Times ‘a Ticking… to Forensicate the Apple Watch!

Sarah Edwards &
Heather Mahalik

05/06/15

Who Are We?

- **Sarah Edwards**
  - Course Author/Instructor for FOR518
  - Works at Parsons Corporation
  - Apple fan girl by day, Apple fan girl by night (I wish I had another hobby…)
  - @iamevltwin
  - mac4n6.com

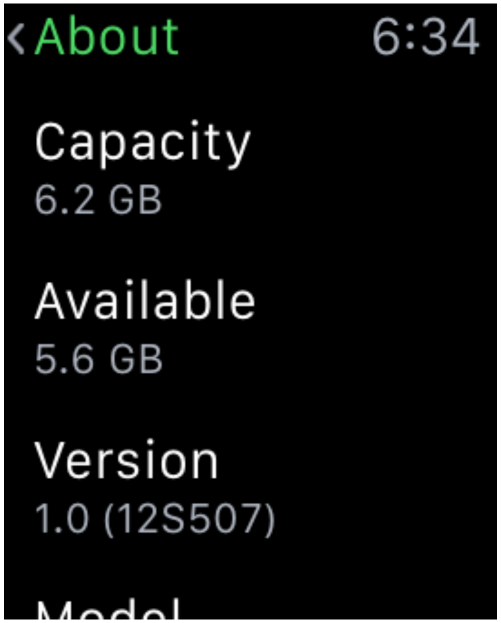
- **Heather Mahalik**
  - Course Author/Instructor for FOR585
  - Works at Oceans Edge, Inc.
  - Fox hunter by day, wine drinker by night (or bud light…)
  - Co-Author of Practical Mobile Forensiscs
  - @HeatherMahalik
  - smarterforensics.com

The Apple Whaaaa?

- Apple’s New Wearable Technology
- “Smart Watch”
- Size: 38mm / 42mm
- Must be paired with iPhone (iOS 8.2, iPhone 5 or newer)
- $350 - $17,000!

Apple Watch Hardware

- Internal Hardware
  - Chip: S1 “System in a Package (SiP)” - Contains RAM, Processor, Storage, Radios, etc…wrapped up in a single package.
    - RAM: 512 MB
    - Flash Storage: 8 GB
    - Radios: WiFi & Bluetooth LE
  - Taptic Engine
    - For Haptic Feedback
  - Check out:
    - https://www.ifixit.com/Teardown/Apple+Watch+Teardown/40655



‹About 6:34

Capacity
6.2 GB

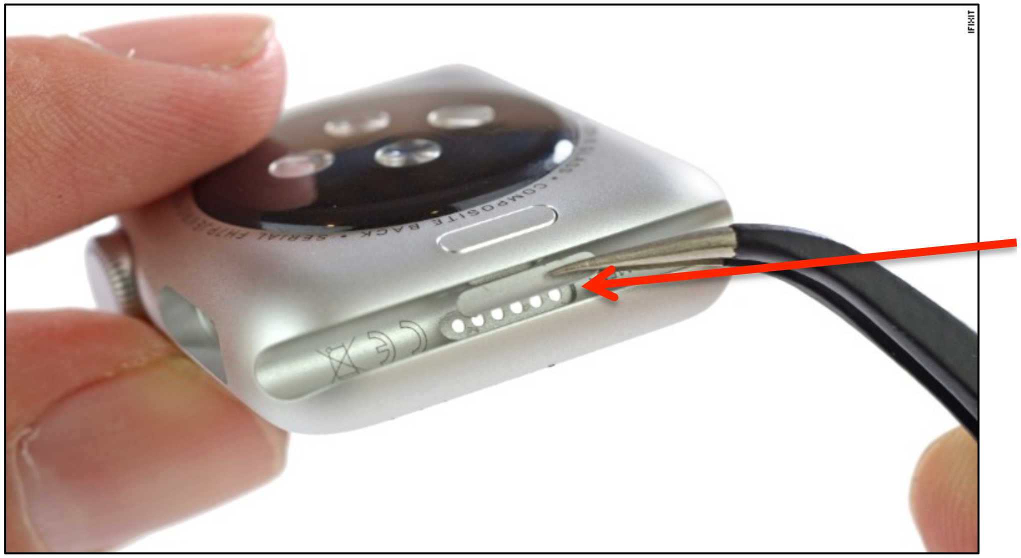
Available
5.6 GB

Version
1.0 (12S507)

Model

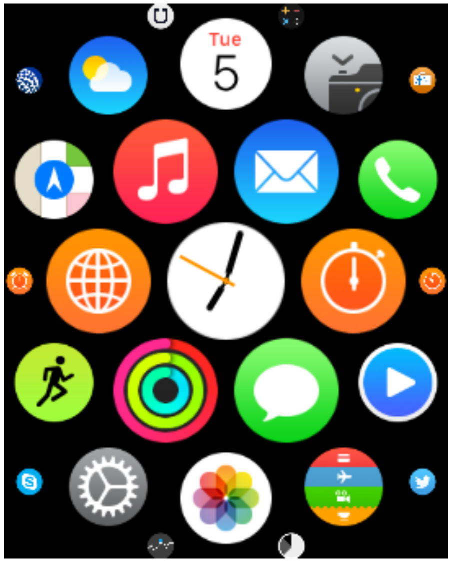
Apple Watch Hardware

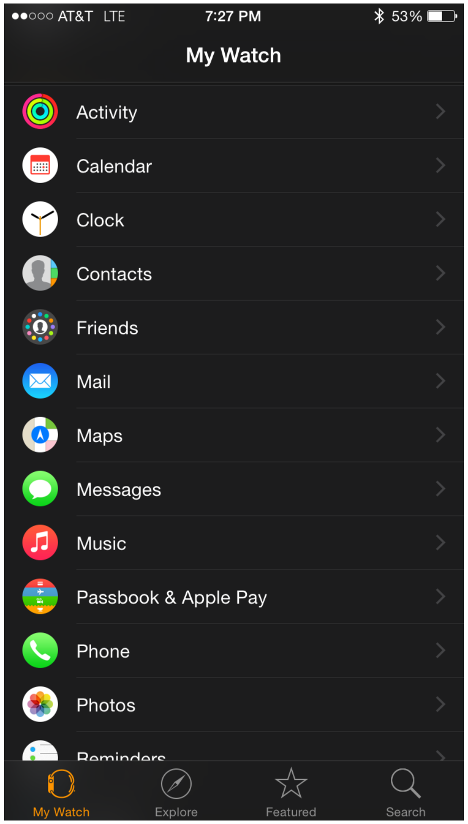
- External Hardware
  - Underside
    - MagSafe Induction
      - Power Charge
    - LEDs & Photodiodes
      - Heart Rate Sensor
  - “Diagnostic Port”
    - Power
    - Firmware
    - Forensics?
  - Touch Screen
    - Pressure Sensitive – “Force Touch”
  - Digital Crown
    - Zooming/Scrolling
  - Side Button
    - Contact Selection



Software

- Software
  - "WatchOS 1.0" – iOS-Based? (YMMV, from Wikipedia)
  - Carousal - The Interface
    - Ie: Springboard / Finder
- Apps:
  - Native: Activity, Calendar, Clock, Contacts, Friends, Mail, Maps, Messages, Music, Passbook/Apple Pay, Phone, Photos, Reminders, Stocks, Weather, Workout
  - 3rd Party Apps!
- Use the Apple Watch App on iPhone to sync data.

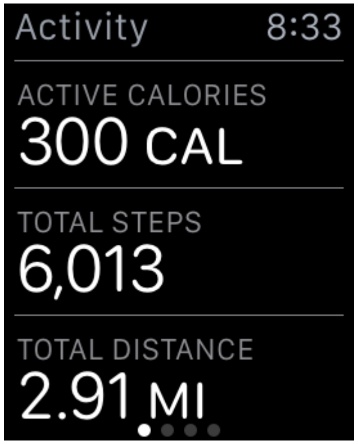



●●○○○ AT&T LTE 7:27 PM 53%

My Watch

- Activity
- Calendar
- Clock
- Contacts
- Friends
- Mail
- Maps
- Messages
- Music
- Passbook & Apple Pay
- Phone
- Photos
- Reminders

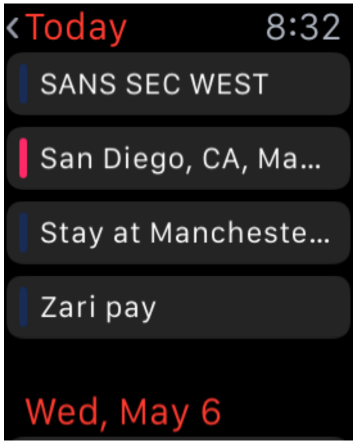
Capabilities


Activity 8:33

ACTIVE CALORIES
300 CAL

TOTAL STEPS
6,013

TOTAL DISTANCE
2.91 MI


Today 8:32

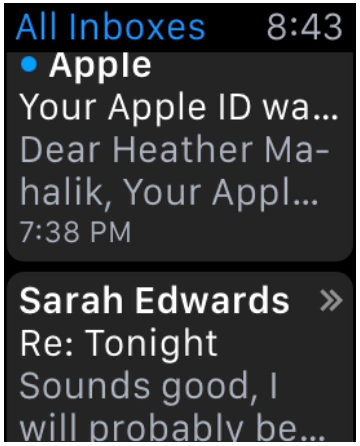
SANS SEC WEST

San Diego, CA, Ma...

Stay at Mancheste...

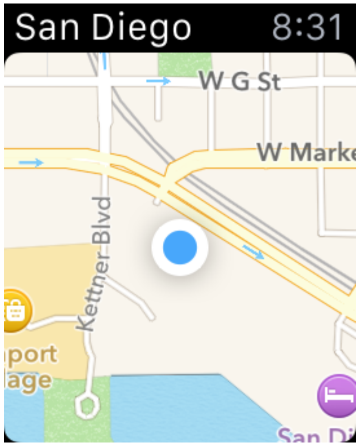
Zari pay

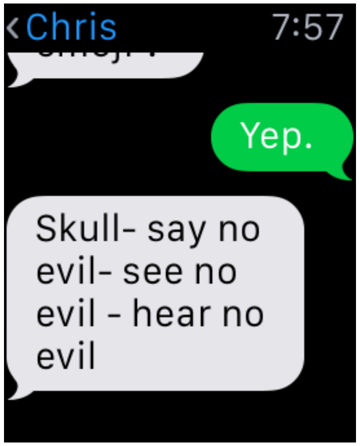
Wed, May 6


All Inboxes 8:43

Apple
Your Apple ID wa...
Dear Heather Mahalik, Your Appl...
7:38 PM

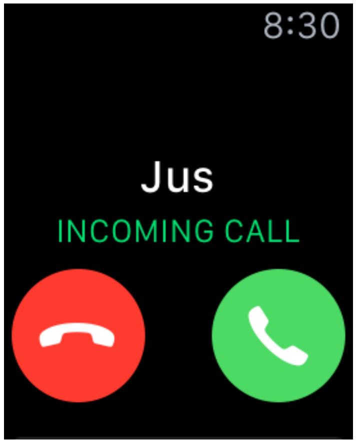
Sarah Edwards
Re: Tonight
Sounds good, I will probably be...


San Diego 8:31

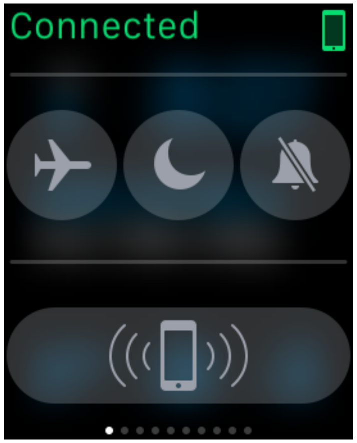

Chris 7:57

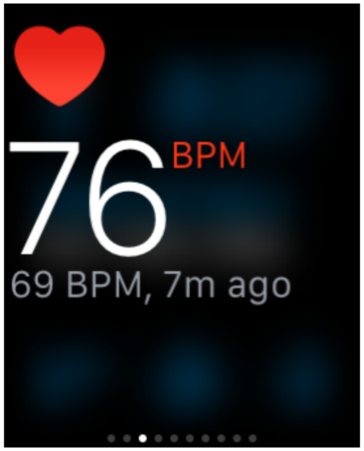
Yep.

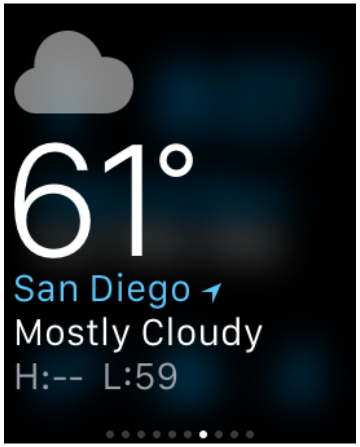
Skull- say no evil- see no evil - hear no evil


8:30

Jus
INCOMING CALL


Connected


76 BPM
69 BPM, 7m ago


61°
San Diego
Mostly Cloudy
H:-- L:59

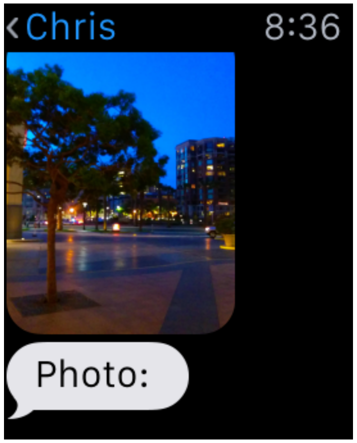

Chris 8:36

Photo:

Implications

Forensic

- iOS Backups
  - What is synced?
- Physical Access?
  - Lost, Stolen, Evidence Intake

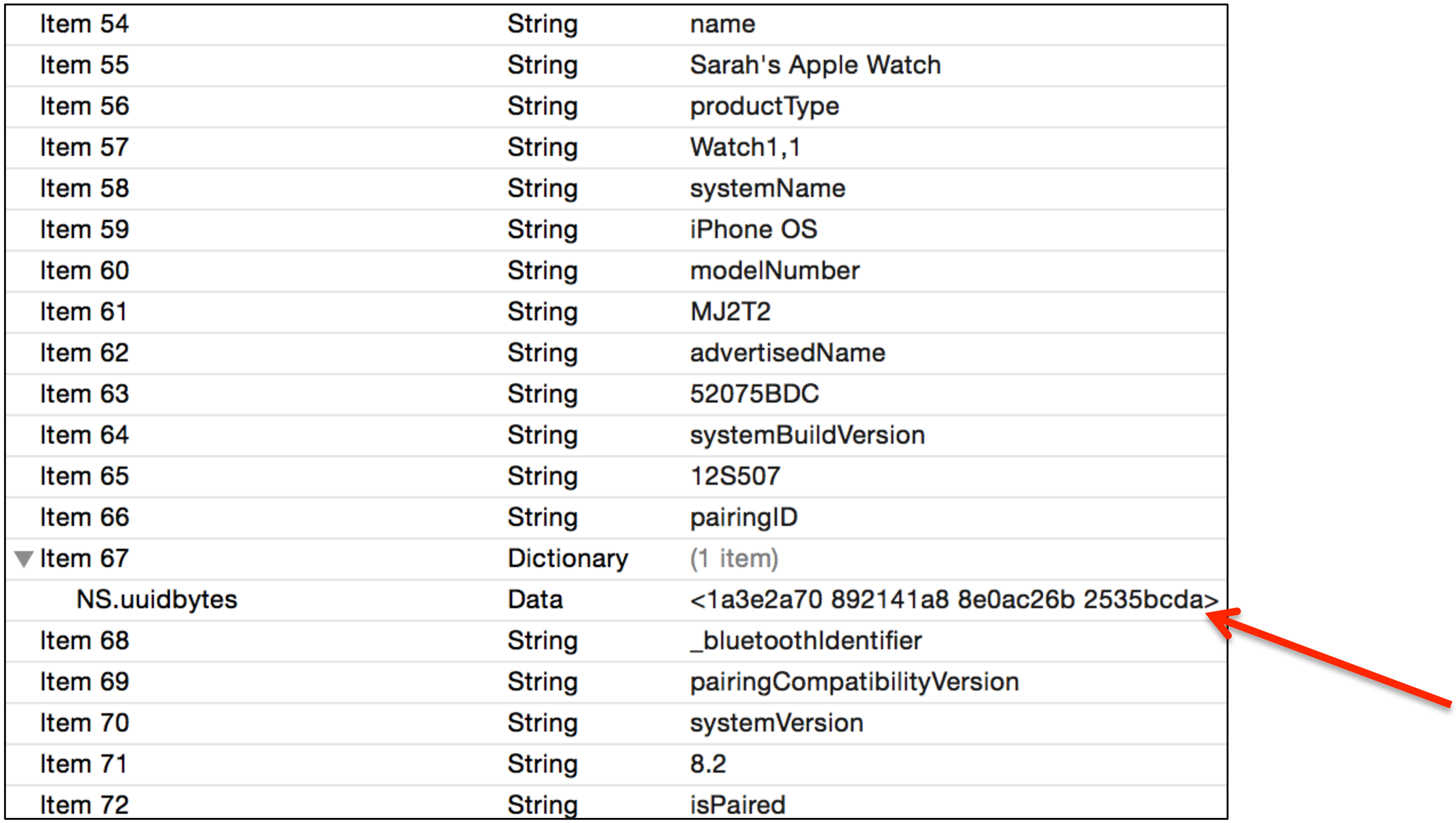
Security

- WiFi & Bluetooth Always On (to sync w/ iPhone)
- Passbook w/o Biometric Authentication
- Security Assessments

iOS Backup Data

/mobile/Library/DeviceRegistry.state/properties.bin

- Binary Plist File – Contains Paired Apple Watch Specifics incl: Watch Name, Make, Model, OS, GUID

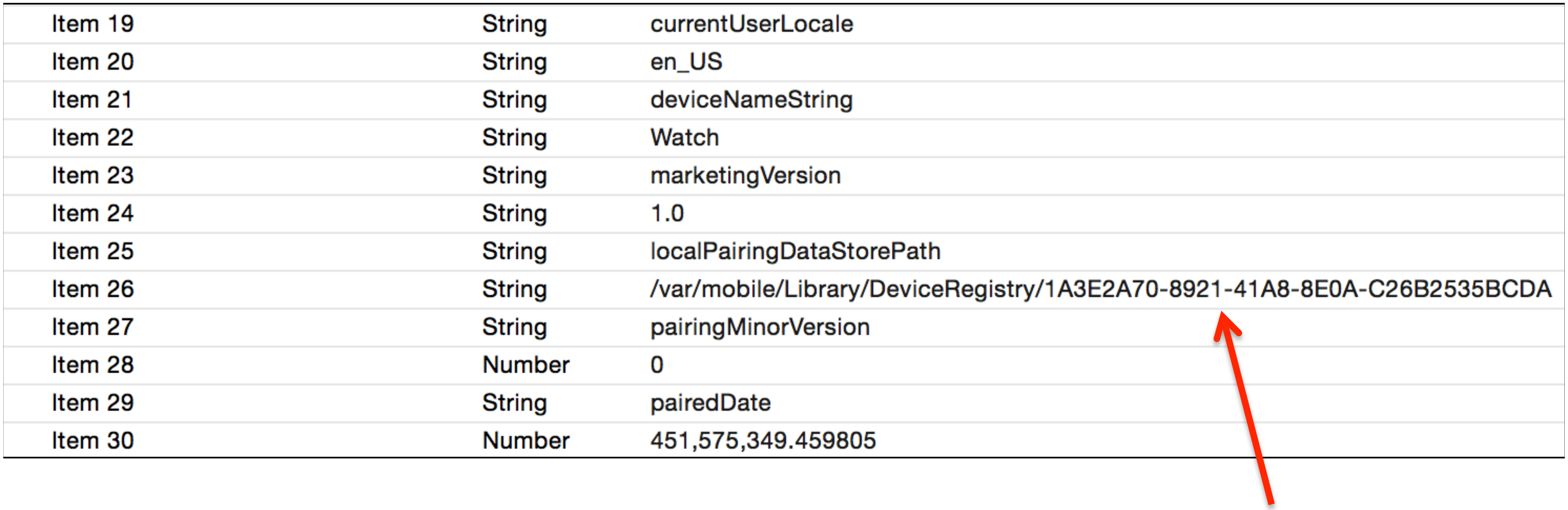


Item 54	String	name
Item 55	String	Sarah's Apple Watch
Item 56	String	productType
Item 57	String	Watch1,1
Item 58	String	systemName
Item 59	String	iPhone OS
Item 60	String	modelNumber
Item 61	String	MJ2T2
Item 62	String	advertisedName
Item 63	String	52075BDC
Item 64	String	systemBuildVersion
Item 65	String	12S507
Item 66	String	pairingID
▼ Item 67	Dictionary	(1 item)
NS.uuidbytes	Data	<1a3e2a70 892141a8 8e0ac26b 2535bcda>
Item 68	String	_bluetoothIdentifier
Item 69	String	pairingCompatibilityVersion
Item 70	String	systemVersion
Item 71	String	8.2
Item 72	String	isPaired

iOS Backup Data

/mobile/Library/DeviceRegistry.state/properties.bin

- Synced Data Path with GUID, date, local

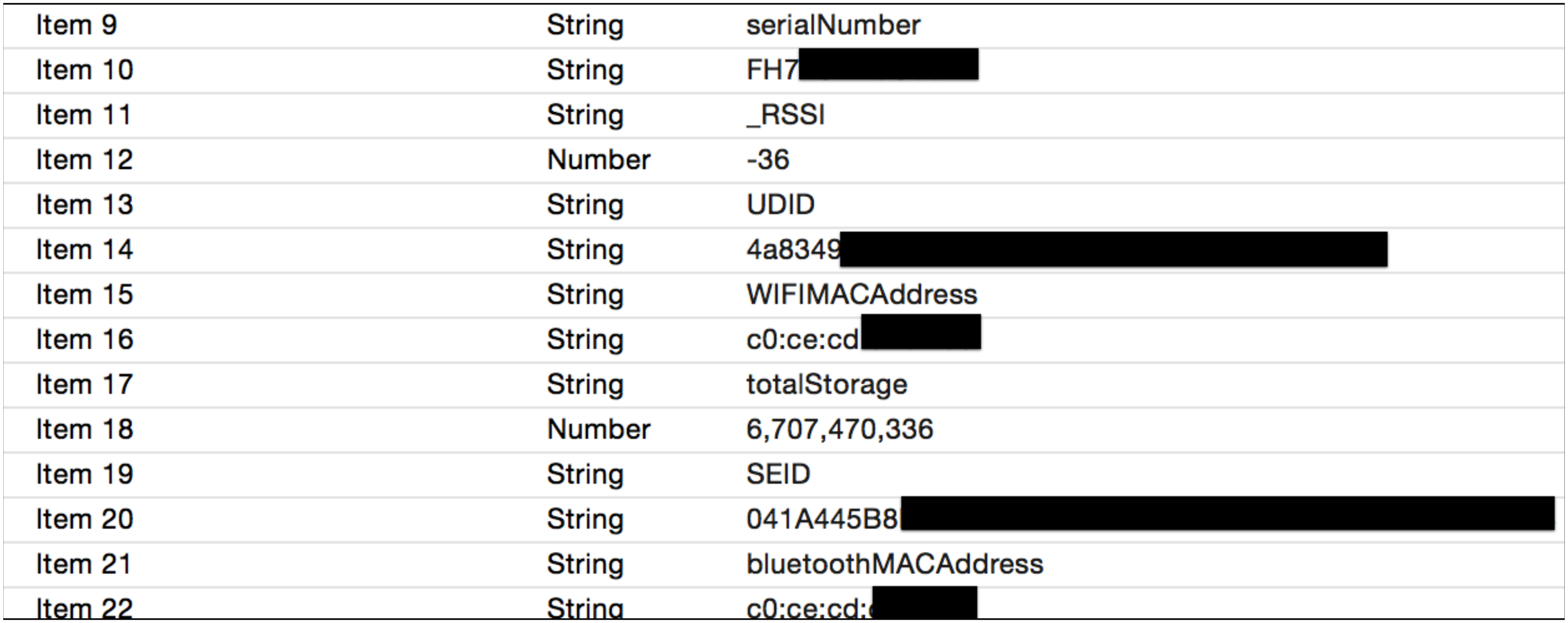


Item 19	String	currentUserLocale
Item 20	String	en_US
Item 21	String	deviceNameString
Item 22	String	Watch
Item 23	String	marketingVersion
Item 24	String	1.0
Item 25	String	localPairingDataStorePath
Item 26	String	/var/mobile/Library/DeviceRegistry/1A3E2A70-8921-41A8-8E0A-C26B2535BCDA
Item 27	String	pairingMinorVersion
Item 28	Number	0
Item 29	String	pairedDate
Item 30	Number	451,575,349.459805

iOS Backup Data

/mobile/Library/DeviceRegistry.state/secureProperties.bin

- Apple Watch Identifiers: Serial Number, UDID, WiFi MAC, SEID (Secure Element ID), Bluetooth MAC

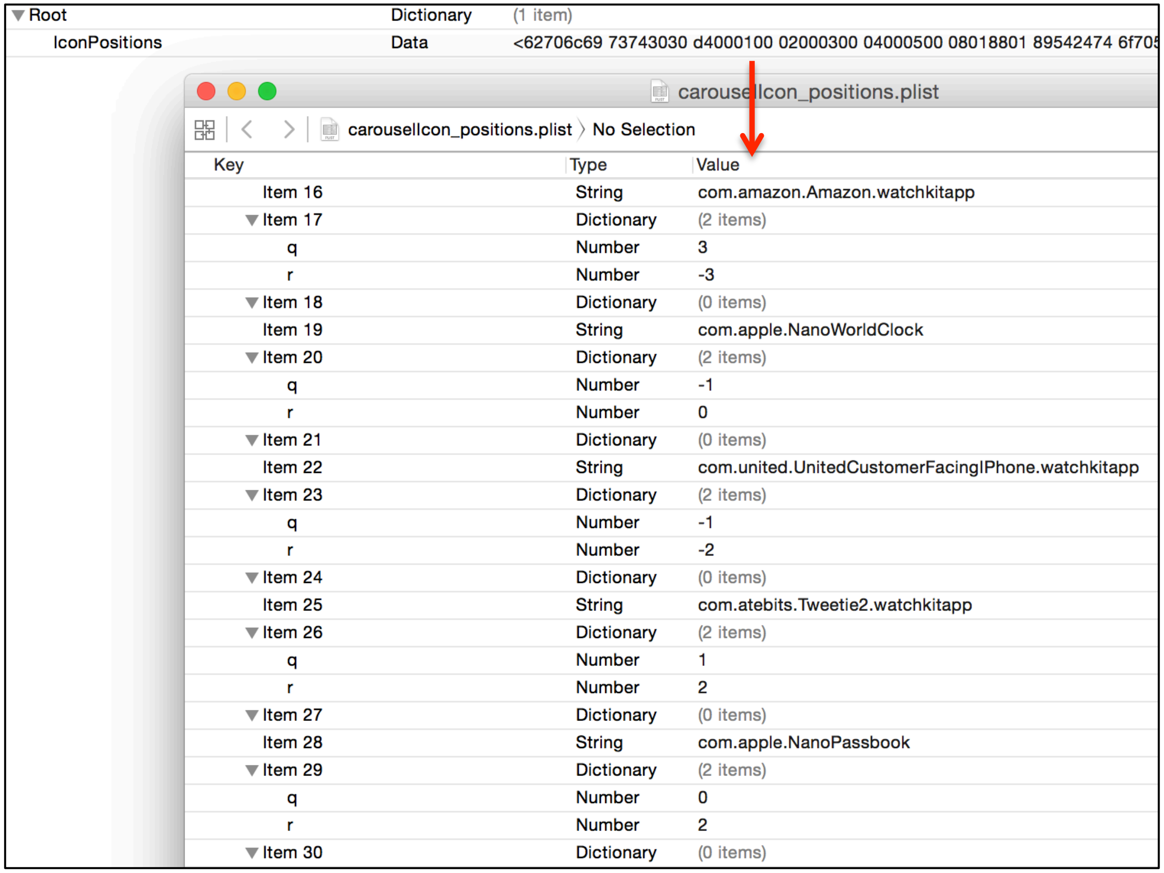


Item 9	String	serialNumber
Item 10	String	FH7[redacted]
Item 11	String	_RSSI
Item 12	Number	-36
Item 13	String	UDID
Item 14	String	4a8349[redacted]
Item 15	String	WIFIMACAddress
Item 16	String	c0:ce:cd[redacted]
Item 17	String	totalStorage
Item 18	Number	6,707,470,336
Item 19	String	SEID
Item 20	String	041A445B8[redacted]
Item 21	String	bluetoothMACAddress
Item 22	String	c0:ce:cd:[redacted]

Synced Data Directory – Installed Apps

/mobile/Library/DeviceRegistry/<GUID>/NanoPreferencesSync/NanoDomains/com.apple.Carousel

- Binary Plist w/ Embedded Plist containing installed apps on Apple Watch

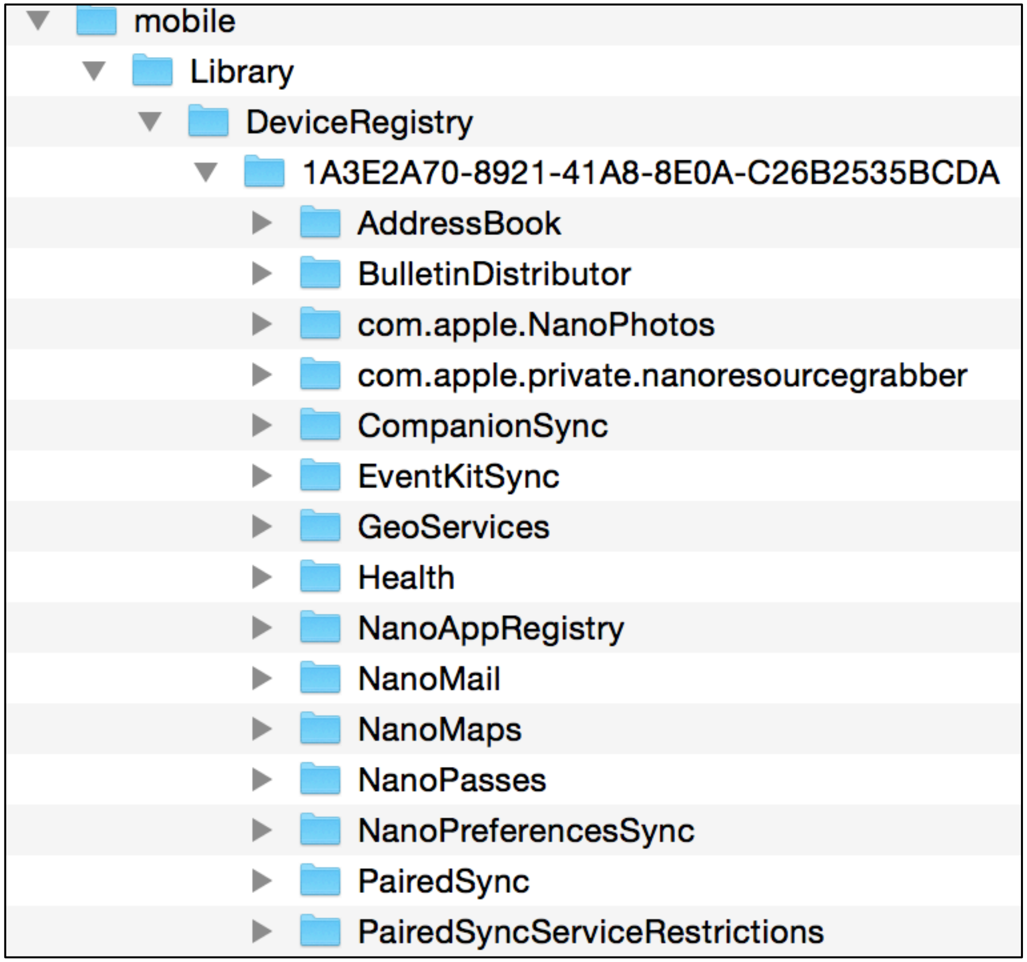


Root	Dictionary	(1 item)
IconPositions	Data	<62706c69 73743030 d4000100 02000300 04000500 08018801 89542474 6f70

carouselIcon_positions.plist
carouselIcon_positions.plist 〉 No Selection

Key	Type	Value
Item 16	String	com.amazon.Amazon.watchkitapp
▼ Item 17	Dictionary	(2 items)
q	Number	3
r	Number	-3
▼ Item 18	Dictionary	(0 items)
Item 19	String	com.apple.NanoWorldClock
▼ Item 20	Dictionary	(2 items)
q	Number	-1
r	Number	0
▼ Item 21	Dictionary	(0 items)
Item 22	String	com.united.UnitedCustomerFacingIPhone.watchkitapp
▼ Item 23	Dictionary	(2 items)
q	Number	-1
r	Number	-2
▼ Item 24	Dictionary	(0 items)
Item 25	String	com.atebits.Tweetie2.watchkitapp
▼ Item 26	Dictionary	(2 items)
q	Number	1
r	Number	2
▼ Item 27	Dictionary	(0 items)
Item 28	String	com.apple.NanoPassbook
▼ Item 29	Dictionary	(2 items)
q	Number	0
r	Number	2
▼ Item 30	Dictionary	(0 items)

Synced Data Directory
/mobile/Library/DeviceRegistry/<GUID>

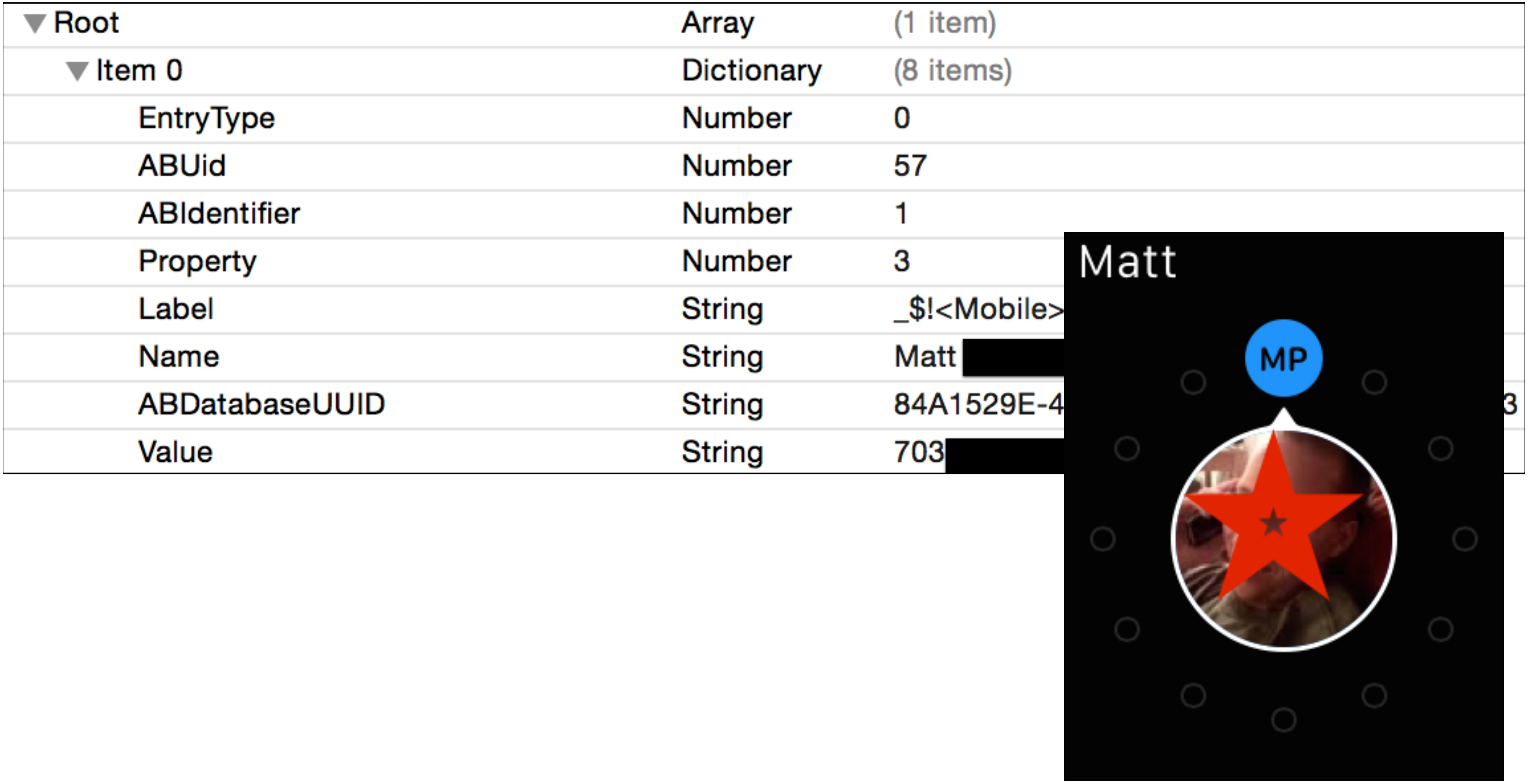


```
mobile
  Library
    DeviceRegistry
      1A3E2A70-8921-41A8-8E0A-C26B2535BCDA
        AddressBook
        BulletinDistributor
        com.apple.NanoPhotos
        com.apple.private.nanoresourcegrabber
        CompanionSync
        EventKitSync
        GeoServices
        Health
        NanoAppRegistry
        NanoMail
        NanoMaps
        NanoPasses
        NanoPreferencesSync
        PairedSync
        PairedSyncServiceRestrictions
```

Synced Data Directory - AddressBook

/mobile/Library/DeviceRegistry/<GUID>/AddressBook/

- favorites.previous - The Favorites List



▼ Root	Array	(1 item)
▼ Item 0	Dictionary	(8 items)
EntryType	Number	0
ABUid	Number	57
ABIdentifier	Number	1
Property	Number	3
Label	String	_$!<Mobile>
Name	String	Matt [redacted]
ABDatabaseUUID	String	84A1529E-4 3
Value	String	703 [redacted]

Synced Data Directory - Email
/mobile/Library/DeviceRegistry/<GUID>/NanoMail/registry.sqlite

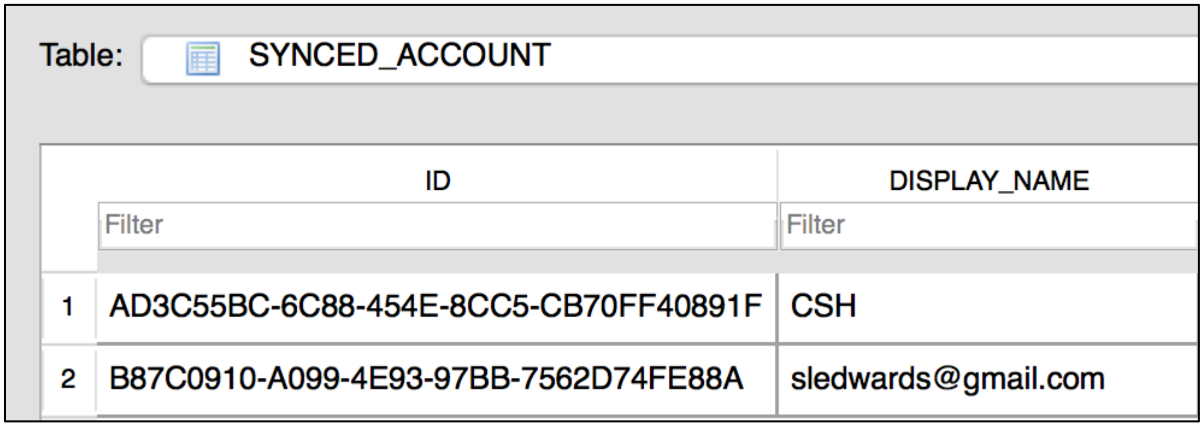


Table: SYNCED_ACCOUNT

	ID	DISPLAY_NAME
1	AD3C55BC-6C88-454E-8CC5-CB70FF40891F	CSH
2	B87C0910-A099-4E93-97BB-7562D74FE88A	sledwards@gmail.com

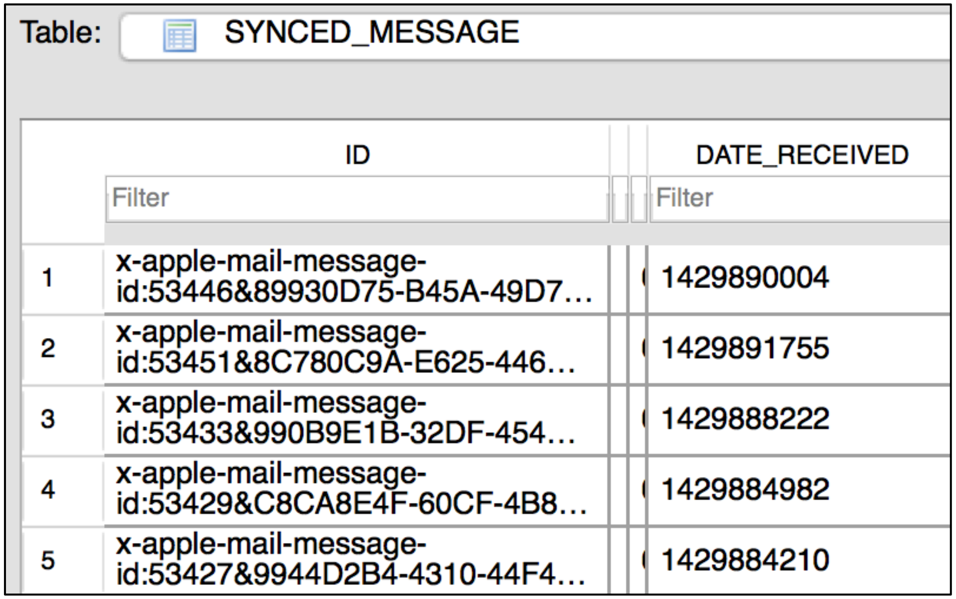


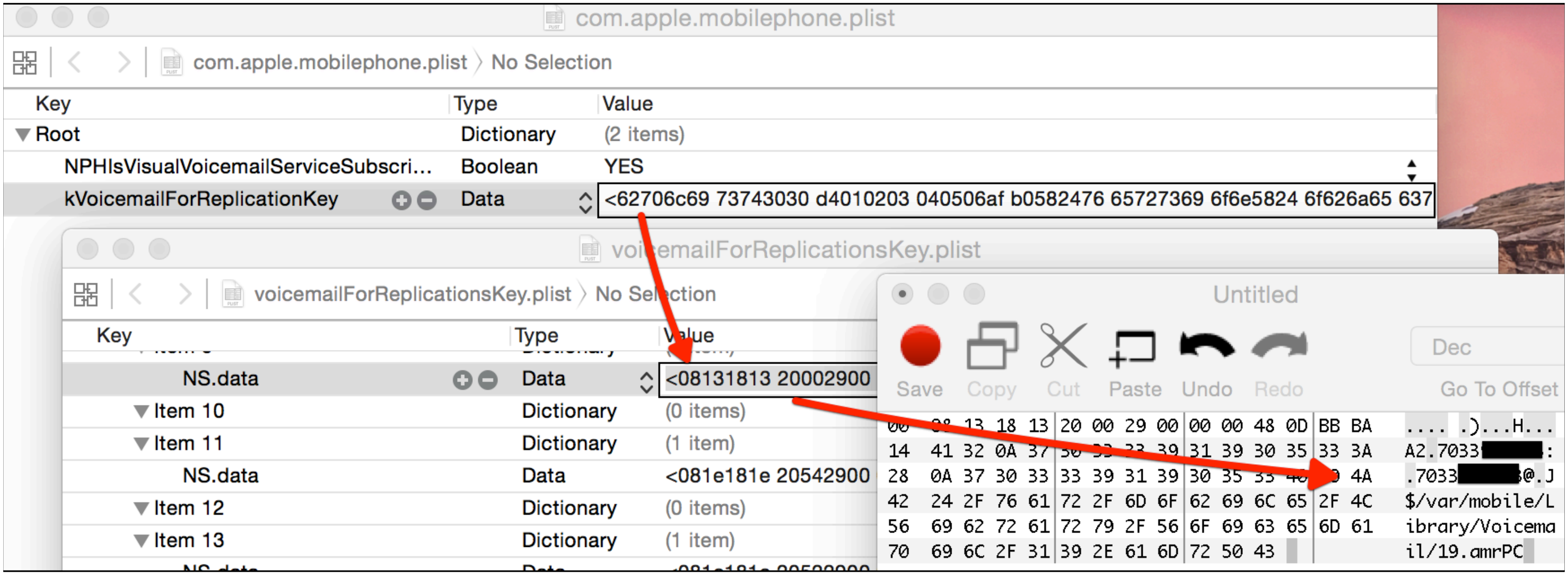
Table: SYNCED_MESSAGE

	ID	DATE_RECEIVED
1	x-apple-mail-message-id:53446&89930D75-B45A-49D7…	1429890004
2	x-apple-mail-message-id:53451&8C780C9A-E625-446…	1429891755
3	x-apple-mail-message-id:53433&990B9E1B-32DF-454…	1429888222
4	x-apple-mail-message-id:53429&C8CA8E4F-60CF-4B8…	1429884982
5	x-apple-mail-message-id:53427&9944D2B4-4310-44F4…	1429884210

Synced Data Directory – Voicemails

/mobile/Library/DeviceRegistry/<GUID>/PreferencesSync/
NanoDomains/com.apple.mobilephone

- Records containing Phone Numbers and paths to synced voicemail files.



com.apple.mobilephone.plist

com.apple.mobilephone.plist 〉 No Selection

Key	Type	Value
▼ Root	Dictionary	(2 items)
NPHIsVisualVoicemailServiceSubscri…	Boolean	YES
kVoicemailForReplicationKey	Data	<62706c69 73743030 d4010203 040506af b0582476 65727369 6f6e5824 6f626a65 637

voicemailForReplicationsKey.plist

voicemailForReplicationsKey.plist 〉 No Selection

Key	Type	Value
NS.data	Data	<08131813 20002900
▼ Item 10	Dictionary	(0 items)
▼ Item 11	Dictionary	(1 item)
NS.data	Data	<081e181e 20542900
▼ Item 12	Dictionary	(0 items)
▼ Item 13	Dictionary	(1 item)

Untitled

```
00 08 13 18 13 | 20 00 29 00 | 00 00 48 0D | BB BA    .... .)...H...
14 41 32 0A 37 | 30 33 33 39 | 31 39 30 35 | 33 3A    A2.7033[redacted]:
28 0A 37 30 33 | 33 39 31 39 | 30 35 33 40 | [illegible] 4A    .7033[redacted]@.J
42 24 2F 76 61 | 72 2F 6D 6F | 62 69 6C 65 | 2F 4C    $/var/mobile/L
56 69 62 72 61 | 72 79 2F 56 | 6F 69 63 65 | 6D 61    ibrary/Voicema
70 69 6C 2F 31 | 39 2E 61 6D | 72 50 43             il/19.amrPC
```

Synced Data Directory - PassBook /mobile/Library/DeviceRegistry/<GUID>/ NanoPasses/nanopasses.sqlite3

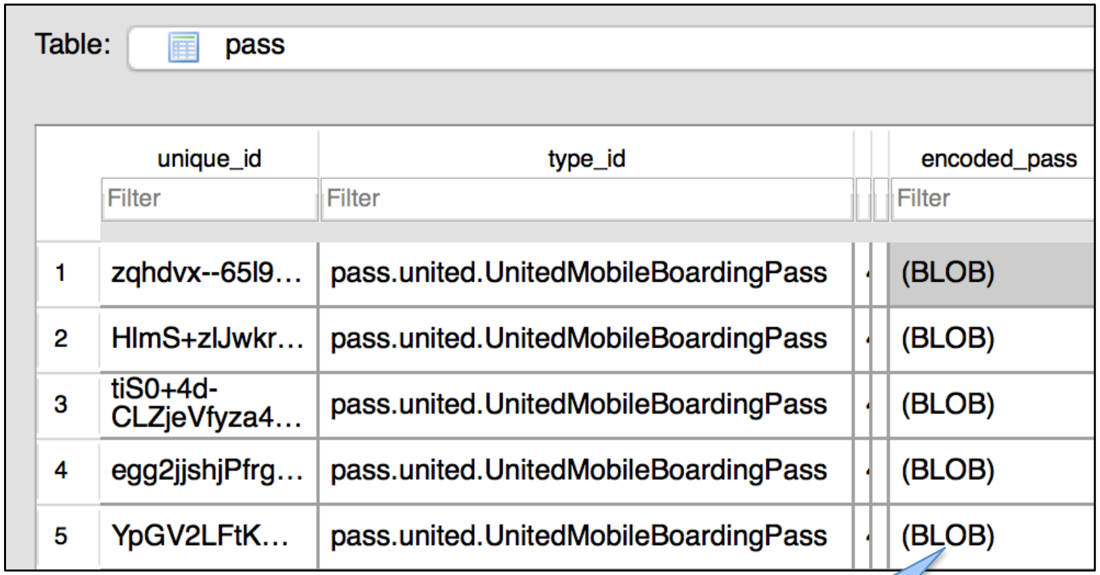
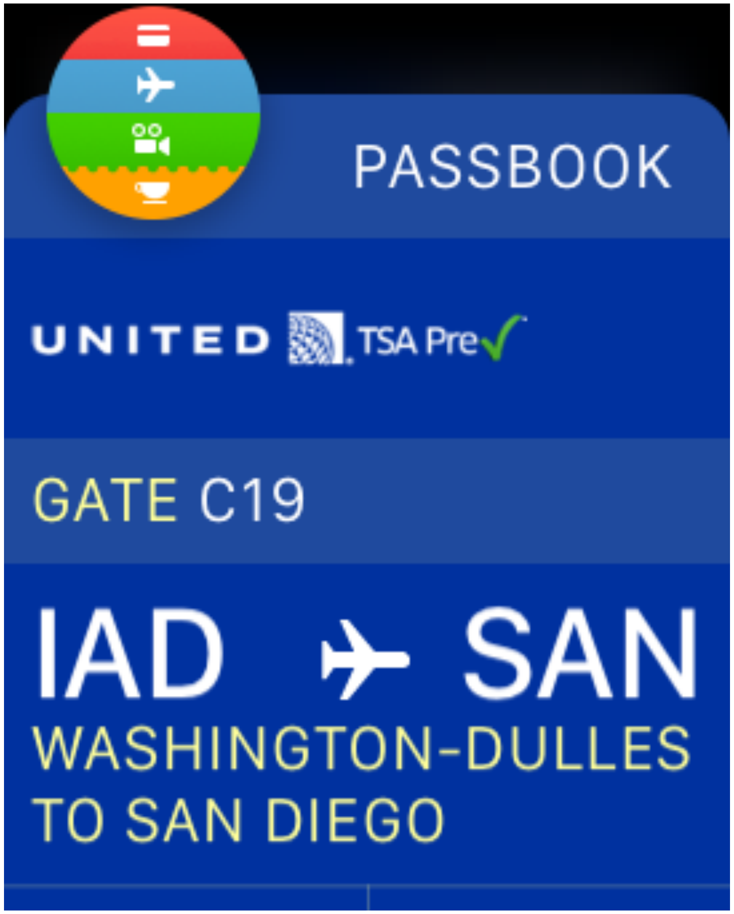


Table: pass

	unique_id	type_id	encoded_pass
	Filter	Filter	Filter
1	zqhdvx--65l9…	pass.united.UnitedMobileBoardingPass	(BLOB)
2	HlmS+zlJwkr…	pass.united.UnitedMobileBoardingPass	(BLOB)
3	tiS0+4d-CLZjeVfyza4…	pass.united.UnitedMobileBoardingPass	(BLOB)
4	egg2jjshjPfrg…	pass.united.UnitedMobileBoardingPass	(BLOB)
5	YpGV2LFtK…	pass.united.UnitedMobileBoardingPass	(BLOB)

Contains Pass Data!



Reality Check Caveat

- We spent a few hours looking into these.
- Only analyzed iOS Backup Files
- Digging Deeper…
  - 3rd Party Apps
  - iCloud Backups
  - Physical Imaging/Chip Off Possibilities
  - WiFi/Bluetooth Network Analysis

Shameless Plug

Vote for us…

- Digital Forensic Examiner of the Year – Sarah Edwards
- Forensic Book of the Year – Practical Mobile Forensics (Bommisetty, Mahalik & Tamma)

https://forensic4cast.com/forensic-4cast-awards/

Take our classes!

- FOR518 and FOR585