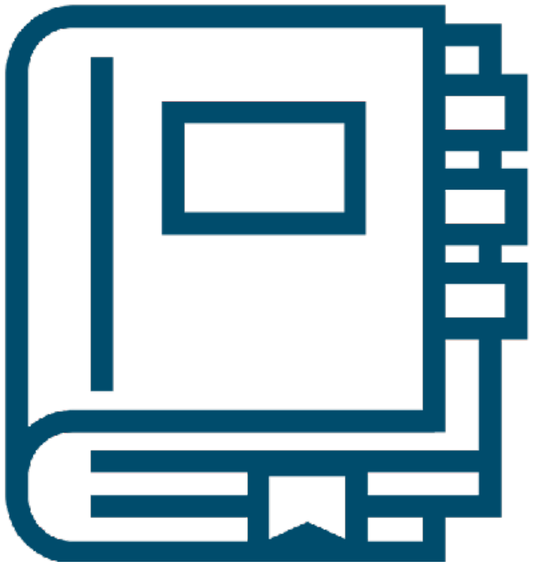
Smartphone Forensics

Dr. Michael Spreitzenbarth

Agenda and Dates

Agenda

- 2018-05-11: Mobile Device Forensics
- 2018-05-25: Android and Forensic Investigation of this OS
- **2018-06-01: Apple iOS and Forensic Investigation of this OS**
- 2018-06-08: Mobile Malware & Hacking Android Apps



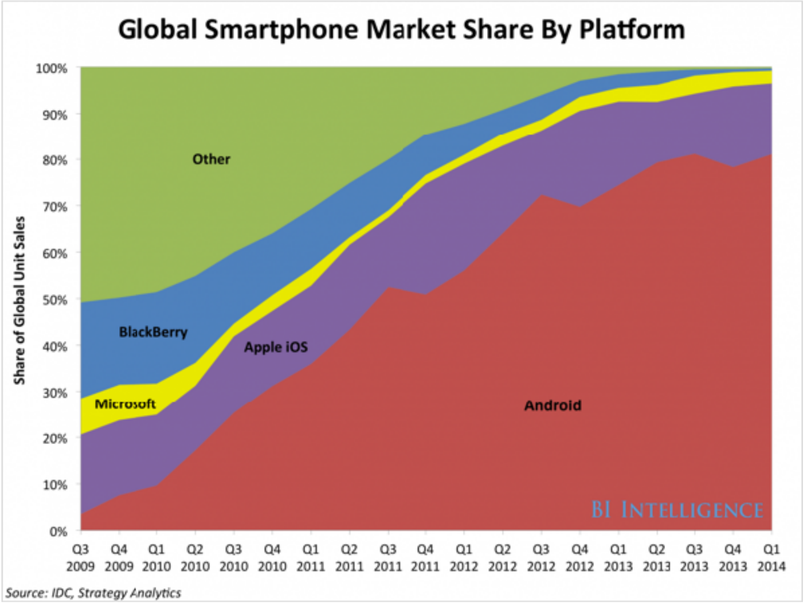
Success and Issues of Apple’s iOS

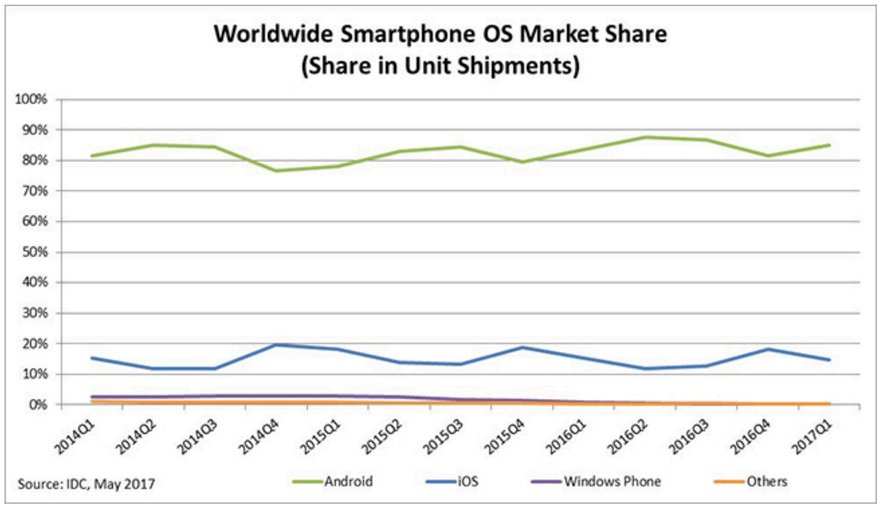
(Apple) iOS

- Formally based on Mac OS X, now only minor similarities but still both are based on a BSD kernel.
- It is mainly used on smartphones and tablets
- Watches and TV boxes use a similar OS but not the same (watchOS/tvOS)
- Backup through iTunes (local PC) or iCloud

Why iOS is not as successful as Android

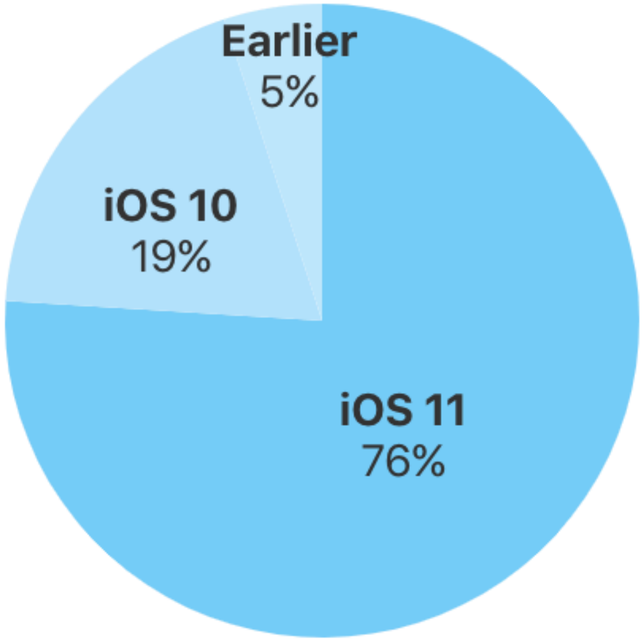
- The majority of the system is closed-source
- Apps are developed either in Objective-C or Swift
- Hughe amount of limitations and restrictions when it comes to publishing the apps
- Higher costs for developers (~90€/year)
- Devices are more expensive and simulator is not identical to a real device





iOS Versions as of April 2018

76% of devices are using iOS 11.

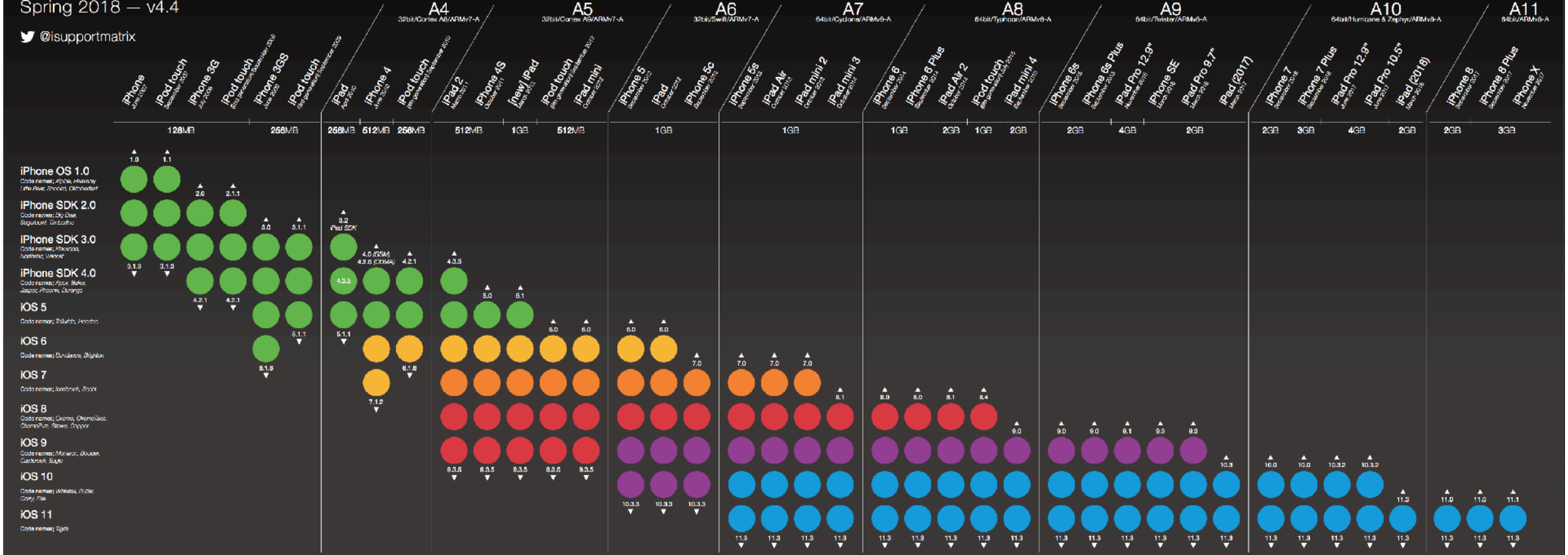


As measured by the App Store on
April 22, 2018.

iOSSupportMatrix.com

Spring 2018 — v4.4

@isupportmatrix



Notes: All dates refer to the US product launch date. Code names are courtesy of iMore.com, thanks to Serenity Caldwell (http://twitter.com/iserenity, https://www.imore.com/author/serenity%20caldwell) for the iPad (2018) info.

The matrix will return in Summer 2018.

iOS - Security Features

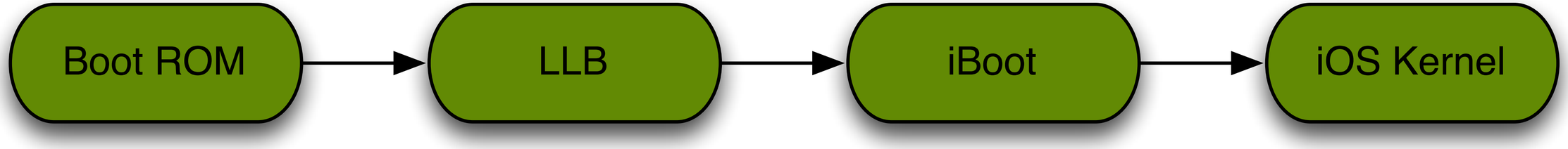
Secure Boot Chain

- As soon as the device starts, it is booting the Boot ROM. This is a special piece of code that had been written on the device during manufacturing and cannot be changed afterwards. Part of this code is the public key of Apples root CA.

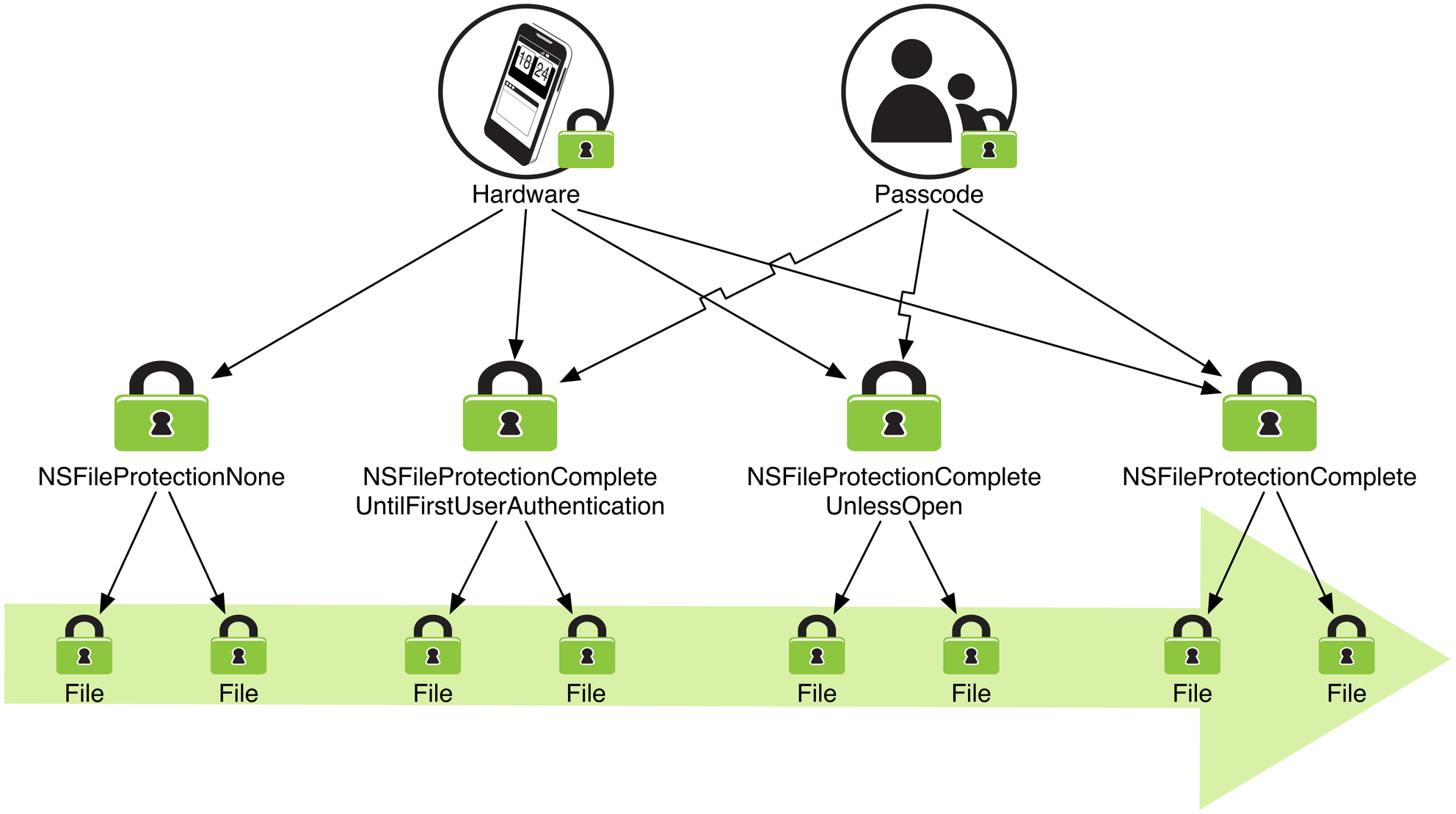
- This public key is then used to ensure the integrity of the Low Level Bootloader (LLB) before starting it. Besides a lot of other features, the LLB is able to locate and validate the iBoot image on the local flash. If this integrity check again succeeds, the iBoot-OS will be started.

- iBoot then gain checks the integrity of the iOS Kernel and is booting the kernel image.

- The iOS kernel is then loading all the drivers and starting the iOS system as the users knows it.



Data Protection



Secure Enclave

- The Secure Enclave boots separately from the rest of the device.
- It runs its own microkernel, which is not directly accessible by the operating system nor by any programs running on the device.
- There’s 4MB of flashable storage, which is used exclusively to store 256-bit elliptic curve private keys.
- These keys are unique to the device, and are never synced to the cloud or even directly seen by the device’s primary operating system.
- Instead, the system asks the Secure Enclave to decrypt information using the keys.

Secure Enclave

„When you store a private key in the Secure Enclave, you never actually handle the key, making it difficult for the key to become compromised. Instead, you instruct the Secure Enclave to create the key, securely store it, and perform operations with it. You receive only the output of these operations, such as encrypted data or a cryptographic signature verification outcome.“ - Apple

Lockdown Profiles

- Since iOS 7 every iOS-based device needs to establish a trust relation to the PC or Mac it will be backed up to.
- Starting with iOS 11 those key pairs had been invalidated after a unspecific time (in our tests between 2 and 3 weeks without a connection between device and PC/Mac)
- Starting iOS 11.3 Apple reduced this time to 7 days

Lockdown Profiles

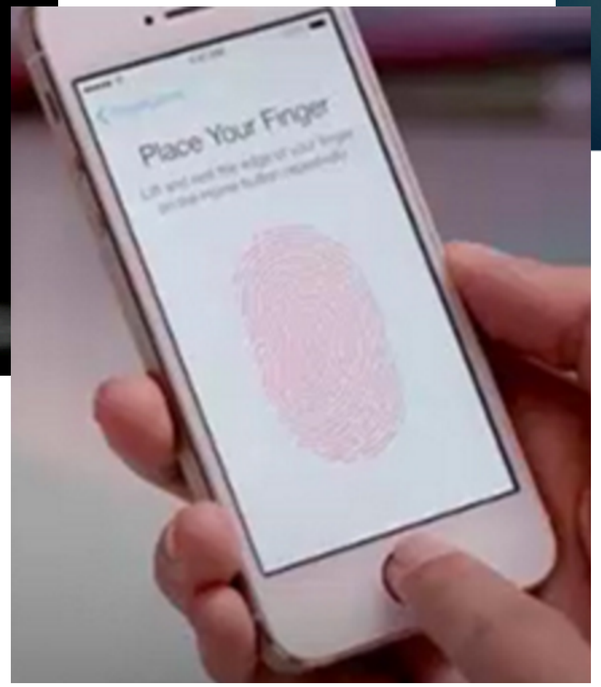
- One half of the key pair (escrow keybag) will be stored on the Mac or PC during the trust establishing process.
    - If the comparison of the key pair matches, the PC/Mac can access the device without unlocking it.
    - If the comparison does not match or if there is no key pair stored on the PC/Mac, the user is asked if he/she wants to establish the trust relationship. Therefore, the screen needs to be unlocked.
- The key pair is stored locally at:
    - Windows: %AllUserProfiles%\Apple\Lockdown\
    - Mac: /private/var/db/lockdown/

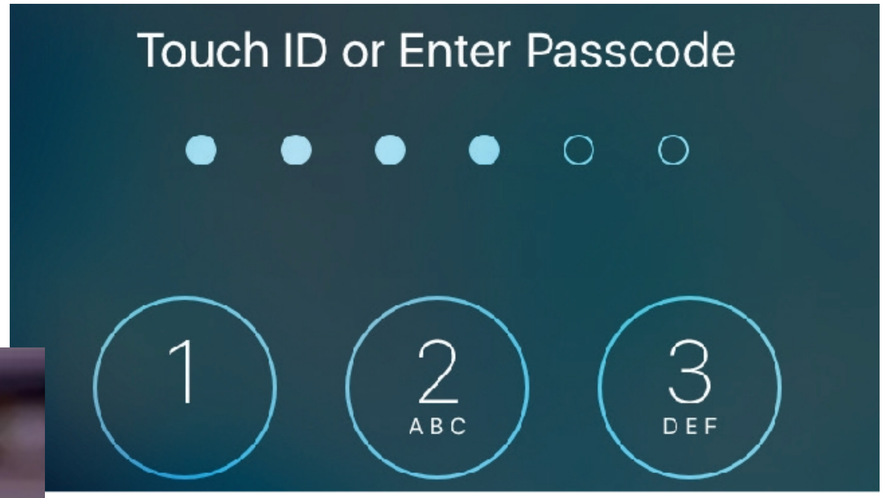
USB Restricted Mode

- In the iOS 11.4 (this Tuesday), Apple introduced a new feature called USB Restricted Mode
- This new mode protects the device from attacks like the GrayKey by disabling the lightning port on the device after 7 days of inactivity.

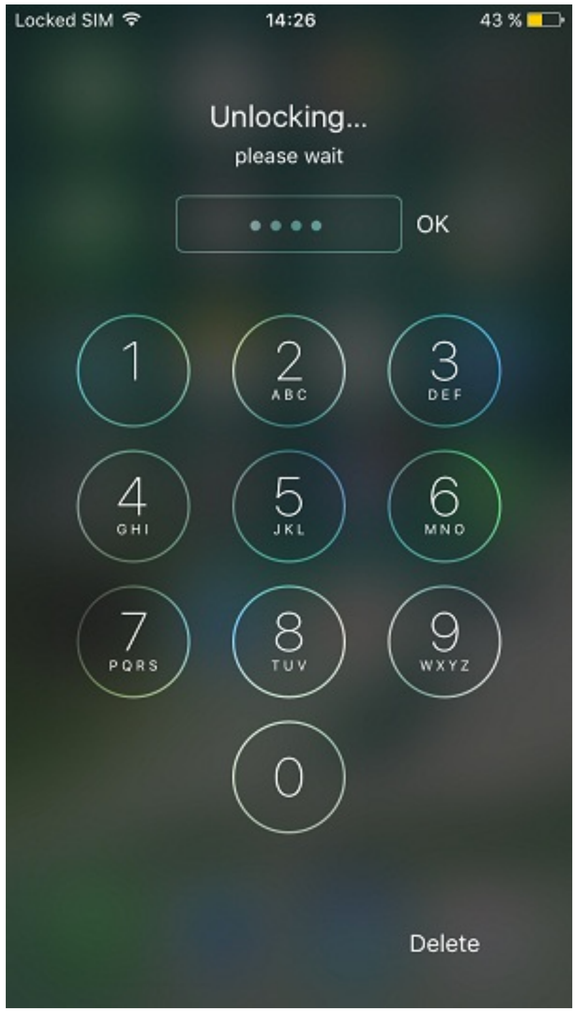
> *“To improve security, for a locked iOS device to communicate with USB accessories you must connect an accessory via lightning connector to the device while unlocked – or enter your device passcode while connected – at least once a week.” - Apple*

Screenlock

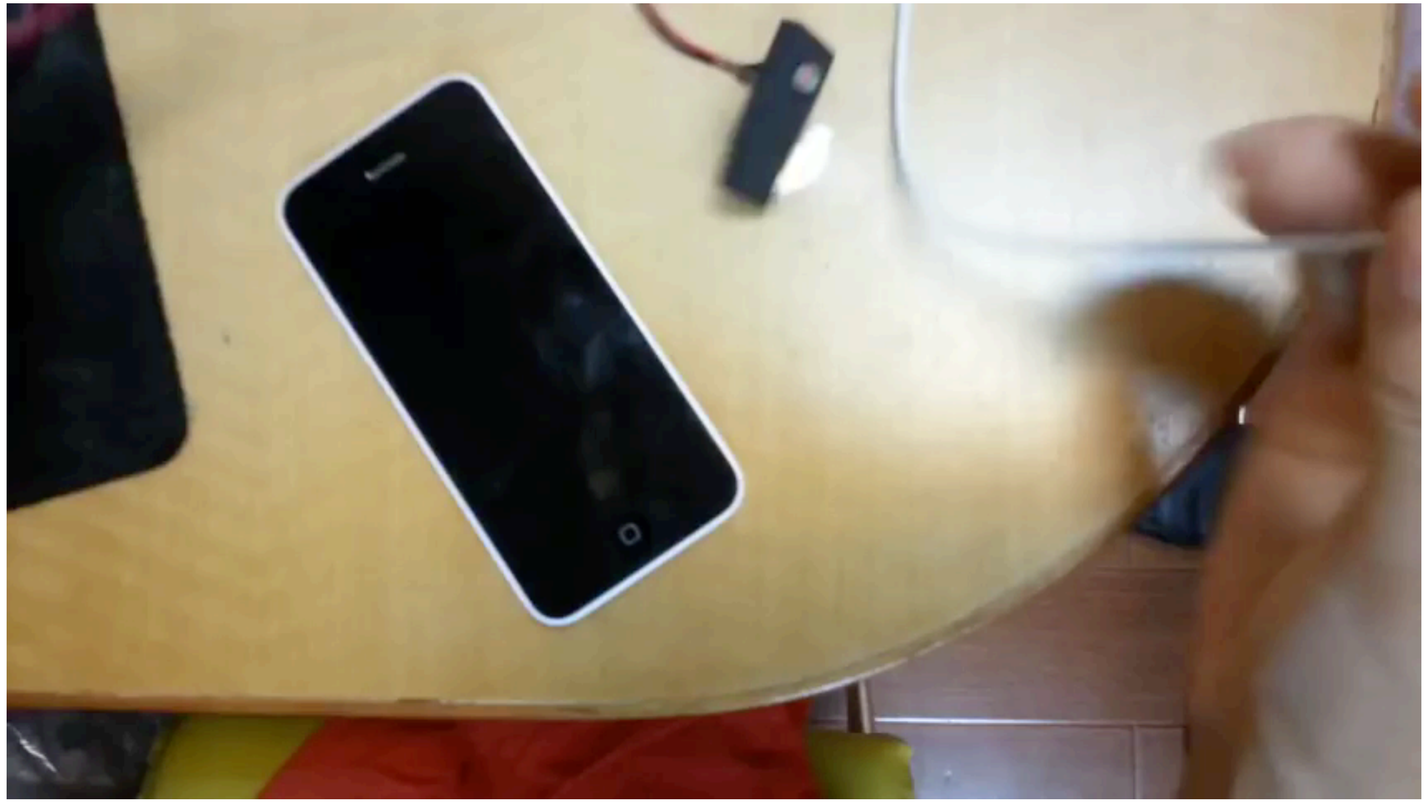




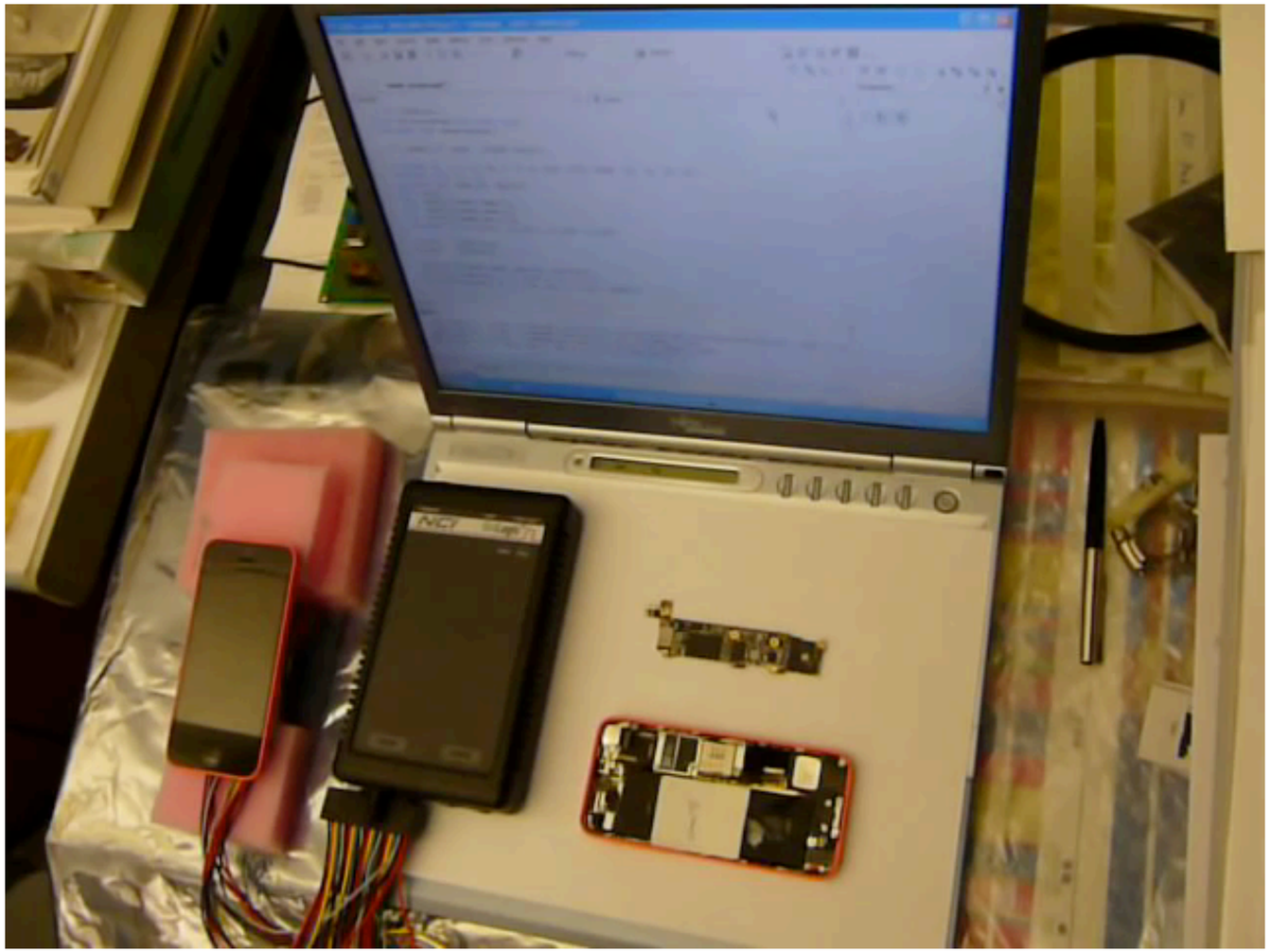
PIN / Password



Bruteforcing IP-Box



NAND Mirroring (iPhone 5c)



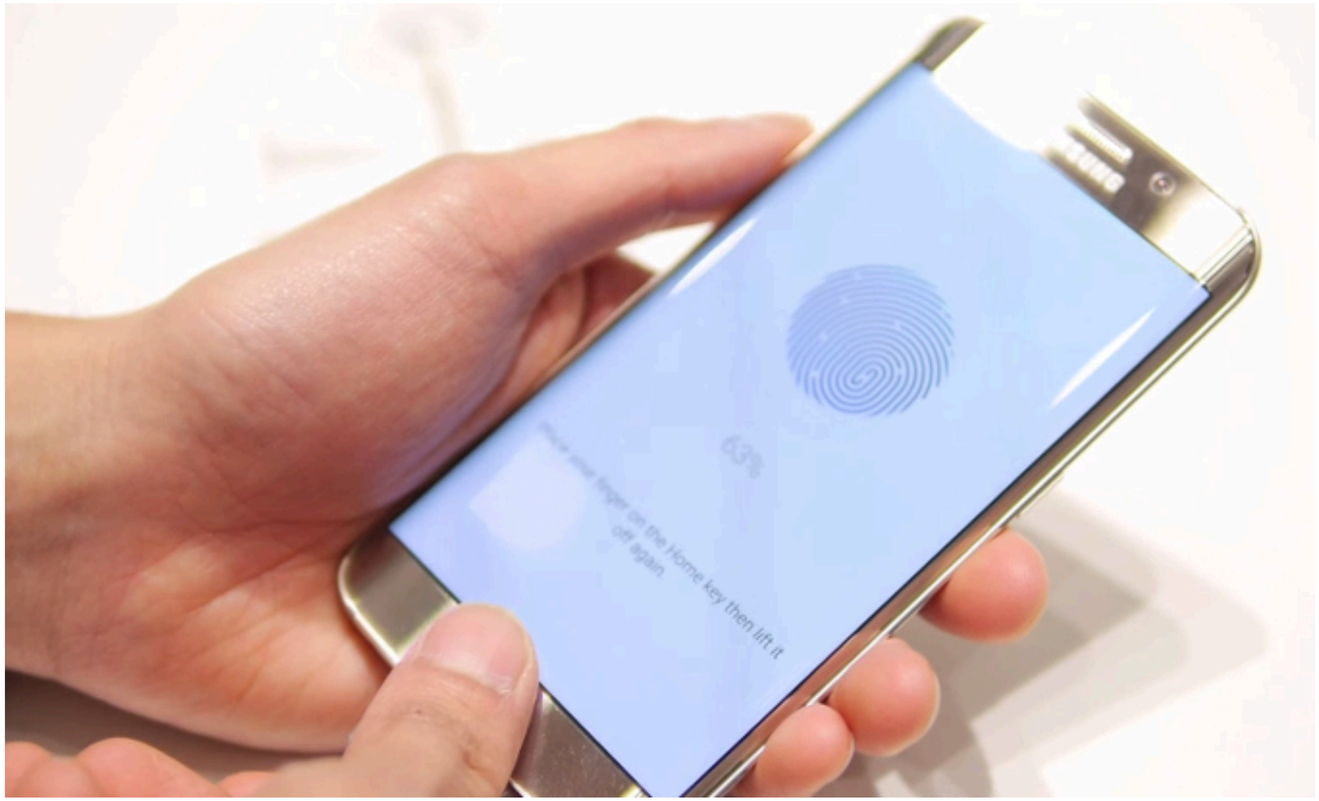
GrayKey

https://www.macrumors.com/2018/03/15/graykey-iphone-unlocking-box/

Screenlock

- Unlocking the screen without knowing the PIN or password is only working at specific devices / iOS versions due to vulnerabilities or design issues
- Since introduction of the iPhone 6 and secure enclave there is no publicly known technique to unlock a device, but special hardware is available
- Used PIN or password is also a part of the key that is used for encryption

Touch ID



Touch ID

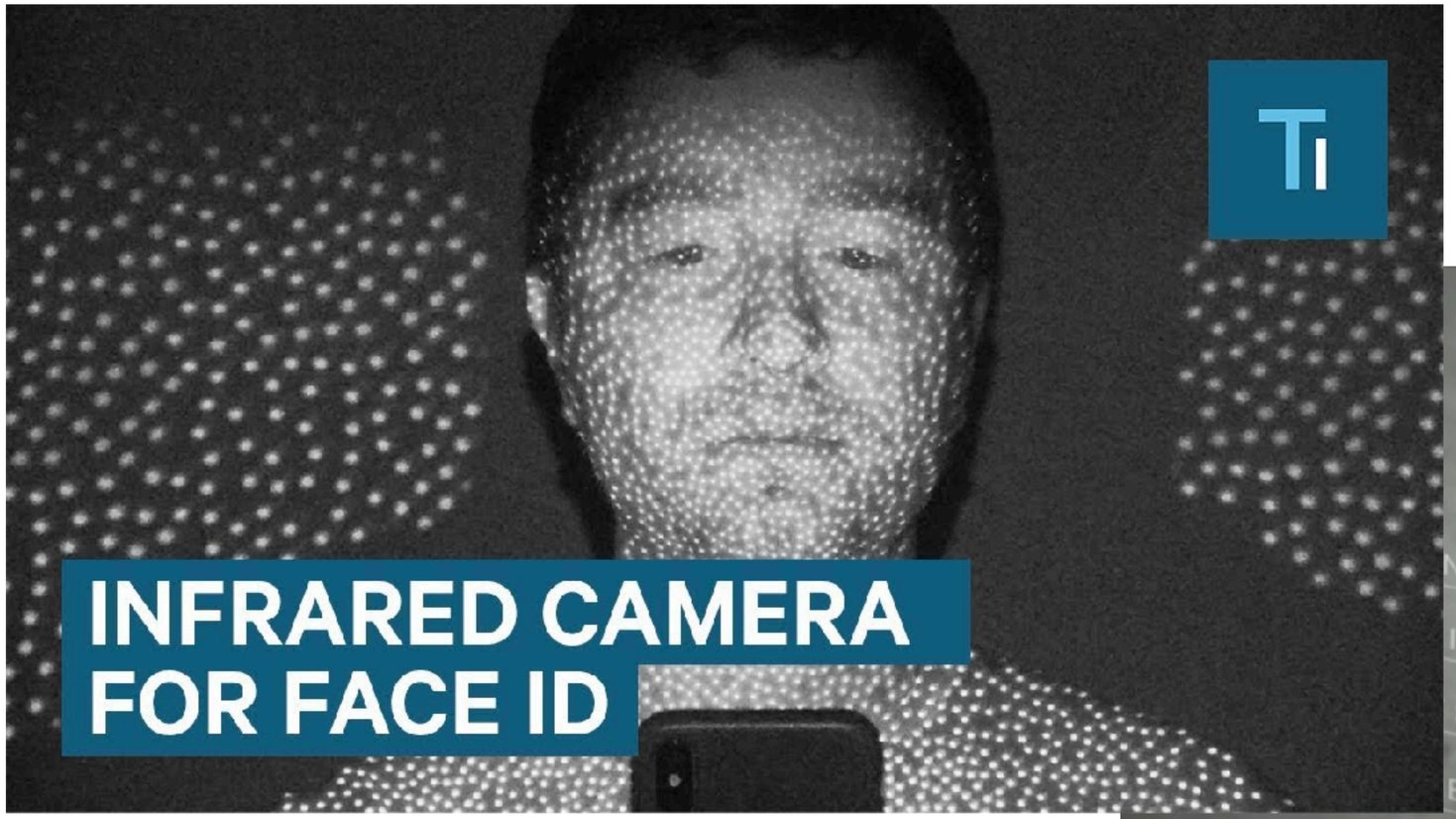
- iOS introduced the feature to unlock the device by using your fingerprint as the first smartphone manufacturer
- iOS-based devices have 5 tries to identify the fingerprint
- The needed quality of the copied fingerprint has to be of high conformity (>80% is needed)
- No chance to unlock the device with the fingerprint after a reboot
- No chance to unlock the device with the fingerprint after 48 hours without a successful unlock

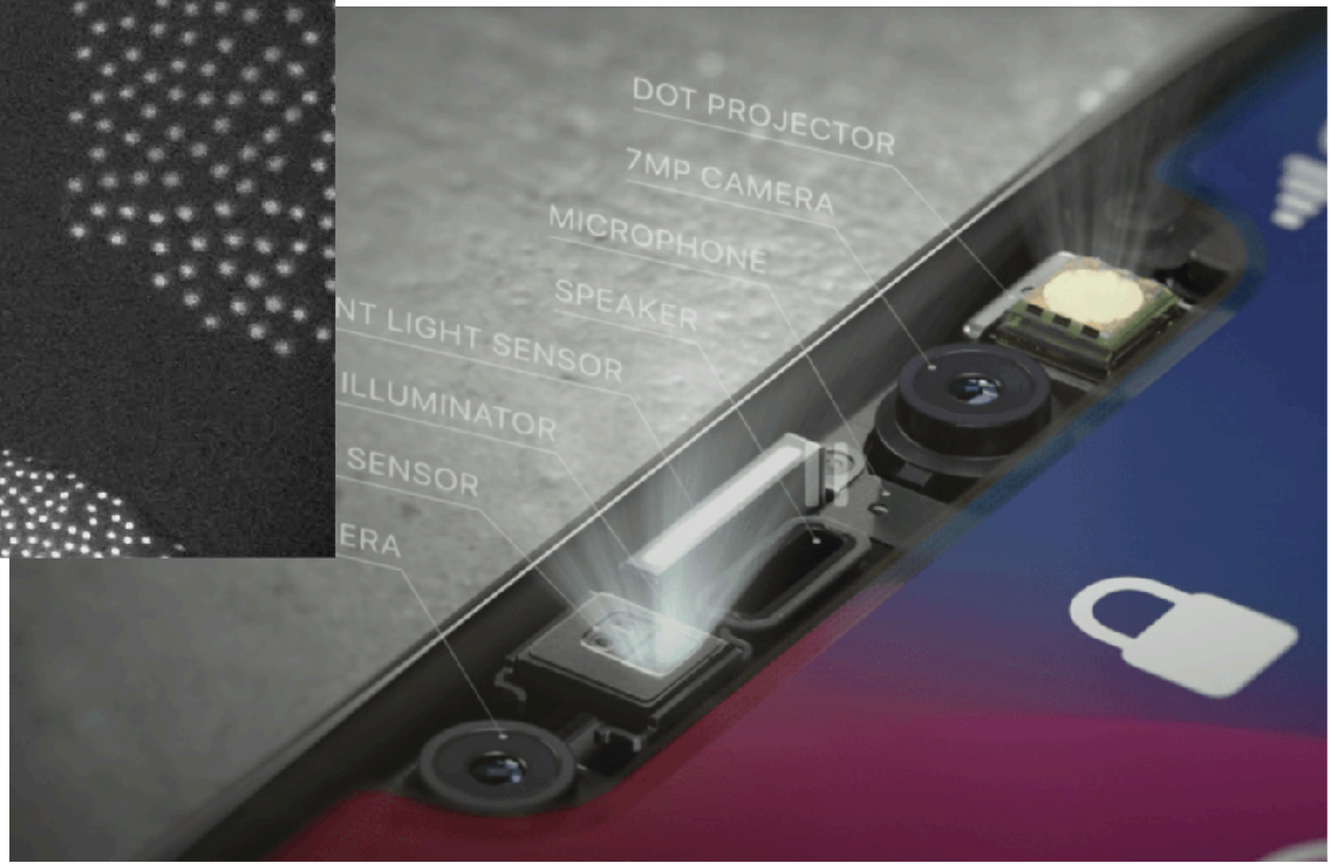
[2]

Touch ID

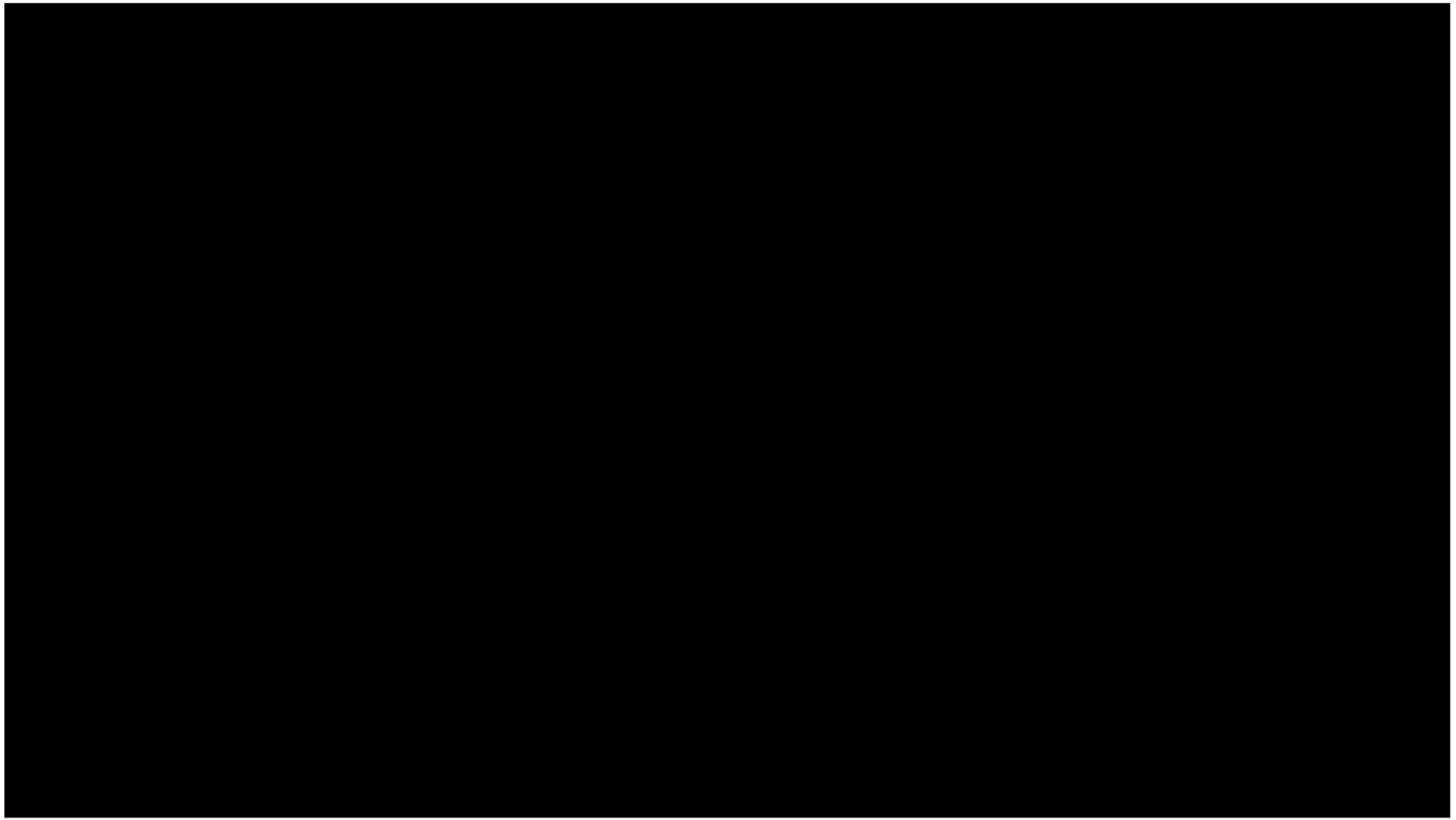
Face ID

Face ID


INFRARED CAMERA
FOR FACE ID


DOT PROJECTOR
7MP CAMERA
MICROPHONE
SPEAKER
NT LIGHT SENSOR
ILLUMINATOR
SENSOR
ERA

Face ID



Face ID

- The device has just been turned on or restarted.
- The device hasn’t been unlocked for more than 48 hours.
- The passcode hasn’t been used to unlock the device in the last six and a half days and Face ID hasn't unlocked the device in the last 4 hours.
- The device has received a remote lock command.
- After five unsuccessful attempts to match a face.
- After initiating power off/Emergency SOS by pressing and holding either volume button and the side button simultaneously for 2 seconds.
- If your device is lost or stolen, you can prevent Face ID from being used to unlock your device with Find My iPhone Lost Mode.

[3]

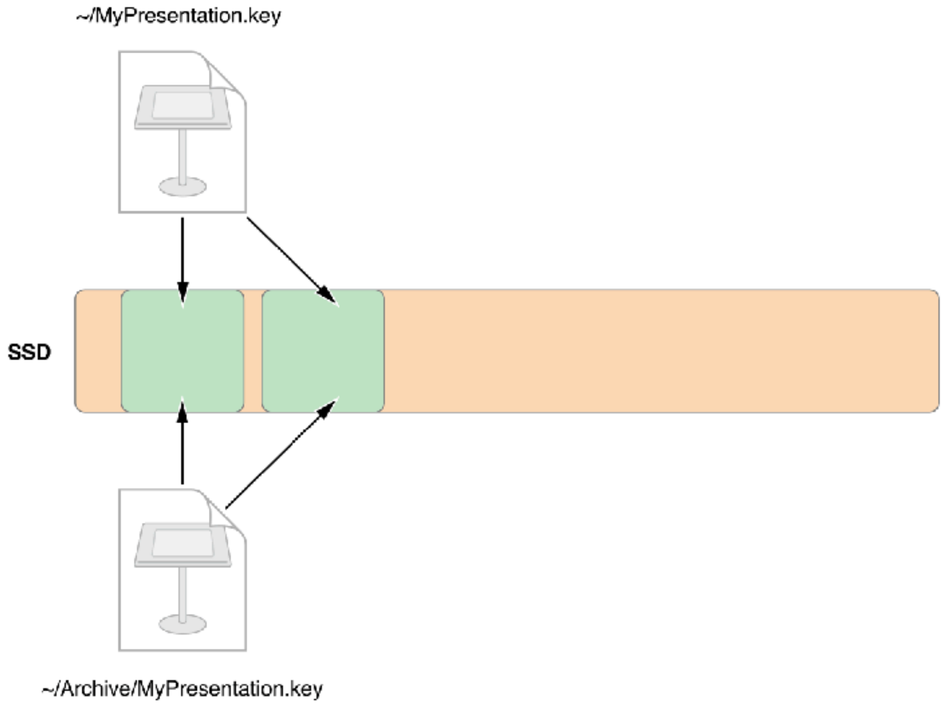
iOS - File System

Apple File System (APFS)

Apple File System is a new, modern file system for iOS, macOS, tvOS, and watchOS. It is optimized for Flash/SSD storage and features strong encryption, copy-on-write metadata, space sharing, cloning for files and directories, snapshots, fast directory sizing, atomic safe-save primitives, and improved file system fundamentals.

APFS replaces HFS+ as the default file system for iOS 10.3 and later, and macOS High Sierra and later.

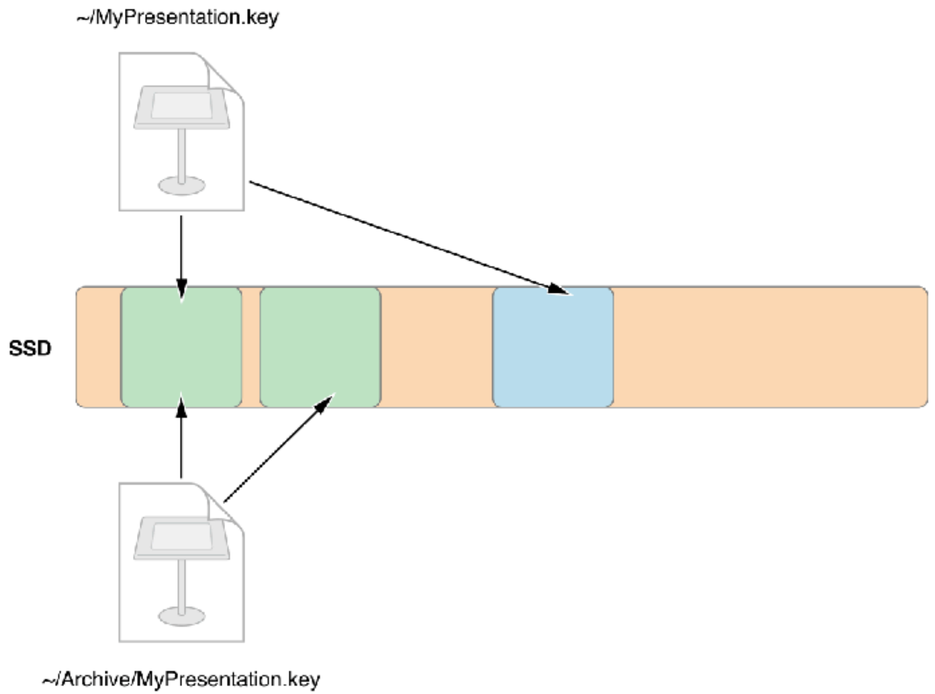
Apple File System (APFS) - Forensic Features



A **clone** is a nearly instantaneous copy of a file or directory that occupies no additional space for file data. Clones allow the operating system to make fast, power-efficient file copies on the same volume without occupying additional storage space.

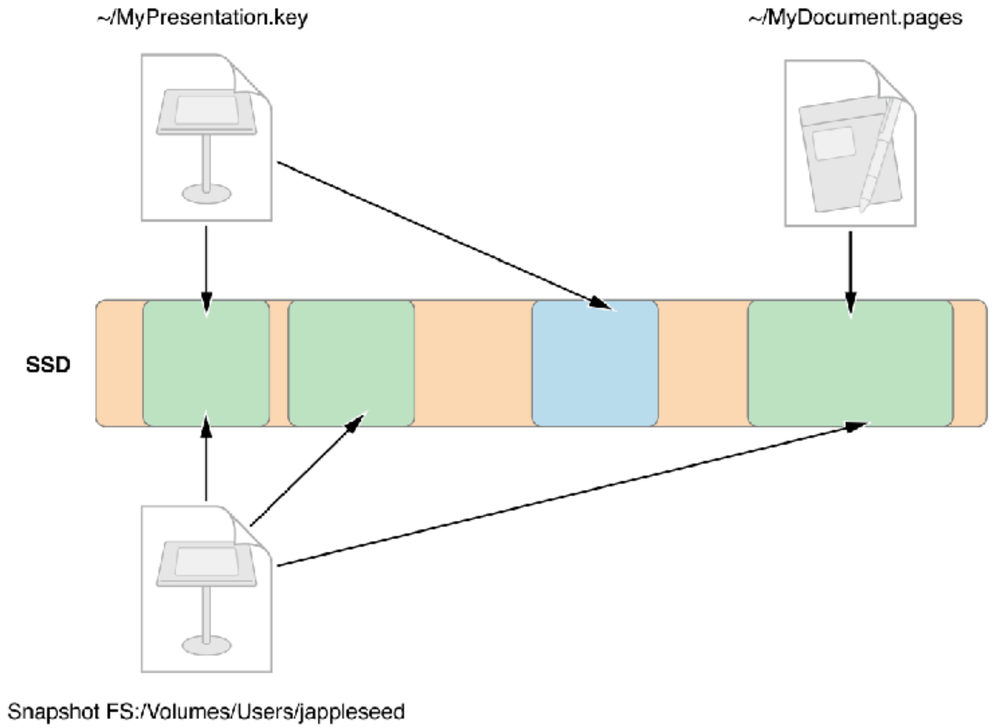
[4]

Apple File System (APFS) - Forensic Features



Modifications to the data write the new data elsewhere and continue to share the unmodified blocks. Changes to a file are saved as deltas of the cloned file.

Apple File System (APFS) - Forensic Features



A **volume snapshot** is a point-in-time, read-only instance of the file system. The operating system uses snapshots to make backups work more efficiently and offer a way to revert changes to a given point in time.

[4]

Apple File System (APFS) - Encryption

Security and privacy are fundamental in the design of Apple File System. That's why Apple File System implements strong full-disk encryption, encrypting files and all sensitive metadata.

Which encryption methods are available depends on hardware and operating system support, and can vary for each type of Apple device.

Apple File System supports the following encryption models for each volume in a container:

- No encryption
- Single-key encryption
- Multi-key encryption with per-file keys for file data and a separate key for sensitive metadata

Multi-key encryption ensures the integrity of user data. Even if someone were to compromise the physical security of the device and gain access to the device key, they still couldn't decrypt the user's files.

Apple File System uses AES-XTS or AES-CBC encryption modes, depending on hardware.

iOS Device Analysis - Overview

All I want to be is ROOT

- User- and group-based permission model on file system layer
- iOS is protecting the user partition with different level of encryption and a TPM

=> know the screen lock and gain root privileges

All I want to be is ROOT

- For many versions of iOS you can find a working public jailbreak. Sometimes you just need to wait ;)

- Cat and Mouse game: as soon as Apple knows about a jailbreak, they will patch the vulnerability. This means you only have a small window to use the jailbreak for a real investigation.

=> gain root privileges and system shell

Where to find Evidence?

- Each App is using its own database (SQLite or PLIST)
- Sandboxes containing data can be found at:
    - private/var/mobile/Containers/Data/Application/<GUID>
- Pictures, music and videos can be found at:
    - private/var/mobile/Media/DCIM/1XXAPPLE
    - private/var/mobile/Media/

Where to find Evidence?

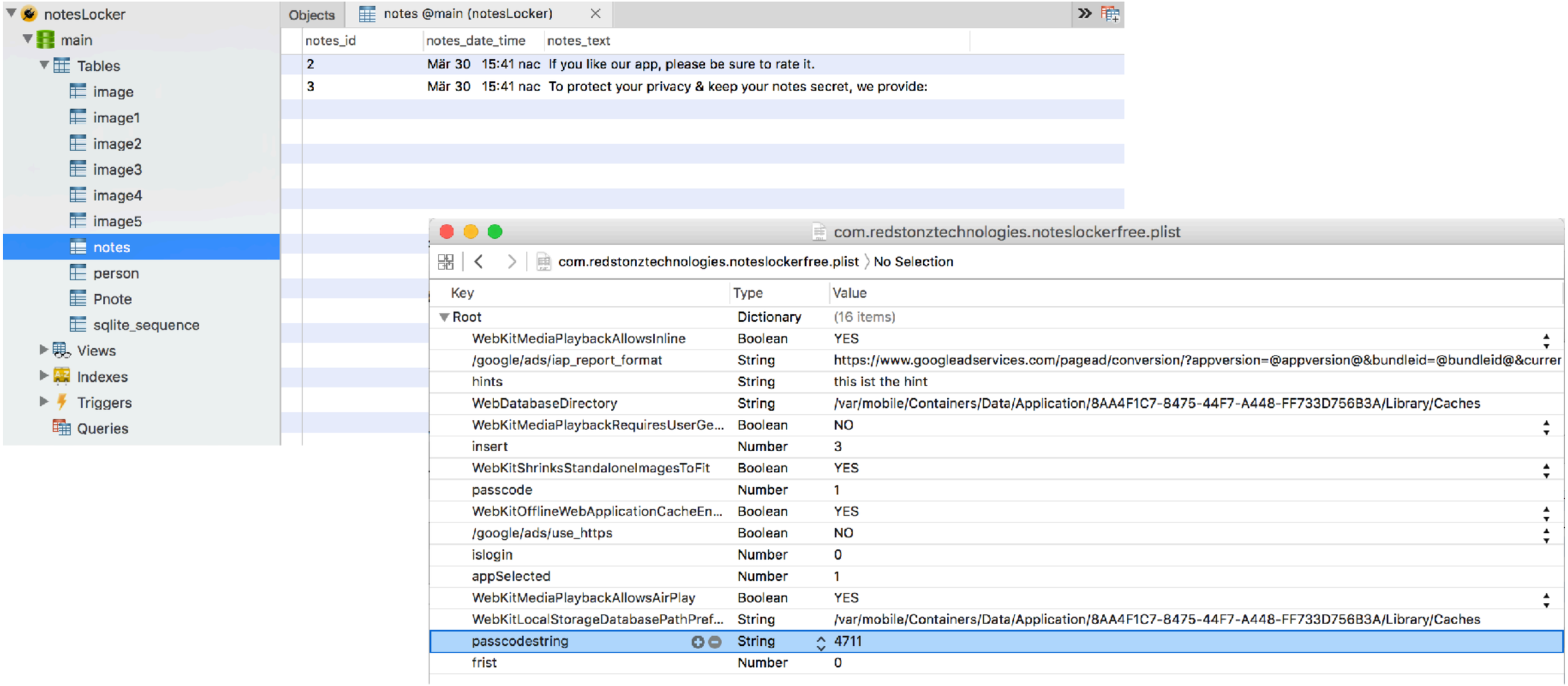
- iOS Keychain
  - System database containing all the credentials and keys the user/ device needs to authorize
- Keyboard- and System-Caches

How does the Evidence look like?

- Pictures are stored as JPEG files
    - look for meta data (EXIF)

- Storage of the apps is often done by using local databases (SQLite DB files or Apple specific PLIST files)
    - for normal use: SQLite Database Browser and PLIST-Viewer for Windows
    - for professional use: Sanderson Forensic Toolkit for SQLite

Databases


notesLocker
main
Tables
image
image1
image2
image3
image4
image5
notes
person
Pnote
sqlite_sequence
Views
Indexes
Triggers
Queries
Objects
notes @main (notesLocker)
notes_id
notes_date_time
notes_text
2
Mär 30 15:41 nac
If you like our app, please be sure to rate it.
3
Mär 30 15:41 nac
To protect your privacy & keep your notes secret, we provide:
com.redstonztechnologies.noteslockerfree.plist
com.redstonztechnologies.noteslockerfree.plist 〉 No Selection
Key
Type
Value
Root
Dictionary
(16 items)
WebKitMediaPlaybackAllowsInline
Boolean
YES
/google/ads/iap_report_format
String
https://www.googleadservices.com/pagead/conversion/?appversion=@appversion@&bundleid=@bundleid@&currer
hints
String
this ist the hint
WebDatabaseDirectory
String
/var/mobile/Containers/Data/Application/8AA4F1C7-8475-44F7-A448-FF733D756B3A/Library/Caches
WebKitMediaPlaybackRequiresUserGe...
Boolean
NO
insert
Number
3
WebKitShrinksStandaloneImagesToFit
Boolean
YES
passcode
Number
1
WebKitOfflineWebApplicationCacheEn...
Boolean
YES
/google/ads/use_https
Boolean
NO
islogin
Number
0
appSelected
Number
1
WebKitMediaPlaybackAllowsAirPlay
Boolean
YES
WebKitLocalStorageDatabasePathPref...
String
/var/mobile/Containers/Data/Application/8AA4F1C7-8475-44F7-A448-FF733D756B3A/Library/Caches
passcodestring
String
4711
frist
Number
0

How to get the important data?

- Unsoldering the flash memory
- Using the JTAG interface
- Software agents installed on the device
- Specific Soft-/Hardware solutions
- iTunes-/iCloud-Backup
- Jailbreaking

Specific Soft-/Hardware-Solutions

- Special software will be installed on the PC and connects to the device via data cables
- The software is often using the default drivers of the manufacturer
- It is still one of the best solutions when it comes to iOS devices

iTunes-/iCloud-Backup

- Most devices are still backed up locally to a PC or Mac
- A growing amount of devices are backed up to iCloud
- Access to those locations are possible through specific tools from companies like Elcomsoft or Cellebrite

[1]

Jailbreaking

- Jailbreaks for iOS-based devices are „more or less“ the same as root exploits for Android-based ones

- Ownership and source of jailbreaks is often unknown and the past has shown that not all of them are benign.

- Since many years you still need to unlock the screen for applying/ installing the jailbreak.

iOS Device Analysis - Preservation

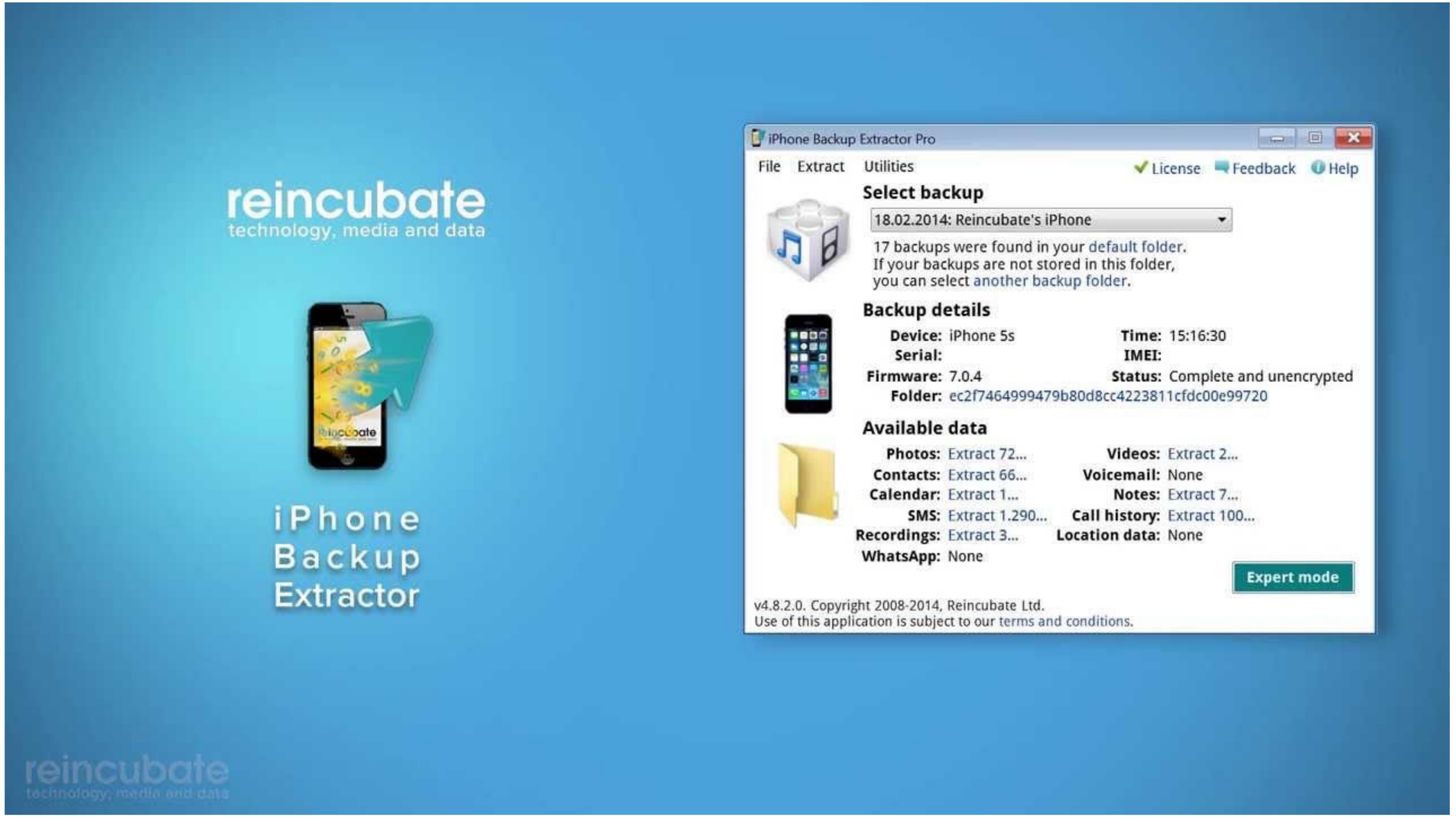
iTunes-/iCloud-Backup

- Content:
  - Pictures, Videos and Screenshots
  - Contacts and Calendar
  - Safari, History, Cookies and cached opened websites
  - Content and databases of all installed apps
  - Keychain
  - etc.

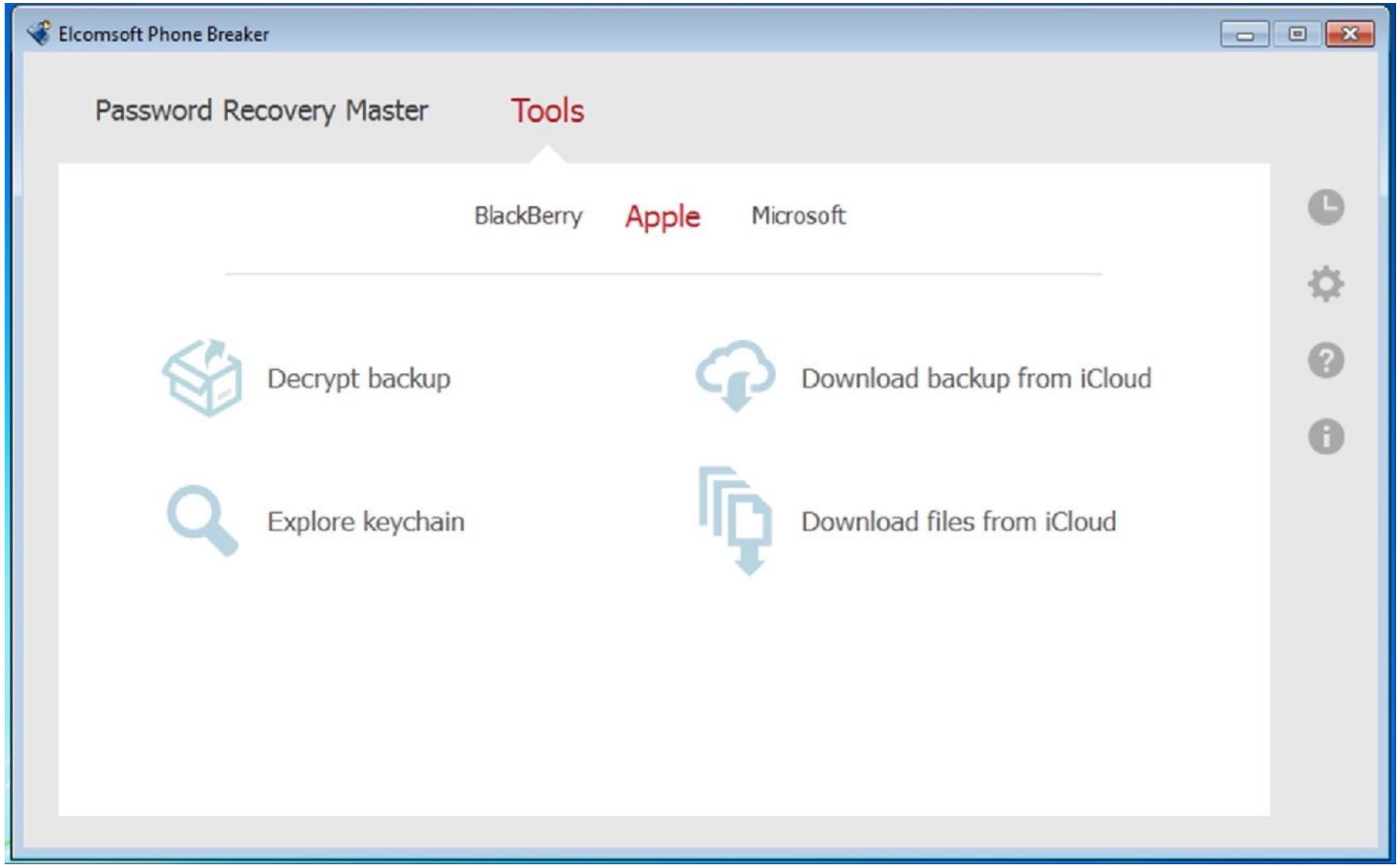
iTunes-/iCloud-Backup

- iTunes Backups stored locally at:
  - Windows:
    \Users\<user>\AppData\Roaming\AppleComputer\MobileSync\Backup\
  - Mac:
    ~/Library/Application Support/MobileSync/Backup/

iTunes-Backup



iCloud-Backup



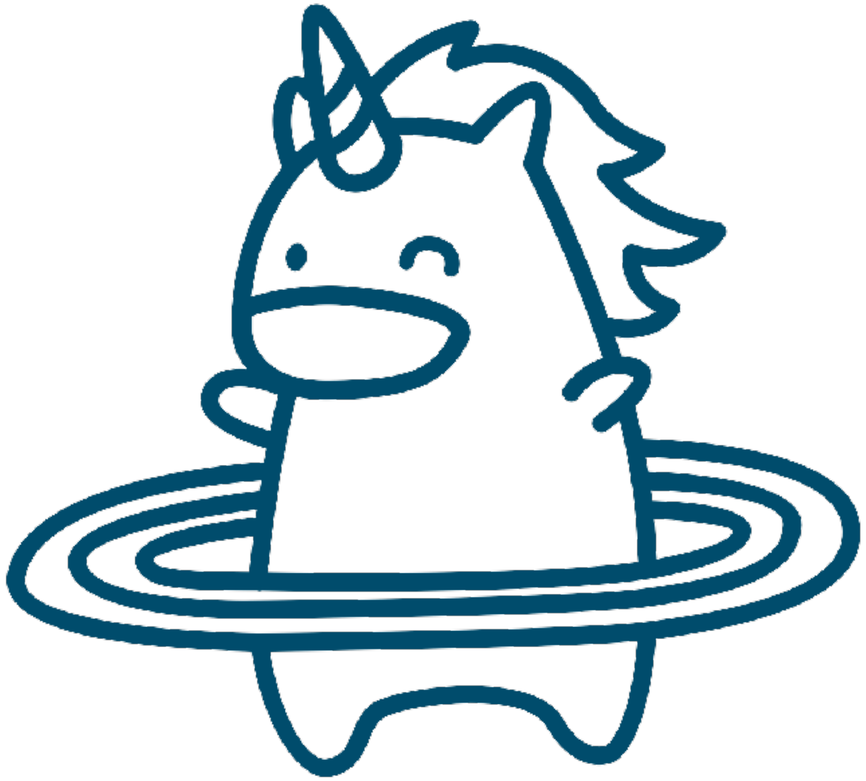
SCP/SSH

- Manuel preservation through SCP/SSH (after Jailbreak)
- Important files:
  - Browser History and Bookmarks: private/var/mobile/Library/Safari/Bookmarks.db
  - Contacts: private/var/mobile/Library/AddressBook/AddressBook.sqlitedb
  - Call Logs: private/var/mobile/Library/CallHistoryDB/CallHistory.storedata
  - SMS/MMS: private/var/mobile/Library/SMS/sms.db
  - Calendar: private/var/mobile/Library/Calendar/Calendar.sqlitedb
  - Installed Apps: private/var/db/lsd/com.apple.lsdidentifiers.plist

SCP/SSH

- More interesting files during an investigation: https://salt4n6.com/2018/05/15/a-few-interesting-ios-forensic-artefacts/

Let's start with the exercises now!



Exercise 1

- Analyze a PLIST file to find the device name

Exercise 2

- Analyze a local backup of an iOS device

Recap

- Know how the secure boot chain looks like and why this could be an issue for forensic investigations.
- Know the different types of file encryption.
- Know what lockdown profiles are and why they are important.
- Understand the issues behind USB restricted mode.
- Where to find the interesting data (evidence)?
- How does the evidence look like?
- 2 ways to perform preservation and start to analyze the evidence

See you next week!

- [1] https://support.apple.com/en-us/HT204136
- [2] https://support.apple.com/en-us/HT204587
- [3] https://support.apple.com/en-us/HT208108
- [4] https://developer.apple.com/library/content/documentation/FileManagement/Conceptual/APFS_Guide/Features/Features.html