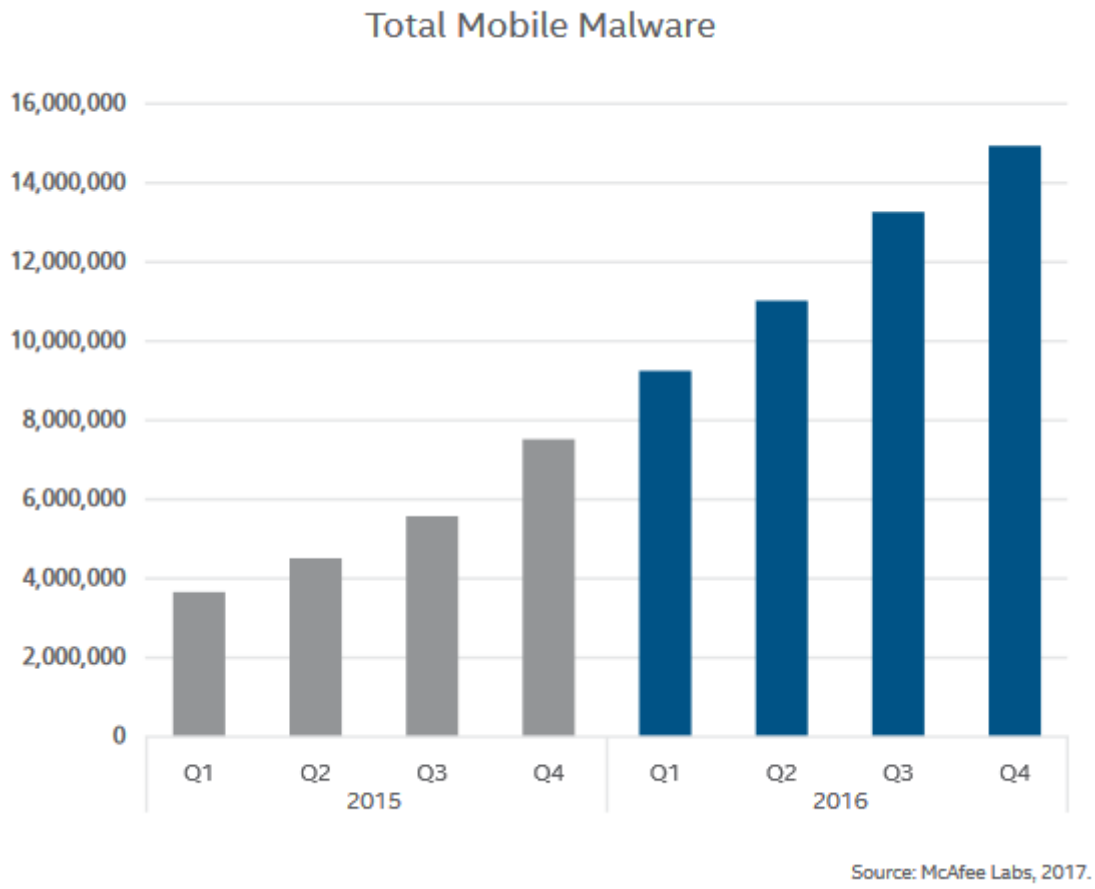
But *sales* data may be misleading

- “Surprise: Google Reveals iOS Market Share Is 65% to 230% Bigger Than We Thought” (Forbes, May 2017)
  - Retrieved from https://www.forbes.com/sites/johnkoetsier/2017/05/18/surprise-google-reveals-apples-ios-market-share-is-65-to-230-bigger-than-we-thought/#78815f165890

Who's interested in mobile data?

- Users
- Organizations
- Developers
- Information security professionals
- Legal system (hence *forensics*)
  - Civil
  - Criminal

InfoSec

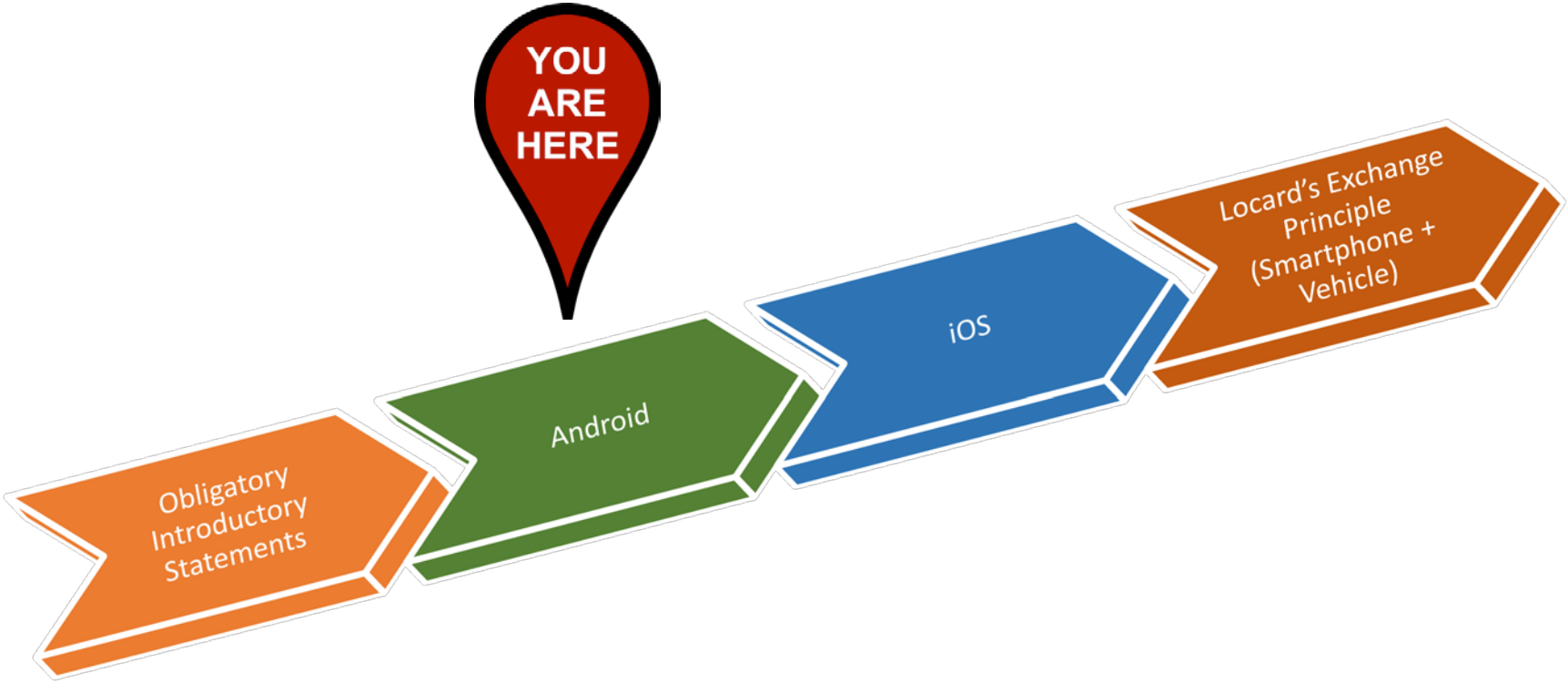


Retrieved from https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

Forensics

- Underwriter for insurance provider took photographs of customer PII and PHI from work computer screen using smartphone
- Recovered deleted photos from cloud backups
- Remediated sensitive information
- Legal action (injunctive relief, damages)

pwd

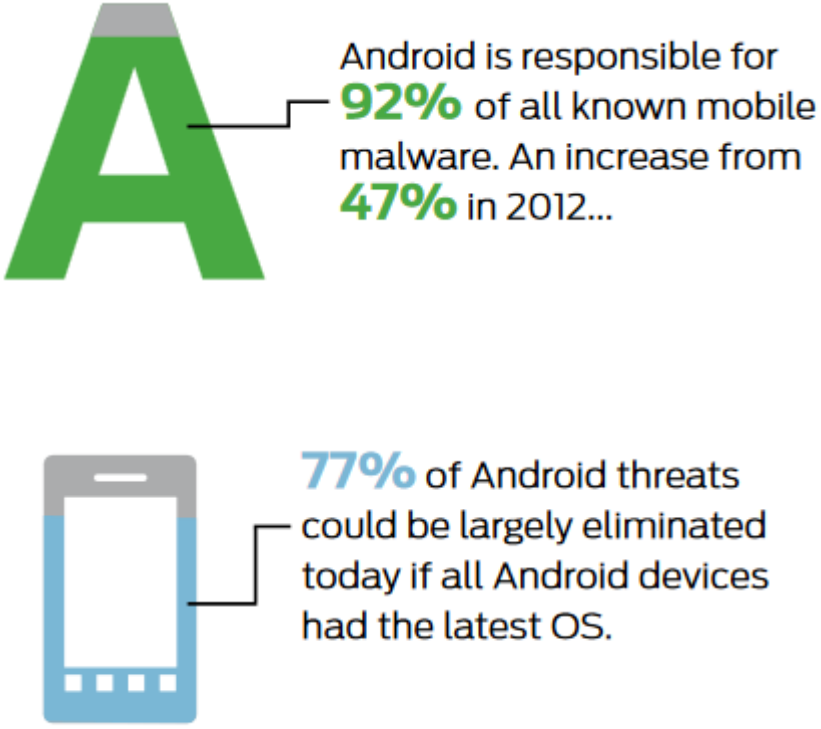

YOU ARE HERE
Obligatory Introductory Statements
Android
iOS
Locard's Exchange Principle (Smartphone + Vehicle)

ANDROID

Why Android?

- F/OSS
- No central point of failure
- No single industry player can control others' innovations
- Widest implementation possible

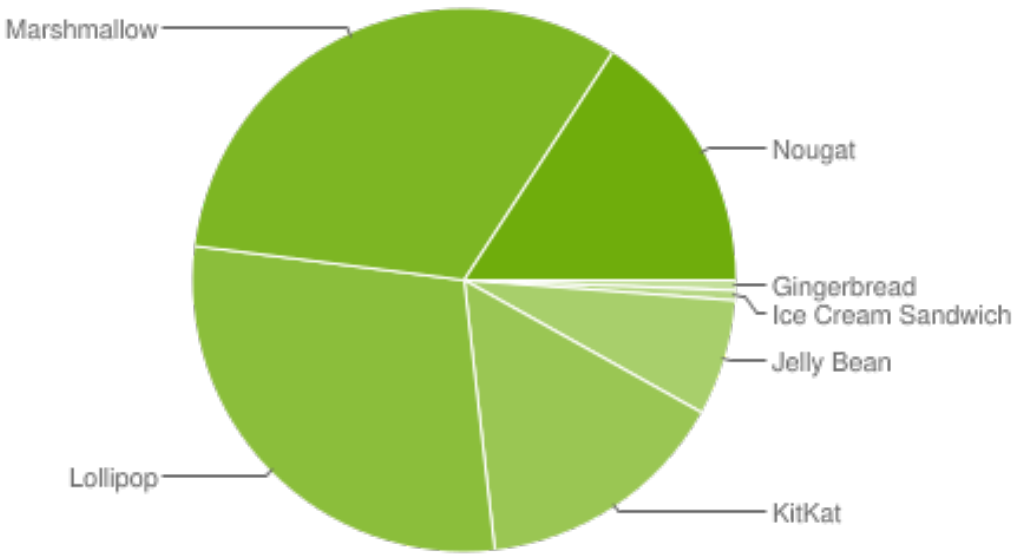
But…



This information is a little dated, but still insightful and generally still true today (even if the numbers are a little off).
Retrieved from https://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

Android version market share distribution

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.6%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.6%
4.1.x	Jelly Bean	16	2.4%
4.2.x		17	3.5%
4.3		18	1.0%
4.4	KitKat	19	15.1%
5.0	Lollipop	21	7.1%
5.1		22	21.7%
6.0	Marshmallow	23	32.2%
7.0	Nougat	24	14.2%
7.1		25	1.6%

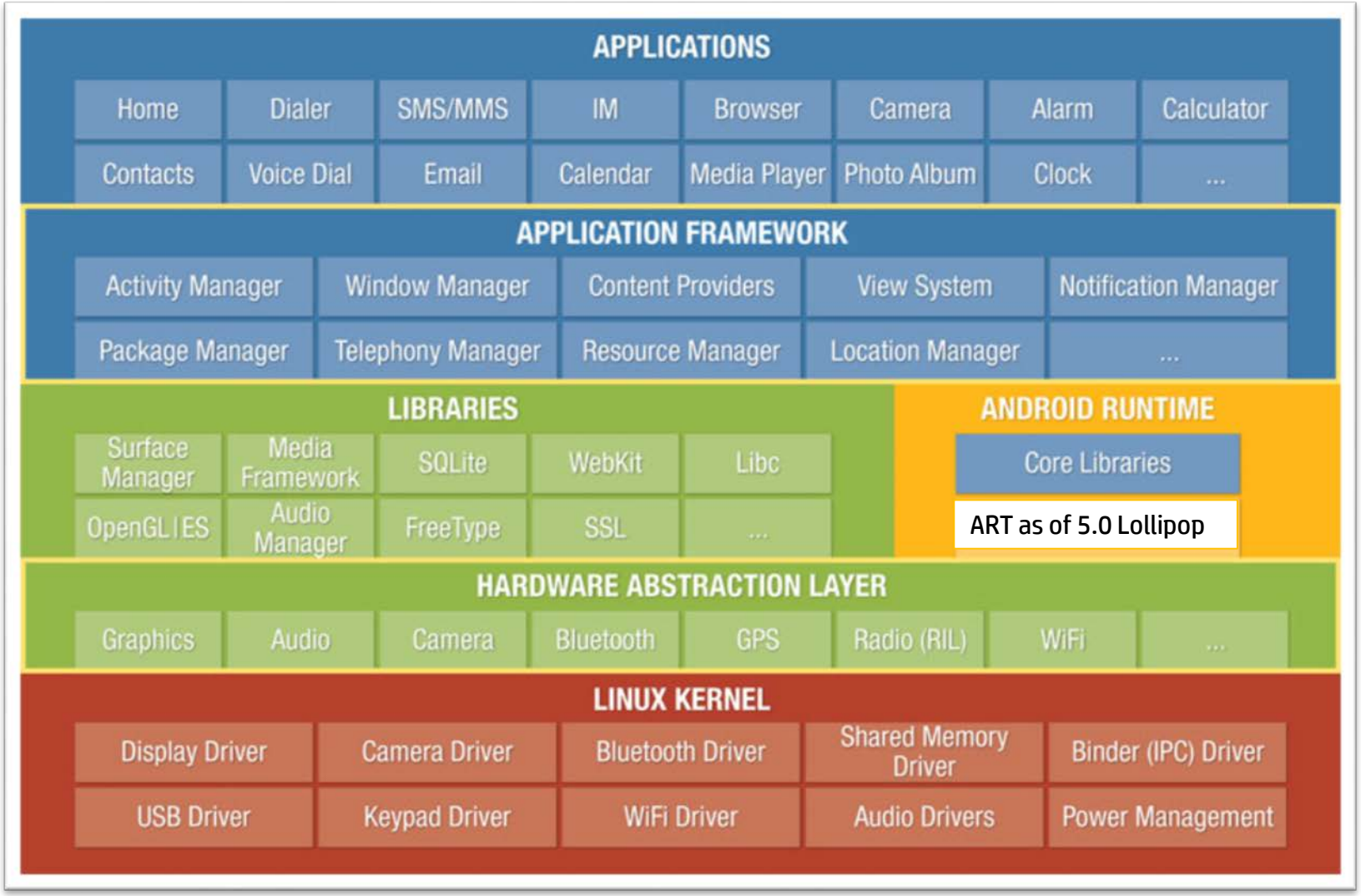


Data collected during a 7-day period ending on September 11, 2017.

Any versions with less than 0.1% distribution are not shown.

Retrieved from https://developer.android.com/about/dashboards/index.html

Android architecture



Retrieved from https://manifestsecurity.com/android-application-security-part-2/

Types of Android data

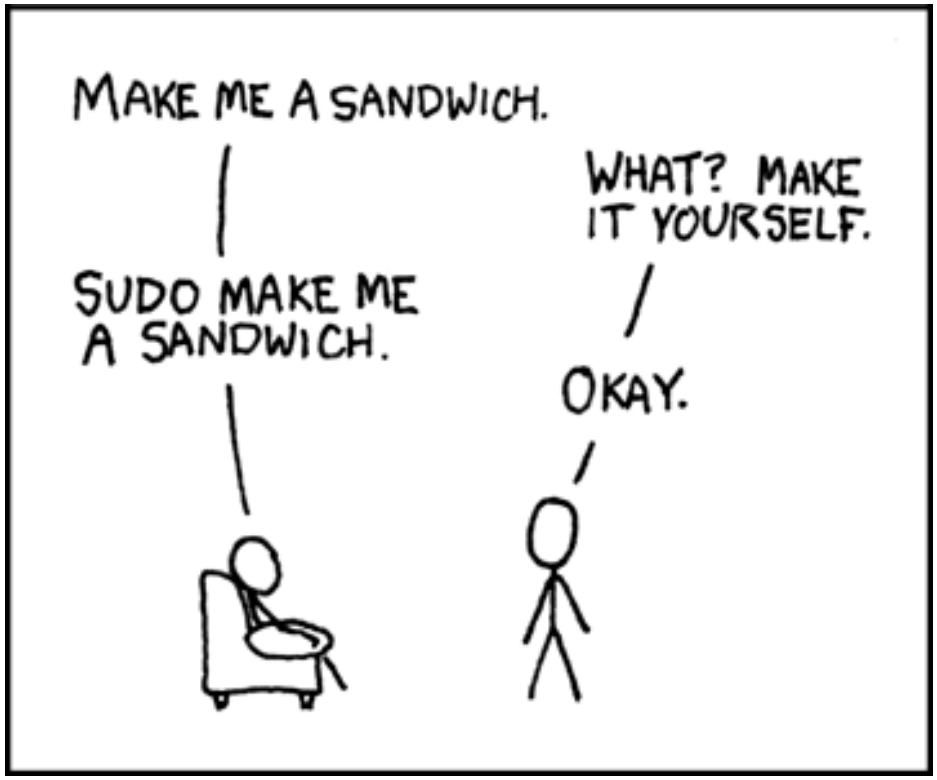
- Preferences (key/value)
- Files
- SQLite databases
- Cloud storage
- Application binaries

Acquiring Android data

USB debugging

- Developer menu
- Sometimes on by default
- Required to connect over ADB

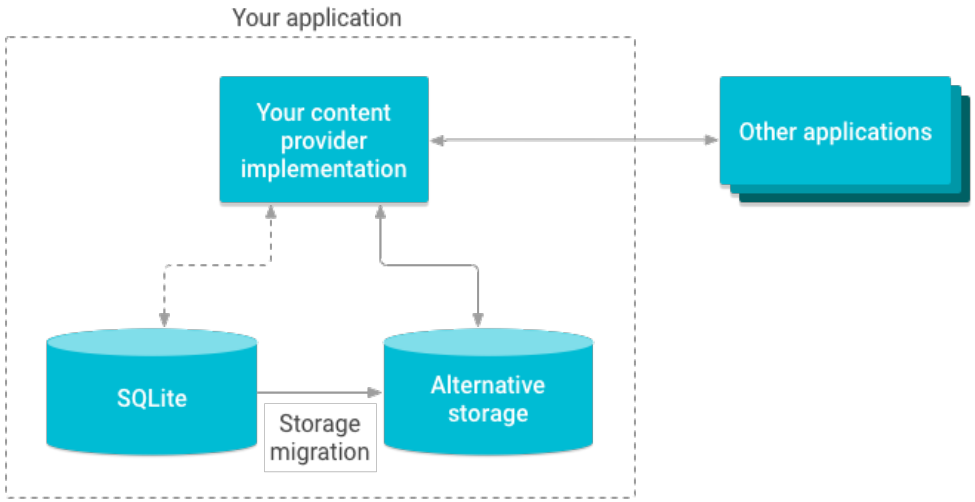
:# “Rooting” Android devices



Retrieved from https://xkcd.com/149/

Logical acquisitions

- Android Debug Bridge (ADB)
- Content Providers (AndroidManifest.xml permissions)
  - Check out NowSecure's AFLogical: https://github.com/nowsecure/android-forensics
- Backup services
- Screen capture
- Got root?
  - File system access



Retrieved from https://developer.android.com/guide/topics/providers/content-providers.html

Physical acquisitions

- Raw disk access
  - Opens possibility of acquiring unallocated data
  - NAND flash chips
  - Methods:
    - Get root!
    - Bootloader (locked/unlocked)
    - Recovery partition
    - Service mode
    - JTAG
    - BGA chip-off
- But encryption....

Don’t forget the microSD card!

Danger!

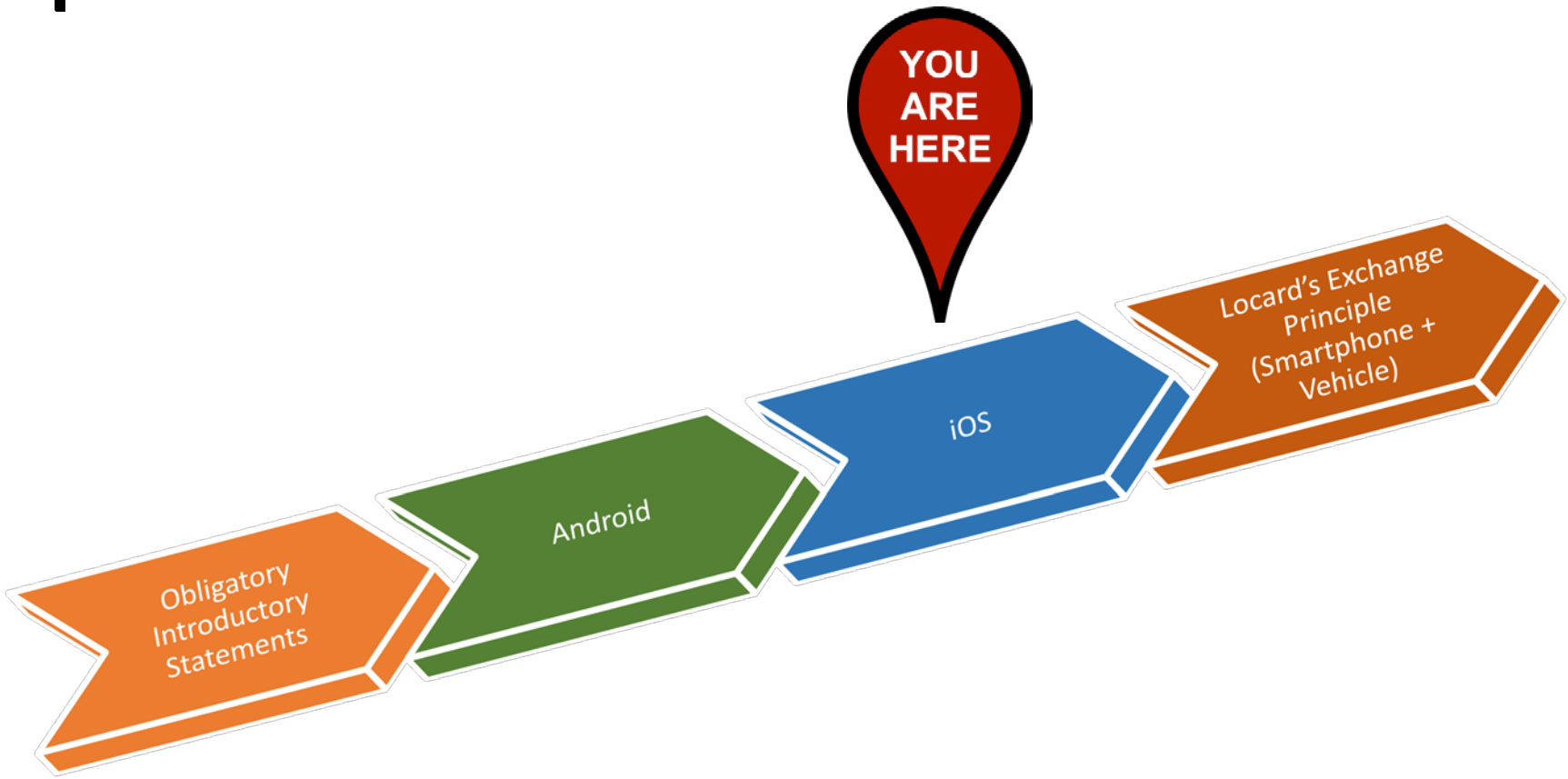
- Device passcodes / gestures (https://gist.github.com/danzek/f9416b1404570754b10f)
- Remote device access (airplane mode is your friend)
- Mobile Device Management (MDM) solutions may create additional obstacles
- Encryption is challenging
- Don’t forget screen capture

Screen capture evidence

“[Deputy Prosecuting Attorney Mark] Watson at trial presented evidence from Google Latitude, which traced Martinez's cellphone to the Austgen business the day she went missing. The phone later that day was traced to the Majestic Star Casino in Gary.”

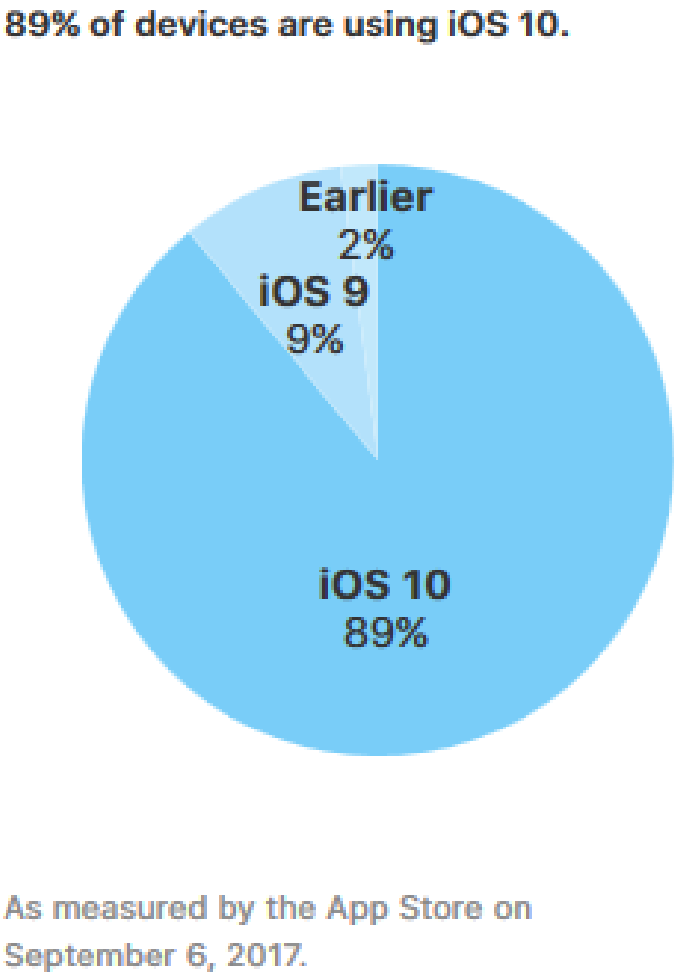
Retrieved from http://www.nwitimes.com/news/local/lake/update-convicted-murderer-in-austgen-slaying-silent-at-sentencing/article_1ea18ff6-771c-5f5a-8524-f5a0eaae0e25.html

pwd


YOU ARE HERE
Obligatory Introductory Statements
Android
iOS
Locard's Exchange Principle (Smartphone + Vehicle)


iOS

iOS version market share distribution

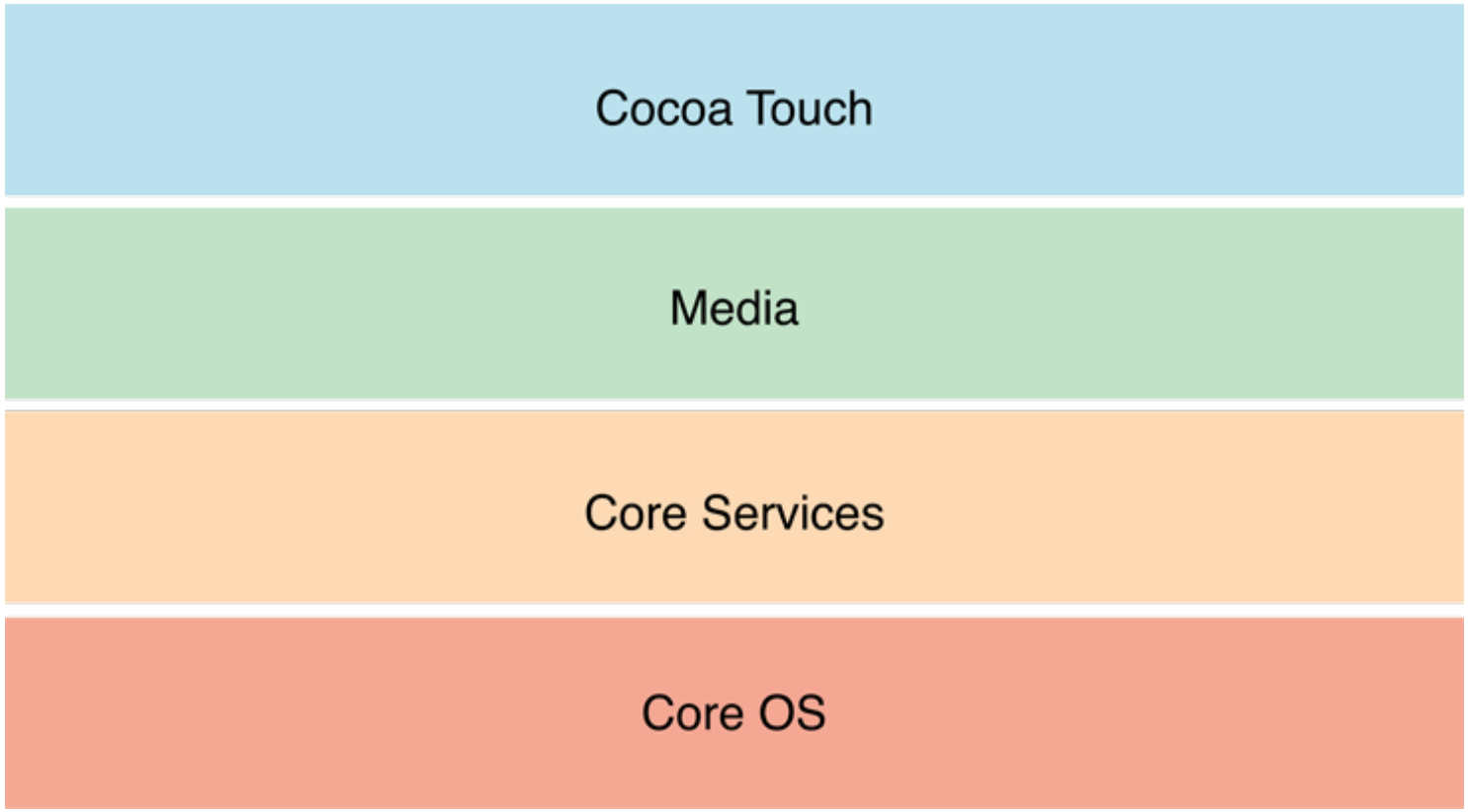


Retrieved from https://developer.apple.com/support/app-store/

Types of iOS data

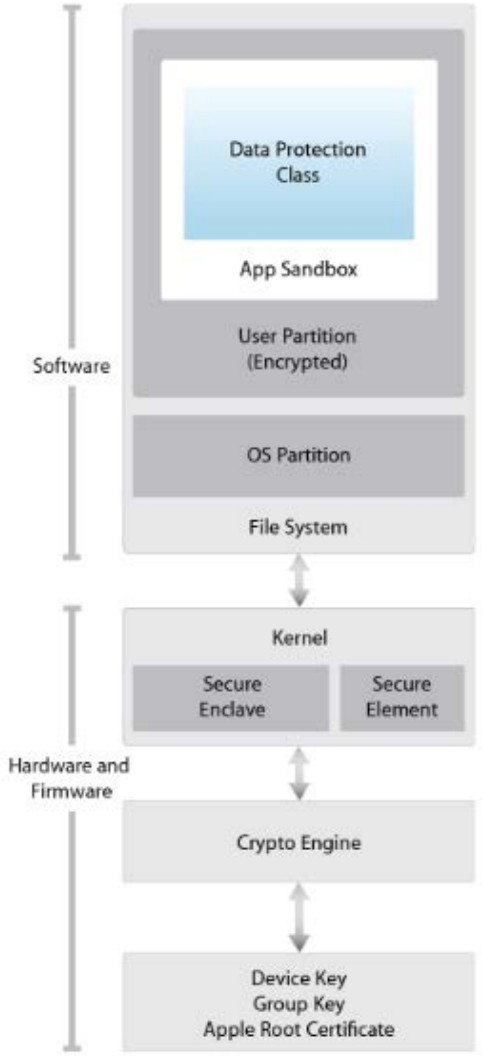
- Property lists
- Files
- SQLite databases
- Cloud storage
- Application binaries

iOS architecture



Retrieved from
https://developer.apple.com/library/content/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/Introduction/Introduction.html

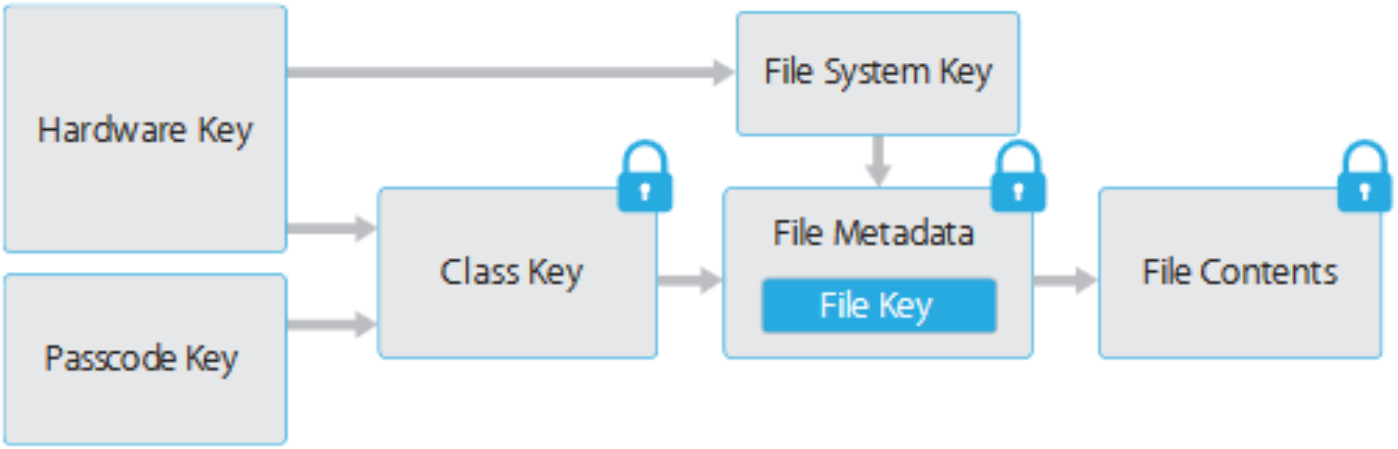
iOS architecture (continued)



- Encryption and Data Protection continue to work *even in the event of kernel compromise* (e.g., "jailbreaking")
- Dedicated AES-256 crypto engine built into DMA path between flash storage and main system memory
- Keys fused into processors during manufacturing

Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Data Protection



Data protection class key

Class A	Complete Protection	(NSFileProtectionComplete)
Class B	Protected Unless Open	(NSFileProtectionCompleteUnlessOpen)
Class C	Protected Until First User Authentication	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Class D	No Protection	(NSFileProtectionNone)

Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Keychain

- Encrypted SQLite database
- Items can be shared between any apps *from the same developer*
- Also have data protection classes (when unlocked, while locked, after first unlock, always, passcode-enabled, *this device only* / non-migratory)

Keychain (continued)

For Keychain items created by iOS, the following class protections are enforced:

Item	Accessible
Wi-Fi passwords	After first unlock
Mail accounts	After first unlock
Exchange accounts	After first unlock
VPN passwords	After first unlock
LDAP, CalDAV, CardDAV	After first unlock
Social network account tokens	After first unlock
Handoff advertisement encryption keys	After first unlock
iCloud token	After first unlock
Home sharing password	When unlocked
Find My iPhone token	Always
Voicemail	Always
iTunes backup	When unlocked, non-migratory
Safari passwords	When unlocked
Safari bookmarks	When unlocked
VPN certificates	Always, non-migratory
Bluetooth® keys	Always, non-migratory
Apple Push Notification service token	Always, non-migratory
iCloud certificates and private key	Always, non-migratory
iMessage keys	Always, non-migratory
Certificates and private keys installed by Configuration Profile	Always, non-migratory
SIM PIN	Always, non-migratory

Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Keybags

- **User** (tied to passcode)
- **Device** (wraps per-file keys, usually same as user)
- **Backup** (iTunes Backup)
- **Escrow** (iTunes sync and MDM)
- **iCloud Backup**

“The [backup] keybag is protected with the password set in iTunes, run through 10 million iterations of PBKDF2. Despite this large iteration count, there’s no tie to a specific device, and therefore a brute-force attack parallelized across many computers could theoretically be attempted on the backup keybag. This threat can be mitigated with a sufficiently strong password.”

Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

iOS access challenges

- Data Protection and Keychain classes
  - Mitigation: acquire encrypted backups (only partial solution)
- Device passcode / Touch ID / Face ID
- iTunes Backup password
- Activation lock
  - Need iCloud credentials
  - Possible mitigation: companies should require managed devices to use company email for iCloud account so admins can reset creds

Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Crack passcode / Touch/Face ID?

bypass passcode ios 10

About 1,430,000 results

FILTER

iOS 10 Lockscreen Bypass Backdoor! Access Photos & Contacts

EverythingApplePro 519K views • 10 months ago

How To **Bypass iOS 10** Lockscreen & Access Photos, Contact Info. Works on **iOS** 10.1 & 10.0.3 on iPhone, iPad & iPod.

4K

How to Unlock ANY iPhone Without Passcode Access Photos, Contacts & More iOS 9 /10 - 10.2

iDeviceHelp 1.2M views • 9 months ago

Ad- iSkysoft Data Recovery for Mac The easiest, fastest and safest software to recover data from Mac hard drive and external ...

BYPASS iOS 10 lock screen password/passcode on any iPhone, iPad, iPod touch !! New method found!

XxWastednowxX • 45K views • 10 months ago

This is a quick tutorial on how **bypass** the **iOS 10 password** lock screen.

Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Cracking iTunes Backup password

- Manifest.plist file can be used to crack backup password
- Brute force supported by :
  - Passware (commercial)
  - Hashcat (F/OSS, see http://irq5.io/2017/03/07/cracking-itunes-backup-passwords-with-hashcat/)

Logical acquisitions

- iTunes Backup (encrypted w/known password)
- Tools built using libimobiledevice and related libraries
  - See http://www.libimobiledevice.org/
  - See https://github.com/libimobiledevice
- Proprietary methods

iOS physical access challenges

- Secure boot chain: each step of startup process verified in cryptographically-signed “chain of trust”
- System Software Authorization prevents downgrades
- Encryption, Data Protection, Keychain
- iOS Security Guide not published for iOS 11 yet
  - https://www.apple.com/business/docs/iOS_Security_Guide.pdf
- “Jailbreaks” must overcome all of these obstacles

“Jailbreaking” iOS devices

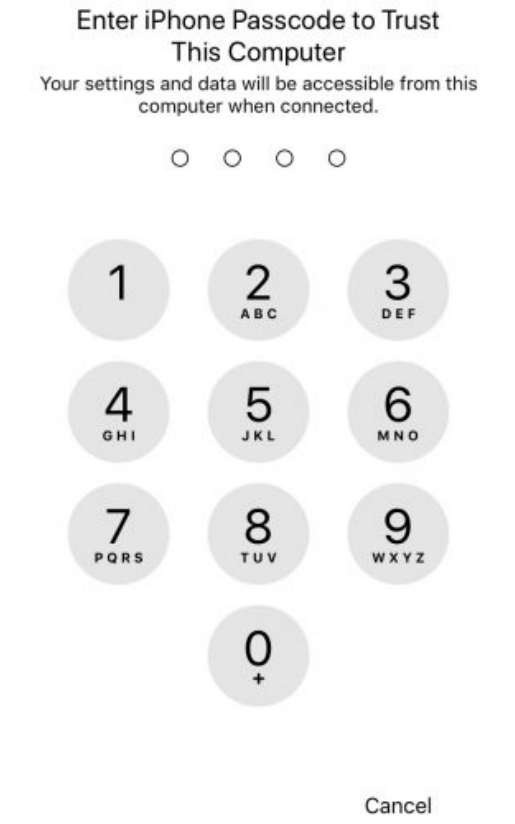
- Patch kernel (`/private/etc/fstab`)
  - Must gain write access to system slice and write new firmware (IPSW’s available at http://www.iclarified.com/750/where-to-download-iphone-firmware-files-from)
  - Patch or bypass checks for signed code in chain of trust
  - Exploits target boot ROM or userland
- Jailbreak types
  - **Untethered** – device reboots and *kernel self-patches*
  - **Tethered** – device needs computer to assist with kernel patching upon reboot *or the device won’t boot at all*
  - **Semi-tethered** – device needs computer to assist with kernel patching upon reboot *in order to run modified code*

iOS jailbreak status

- Latest jailbreak: iOS 10.2 (yalu102 / PPJailbreak)
  - https://github.com/kpwn/yalu102
  - http://ghost.25pp.com/soft/pppc_setup/pphelper_5.1.5.2142_ios10_course_pc5_1487824936_Setup.exe
- Stay current on latest jailbreaks
  - https://www.theiphonewiki.com/wiki/Jailbreak

New iOS 11 challenges

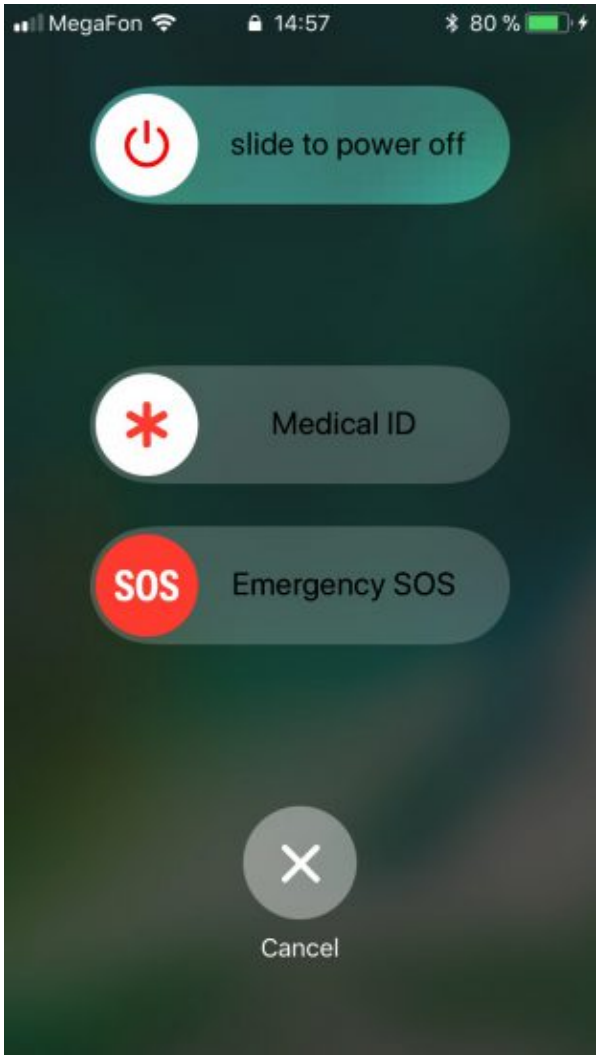
- Establishing trust with a computer now requires a passcode



Retrieved from https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/

New iOS 11 challenges (continued)

- S.O.S. Mode



Retrieved from https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/

Unlock device using pairing record

- Location
  - **Windows:** %ProgramData%\Apple\Lockdown
  - **Mac:** /var/db/lockdown
- Pairing records remain valid even if passcode changed
- Become invalid upon device reboot / shutdown

New iOS 11 challenges (continued)

- Notifications no longer stored in backups
- 2FA pushed harder

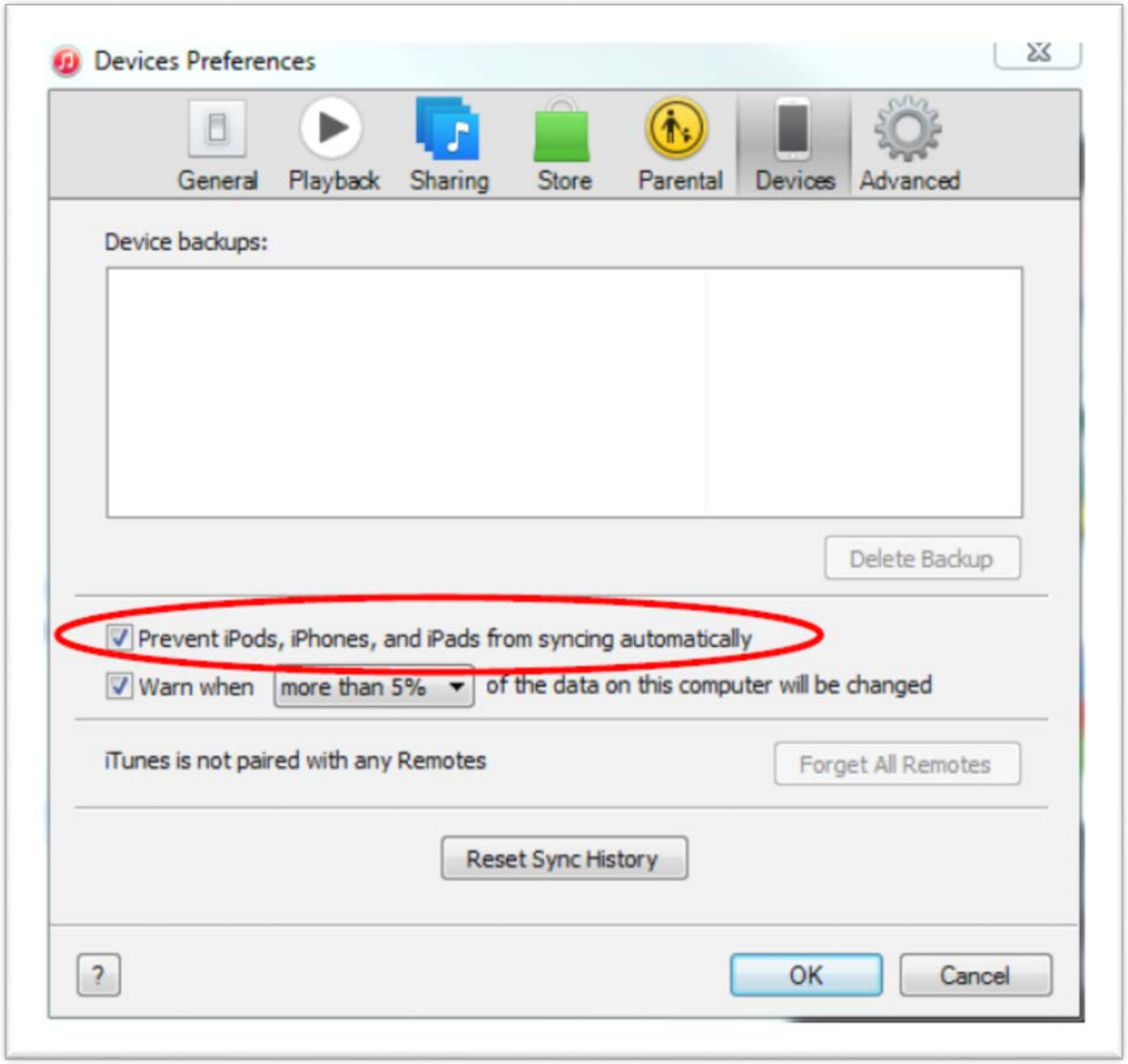
Retrieved from https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/

Warning!

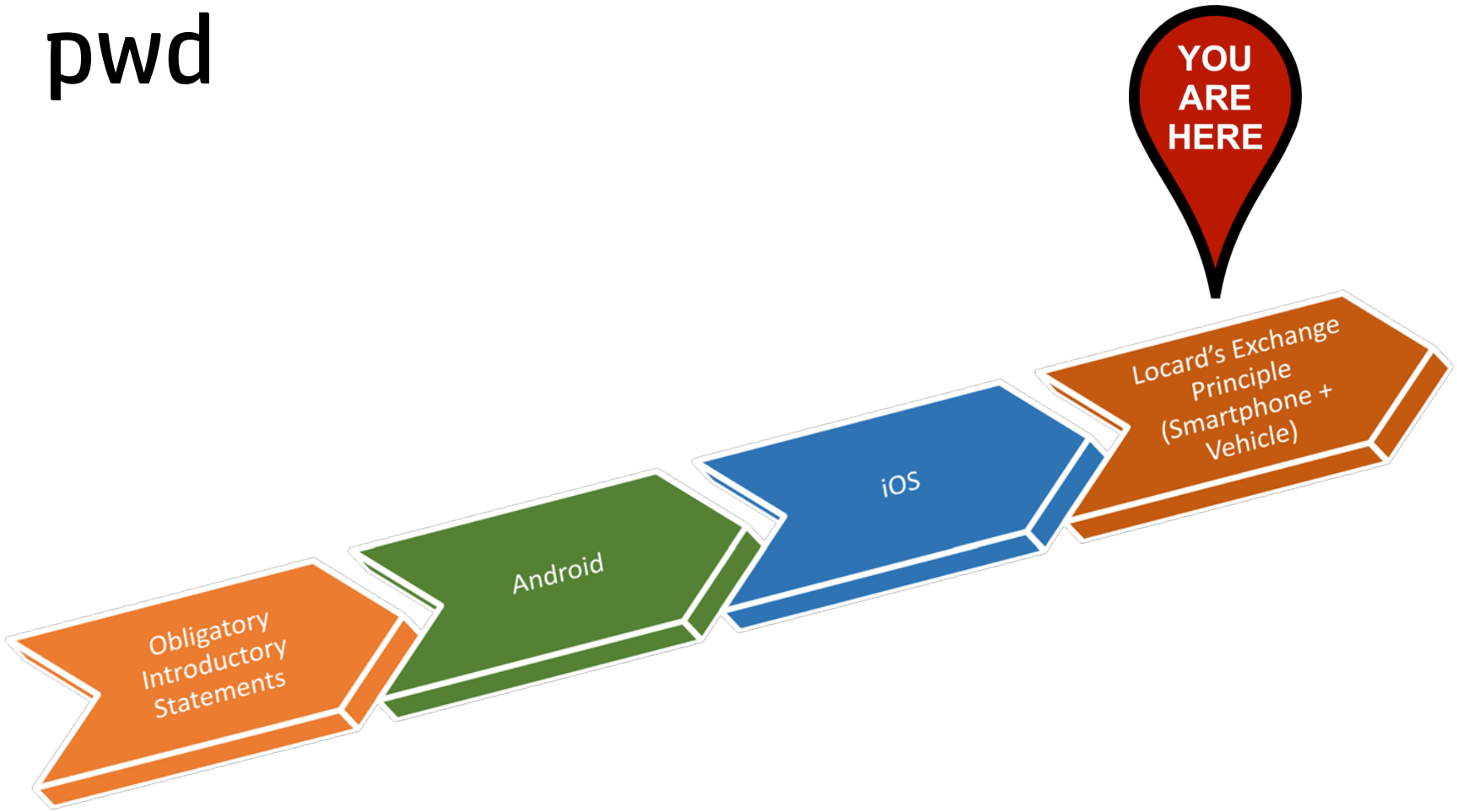
- Remote Wipe and Lost Mode (airplane mode is still your friend)
- Mobile Device Management (MDM) solutions may create additional obstacles here, too
- Screen capture still applies

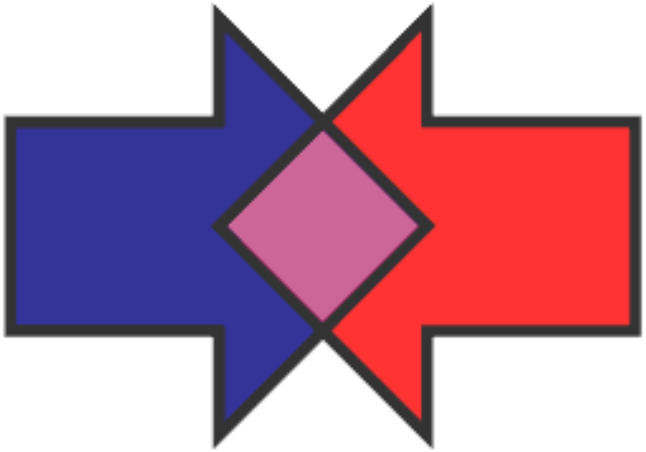
+

Warning!


Devices Preferences
General
Playback
Sharing
Store
Parental
Devices
Advanced
Device backups:
Delete Backup
Prevent iPods, iPhones, and iPads from syncing automatically
Warn when
more than 5%
of the data on this computer will be changed
iTunes is not paired with any Remotes
Forget All Remotes
Reset Sync History
?
OK
Cancel

pwd


YOU ARE HERE
Obligatory Introductory Statements
Android
iOS
Locard's Exchange Principle (Smartphone + Vehicle)



THE LOCARD EXCHANGE

"...contact between two items will result in an exchange."

Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 16 (3d ed., 2011).

People sync phones with vehicles

- People even do this in rental cars!

Data potentially tracked by vehicle infotainment/telematics

- For each event, tracks timestamp and latitude/longitude
  - Door open/close
  - Gear shift
  - Vehicle engine start/stop
  - Odometer readings
  - Brake/acceleration
  - Service data

Data from smartphones

- Text messages
- Call logs
- Contacts
- Data files
- Vehicle-related applications

Free tools

- Android
  - ADB, root solutions
  - netcat + dd
  - AFLogical
  - Backup services
- iOS
  - iTunes Backup
  - Backup Extractor (http://supercrazyawesome.com)
  - PhoneBrowse (https://www.imobie.com/phonebrowse)

Commercial tools

XRY

MAGNET FORENSICS®

Oxygen Forensics

ELCOMSOFT PROACTIVE SOFTWARE

...and many, many more

Thanks

- Any questions?

Dan O'Day
doday@kpmg.com
d@4n68r.com
http://4n68r.com
@4n68r