



# APPLE WATCH FORENSICS: IS IT EVER POSSIBLE, AND WHAT IS THE PROFIT?

MATTIA EPIFANI – VLADIMIR KATALOV

DFRWS 2019 EU

OSLO, 26 APRIL 2019

## SOURCES

- Backup of the synced iPhone (iTunes/iCloud)
- Device
  - Device info and installed applications
  - AFC acquisition
  - Manual acquisition
- Cloud (synced Health data)

## APPLE WATCH BACKUPS

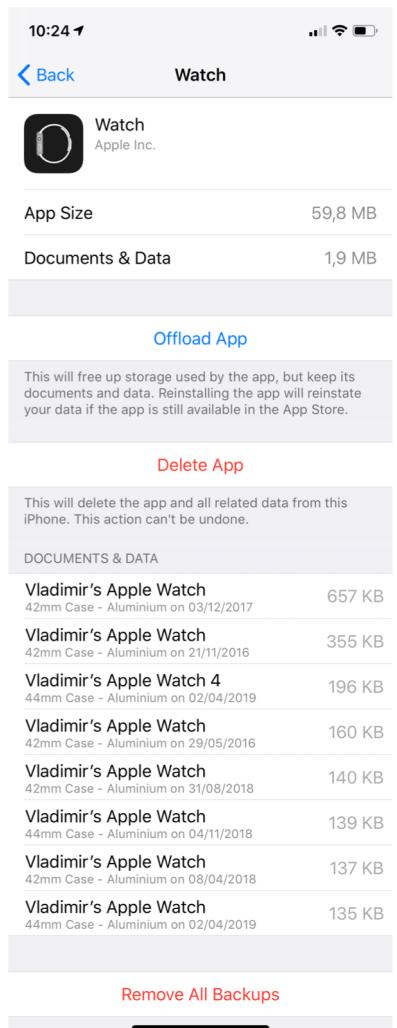
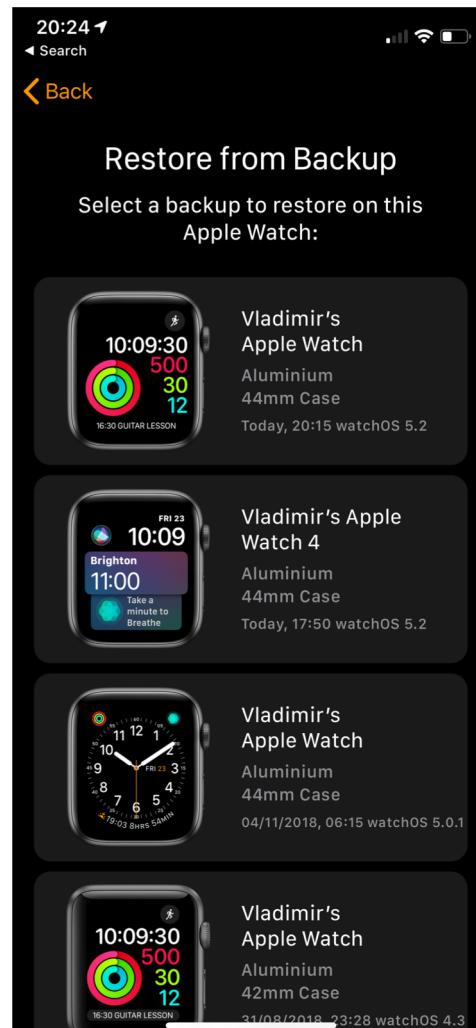
- Apple backs up Apple Watch data
- Comprehensive information at  
<https://support.apple.com/en-us/HT204518>
- Apple Watch content backs up automatically to your companion iPhone, so you can restore your Apple Watch from a backup.
- When you back up your iPhone to iCloud or iTunes, your iPhone backup will also include your Apple Watch data.

## APPLE WATCH BACKUPS

- Apple Watch automatically creates a backup on the iPhone when the user unpairs the Apple Watch from their iPhone
- Unpairing erases all data from the Apple Watch
- If the Apple Watch is unpaired while out of range of the paired iPhone, the backup might not have the latest data
- Users can re-pair their Apple Watch again and set it up from a backup
- We can extract Apple Watch backups from the iPhone and analyze the data

# APPLE WATCH BACKUPS

- List of backups if available on Watch when you try to restore
- On restore, watchOS version should match
- watchOS should match iOS version sometimes
- Some information is visible in the iPhone settings (General | iPhone Storage | Watch)
- No control, can only remove (all backups!!)



# APPLE WATCH BACKUPS:WHAT'S INSIDE?

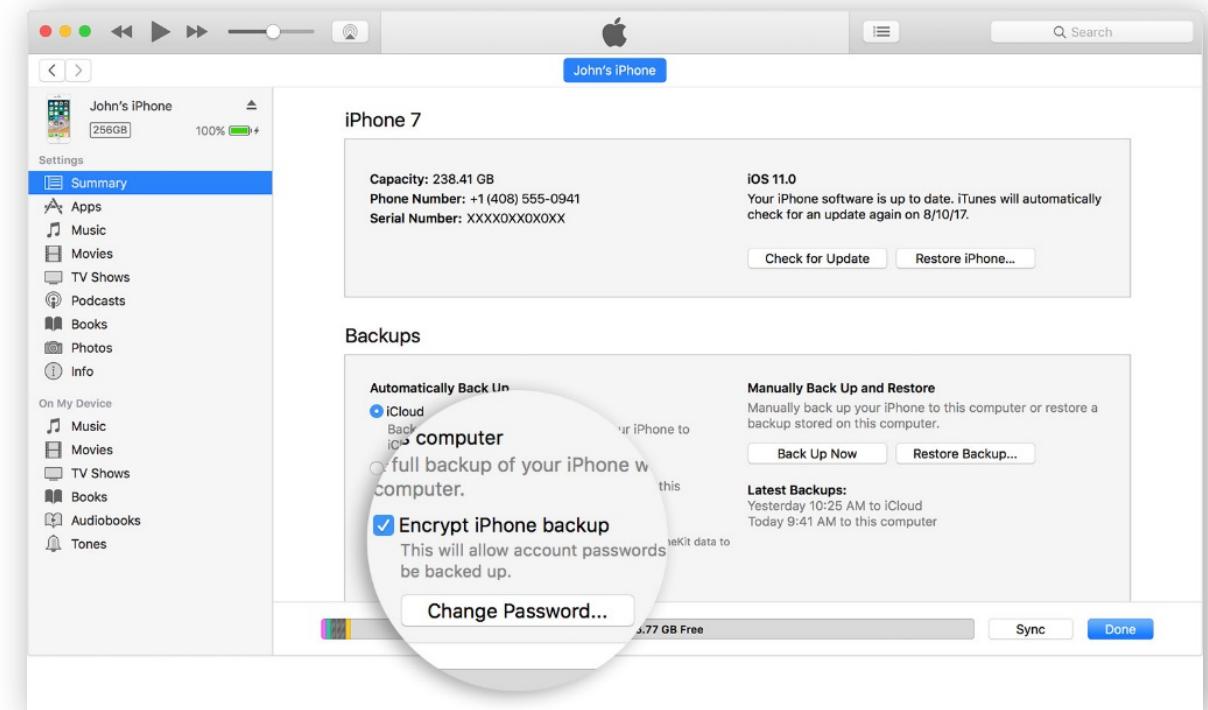
- Built-in apps: app data and settings
- Third-party apps: only settings
- Health and Fitness data: history, achievements, Workout and Activity calibration data, user-entered data
  - **To back up Health and Fitness data, you need to use iCloud or an encrypted iTunes backup.**
  - App layout on Home screen
  - Clock face and dock settings
  - Notification settings
  - Playlists, albums, and mixes
  - The Siri Voice Feedback setting
  - Synced photo album
  - Time Zone

## APPLE WATCH BACKUPS:WHAT'S **NOT** INCLUDED?

- Bluetooth pairings
- Credit or debit cards used for Apple Pay
- Apple Watch Passcode

# BACKUP EXTRACTION

- Apple Watch makes backups to synced iPhone
- Must obtain iPhone data to access Apple Watch backups
- iTunes backups of the synced iPhone are the easiest and most straightforward way to access Apple Watch data
- **Password-protected backups required to access the Watch Health and Fitness data!**



# APPLE WATCH IOS BACKUP

The screenshot shows a file management interface with a sidebar library and a main file list area.

**Library:**

- Library
- + Accessibility
- + Accounts
- + AddressBook
- + Application Support
- + Avatar
- + BulletinBoard
- + Calendar
- + CallHistoryDB
- + CallHistoryTransactions
- + ControlCenter
- + Cookies
- + DataAccess
- + DeviceRegistry
- + DeviceRegistry.state
- + DoNotDisturb

**File List:**

Name	Size	Permission	Date Modified
ClassAFile.txt	13	-rw-r--r--	11/04/17 11:47:30
UDIDChangeTracker.plist	272	-rw-r--r--	08/27/18 14:48:13
activeStateMachine.plist	1.3 kB	-rw-r--r--	12/28/18 11:17:37
history.plist	3.6 kB	-rw-r--r--	12/27/18 15:27:57
historySecureProperties.plist	1.1 kB	-rw-r--r--	09/15/18 09:48:46
recoveryManager-24620D1C-6016-4378-B7E9-7198D7F0C718.plist	1.8 kB	-rw-r--r--	09/15/18 09:51:20
stateMachine-24620D1C-6016-4378-B7E9-7198D7F0C718.plist	1.3 kB	-rw-r--r--	09/15/18 09:51:20

# APPLE WATCH IOS BACKUP – HISTORYSECUREPROPERTIES.PLIST

HomeDomain/Library/DeviceRegistry.state/historySecureProperties.plist

XML View List View

Key	Type	Value
...	dict	...
...	string	Unknown
...	string	R825F542-BCC2-46DD-A290-E80B472ABE29
...	string	b8:41:a4:14:37:df
...	string	04613B9BD249800180981429749463243BAA5B7A15DB60B9
...	string	b8:41:a4:12:e6:b7
...	string	GJ9X86F2J5X4
...	string	2a9fbea1643728ce72f820abd21cf5e854242341
Sarchiver	dict	NSKeyedArchiver
Stop	string	dict

WiFi Mac Address

BT Mac Address  
Serial Number  
UDID

The screenshot shows the Xcode XML Editor displaying the contents of the `historySecureProperties.plist` file. The file is a dictionary of key-value pairs. Several keys correspond to MAC addresses and other unique identifiers. The values for these keys are highlighted with blue boxes, and arrows point from these boxes to callout boxes on the right side of the screen, which list the extracted data: WiFi Mac Address, BT Mac Address, Serial Number, and UDID.

# APPLE WATCH IOS BACKUP – STATEMACHINE-<GUID>.PLIST

HomeDomain/Library/DeviceRegistry.state/stateMachine-24620D1C-6016-4378-B7E9-7198D7F0C718.plist

The screenshot shows a plist editor window displaying the contents of a file named "stateMachine-24620D1C-6016-4378-B7E9-7198D7F0C718.plist". The editor has tabs for "XML View" and "List View", with "List View" selected. The data is organized into a table with columns for "Key", "Type", and "Value".

Key	Type	Value
Root	dict	
\$version	integer	100000
\$objects	array	\$null
finalizePairing	string	
69647CEB	string	
pairSuccess	dict	15U70
PBBuddyControllerFinishe	string	
558690521.293583	real	
NS.time	dict	
\$class	dict	
NSKeyedArchiver	string	NSKeyedArchiver
Stop	dict	

A callout box highlights the "pairSuccess" key and its value "15U70". Arrows point from this value to three descriptive boxes:

- Pair status
- WatchOS Version installed at time of pairing
- Pairing timestamp (Apple Cocoa Core Data)

# APPLE WATCH IOS BACKUP – ACTIVESTATEMACHINE.PLIST

HomeDomain/Library/DeviceRegistry.state/activeStateMachine.plist

XML View List View

Key	Type	Value
Root	dict	
\$version	integer	100000
\$objects	array	\$null
\$+	string	paired
\$+	dict	69647CEB
pairSuccess	string	15U70
\$+	dict	NT2TbAP
\$+	string	16R600
\$+	dict	PBBuddyControllerFinishe
\$+	real	558690521.293583
\$class	dict	
\$+	dict	
\$+	dict	
\$+	dict	

Pair status

WatchOS Version installed at time of pairing

Actually installed WatchOS Version

Pair timestamp (Apple Cocoa Core Data)

# APPLE WATCH IOS BACKUP – DEVICEREGISTRY

Name	Size	Permission	Date Modified	Date Created
24620D1C-6016-4378-B7E9-7198D7F0C718	2.9 MB	drwxr-xr-x	11/13/18 02:19:47	09/15/18 09:48:43

DeviceRegistry

- 24620D1C-6016-4378-B7E9-7198D7F0C718
  - AddressBook
  - BulletinDistributor
  - CoreLocation
  - EventKitSync
  - NanoAppRegistry
  - NanoMail
  - NanoPasses
  - NanoPreferencesSync
  - PairedSync
  - com.apple.NanoPhotos
  - com.apple.private.nanoresourcegrabber
  - com.apple.sharing
  - com.apple.tccd
- DeviceRegistry.state

# APPLE WATCH IOS BACKUP – NANOAPPREGISTRY

The screenshot displays a file browser interface with two main panes. The left pane, titled 'Backups', shows a tree view of a backup folder structure. One of the expanded folders is 'NanoAppRegistry', which contains a subfolder 'Applications' and several individual application entries, such as 'Alitalia.watchkitapp', 'at.runtastic.gpssportapp.watchapp', and 'com.apple.ActivityMonitorApp'. The right pane shows the detailed contents of a file named 'Application.dat'. This file is located at 'HomeDomain/Library/DeviceRegistry/24620D1C-6016-4378-B7E9-7198D7F0C718/NanoAppRegistry/Applications/com.facebook.Messenger.watchkitapp'. The file is displayed in 'XML View', with tabs for 'XML View' and 'List View'. The XML structure is as follows:

Key	Type	Value
CFBundleVersion	string	1.0 kB
CFBundleDisplayName	string	-rw-r--r--
CFBundleShortVersionString	string	12/28/18 22:08:29
CFBundleIdentifier	string	12/28/18 22:08:29
CFBundleName	string	
135382157	string	
Messenger	string	
196.0	string	
com.facebook.Messenger.watchkitapp	string	
MessengerWatchAppBundle	string	
NS.keys	array	
NS.objects	array	
\$class	dict	
itemName	string	
artistName	string	
Facebook, Inc.	string	
488	integer	
User	string	

# APPLE WATCH IOS BACKUP – NANOMAIL\REGISTRY.SQLITE

The screenshot shows the SQLite Database Browser interface. On the left, a tree view displays the backup structure with folders like NanoAppRegistry, NanoMail, NanoPasses, NanoPreferencesSync, and PairedSync. The main area shows the contents of the registry.sqlite database, which contains a single table named SYNCED\_ACCOUNT.

ID	DISPLAY_NAME	SHOULD_ARCHIVE	EMAIL_ADDRESSES	RESEND_REQUESTED	RESEND_INTERVAL	SOURCE_TYPE	USERNAME	LOCAL_ID
1	Digital Forensics	1		1	0	0		S4A03817-58F4-4A6F-9A76-A2E80FB88B9D
2	Segreteria	1		1	0	0		FB0F621D-BDD8-466E-8307-4E7050E029DA
3	Info reality	1		1	0	0		D811EEA3-4148-4738-BC6B-BC5372D0C7F8
4	RealityNet	1		1	0	0		CEFCCB9B-9F86-46E4-A9DE-FBE52D616EFD
5	DFA	1		1	0	0		DA4E8765-53E3-48F8-8C40-6901CBCEFA9E
6	Hotmail	0		1	0	0		019684EA-73A3-4E74-B8A5-C820CD27C005
7	Outlook	0		1	0	0		72E4633E-5E97-4653-8E4F-60EEB2D283E6

# APPLE WATCH IOS BACKUP – NANOPASSES\NANOPASSES.SQLITE3

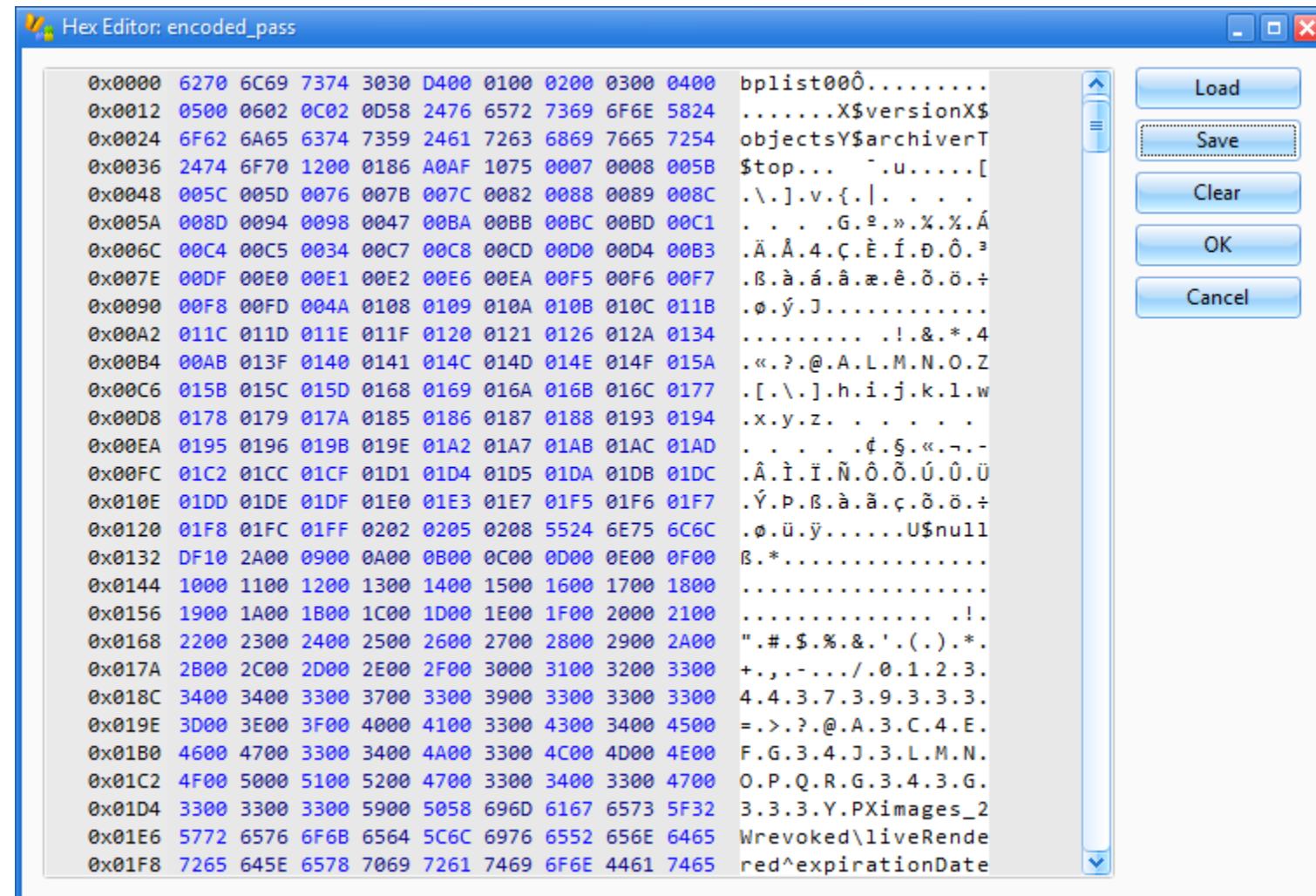
Backups

Name	Size	Permission	Date Modified	Date Created
Catalog.archive	771	-rw-r--r--	11/12/18 23:02:42	11/12/18 23:02:42
PassSyncEngine.archive	1.5 kB	-rw-r--r--	12/15/18 22:23:16	12/15/18 22:23:16
PaymentCards	0	drwxr-xr-x	09/15/18 09:51:20	09/15/18 09:51:20
nanopasses.sqlite3	1.1 MB	-rw-r--r--	12/15/18 22:23:14	09/15/18 09:51:20

unique_id	type_id	organization_name	ingested_date	localized_description
Oc+NJo83fq3-17eDWmzVSyHPfzU=	pass.com.booking.reservation	Booking.com	563059511	<p>Situato nel quartiere Jordaan di Amsterdam, il moderno Bank Hotel si trova nell'antico edificio di una ex banca sulla via Haarlemmerstraat, e offre eleganti camere con decorazioni sobrie, letti particolarmente lunghi e TV satellitare a schermo piatto.</p> <p>Dotate di una vista sulla città, tutte le sistemazioni del Bank Hotel sono insonorizzate, e dispongono di aria condizionata, scrivania e bagno in stile contemporaneo con doccia. Come ospiti della struttura potrete usufruire della connessione Wi-Fi gratuita nelle aree comuni.</p> <p>Il Bank Hotel si trova a meno di 10 minuti a piedi dalla Stazione ferroviaria centrale di Amsterdam e dalla Casa di Anna Frank, e a 15 minuti di cammino da Piazza Dam, che ospita il Palazzo Reale.</p>
?IQx8nkFxkN4p+KDe8lZ0ViNJqag=	pass.com.bestwestern.rewards	Best Western Rewards®	558690775	Go. Get. Rewarded.

# APPLE WATCH IOS BACKUP – NANOPASSES\NANOPASSES.SQLITE3



# APPLE WATCH IOS BACKUP – NANOPASSES\NANOPASSES.SQLITE3

Key	Type	Value
	string	The Bank Hotel
	dict	
	dict	
	dict	
	string	hotelAddress
	string	ADDRESS
	string	Haarlemmerstraat 120, Amsterdam
	dict	
	dict	
	integer	3
	string	guestName
	string	GUEST NAME
	string	Mattia Epifani
	string	Updated guest name is %@
	dict	
	string	totalPrice
	string	TOTAL PRICE
	string	€215,00
	integer	215
	string	New price is %@
	string	EUR
	dict	

Key	Type	Value
	string	The Bank Hotel
	dict	
	string	reservationDetails
	string	Reservation
	string	Booking Number: 1198.273.413
	dict	
	string	checkinDateTime
	string	Check-in
	string	2018-11-08 14:00
	dict	
	string	checkoutDateTime
	string	Check-out
	string	2018-11-09 11:00
	string	New check out date is %@
	dict	
	string	myReservationUrl
	string	View or change your booking:
	string	<a href="https://secure.booking.com/myreservations.html?bn=1198273413;pincode=9181;">https://secure.booking.com/myreservations.html?bn=1198273413;pincode=9181;</a>

# APPLE WATCH HEALTH DATA IN LOCAL (ENCRYPTED) BACKUPS

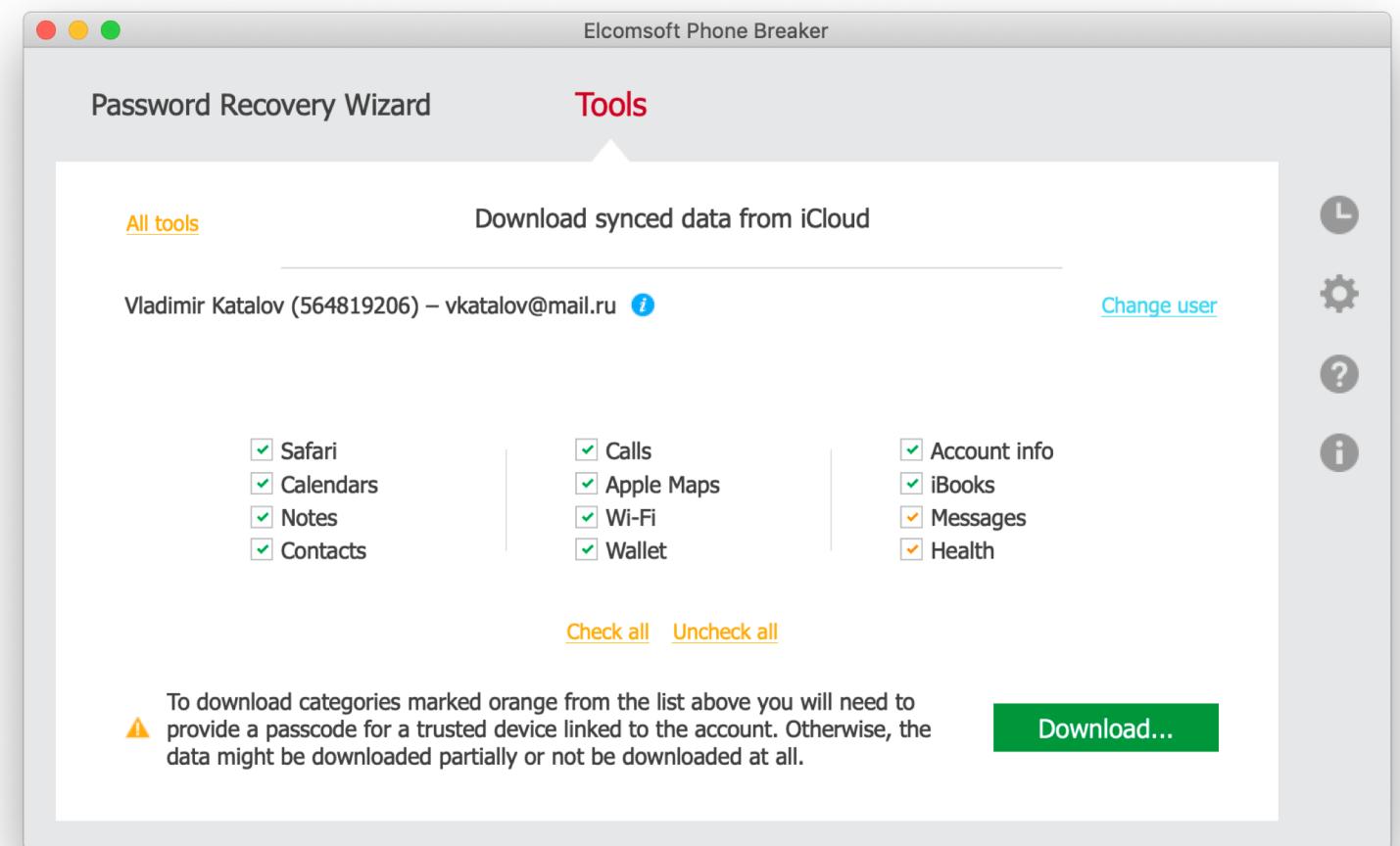
- Most data comes into *Activity* category
- GPS locations are available in *Workouts* category only
- Other useful categories: *Steps*, *Walking/running distance*, *Mindfulness*, *Heart rate*
- No *Sleep* data comes from Watch
- We have not found ECG data yet, sorry

The screenshot shows the Elcomsoft Phone Viewer interface, specifically the 'Health' section. The left sidebar displays a filter panel with 'From: 01.01.2001' and 'Until: 19.04.2019'. Below this are two sections: 'Source' and 'Device'. The 'Source' section lists various apps: Pokémon GO, Strava, Vladimir's Apple Watch 3, Workouts++, Runtastic, Nike Run Club, Vladimir's Apple Watch 4, and Vladimir's Watch 4 (US). The 'Device' section lists: Apple Watch, iPhone X (GSM), Apple Watch Series 3, Apple Watch Series 4 (GPS), and Apple Watch Series 4 (GPS+Cellular). The main area is titled 'Health' and contains a search bar and a navigation bar with icons for User Info, Activity, Body Measurements, Heart, Mindfulness, Nutrition, Reproductive, Results, Sleep, and Vitals. Below the navigation bar, there is a summary: 'Records: 62' and 'Shown records: 62'. It also shows the most recent record (08.04.2019 21:33:41 UTC -4) and the oldest record (08.04.2016 05:03:13 UTC -4). A table below lists the data records with columns: Start Date, End Date, Date Added, Source, Device, Details, and Workout type. The first few rows show entries for Walking, Cycling, and Walking.

Start Date	End Date	Date Added	Source	Device	Details	Workout type
08.04.2019 20:01:56 (U...)	08.04.2019 21...	08.04.2019 21:3...	Workouts++	Apple Watch Series 4 (GPS+C...	Hardware version: Watch4,4 ...	Walking
08.04.2019 20:01:47 (U...)	08.04.2019 20...	08.04.2019 20:0...	Workouts++	Apple Watch Series 4 (GPS+C...	Hardware version: Watch4,4 ...	Cycling
08.04.2019 19:59:01 (U...)	08.04.2019 21...	08.04.2019 21:3...	Vladimir's W...	Apple Watch Series 4 (GPS+C...	Hardware version: Watch4,4 ...	Walking
12.01.2019 14:13:23 (U...)	12.01.2019 14...	12.01.2019 14:5...	Vladimir's A...	Apple Watch Series 4 (GPS)	Hardware version: Watch4,2 ...	Walking
03.12.2018 10:04:59 (U...)	03.12.2018 10...	03.12.2018 10:4...	Vladimir's A...	Apple Watch Series 4 (GPS)	Hardware version: Watch4,2 ...	Core Training
17.11.2018 12:11:49 (U...)	17.11.2018 12...	17.11.2018 12:1...	Vladimir's A...	Apple Watch Series 4 (GPS)	Hardware version: Watch4,2 ...	Elliptical
01.10.2018 12:19:17 (U...)	01.10.2018 13...	01.10.2018 13:0...	Vladimir's A...	Apple Watch Series 3	Hardware version: Watch3,4 ...	Walking
18.09.2018 17:04:45 (U...)	18.09.2018 17...	21.09.2018 12:0...	Vladimir's A...	Apple Watch Series 3	Hardware version: Watch3,4 ...	Other
02.09.2018 12:00:47 (U...)	02.09.2018 12...	02.09.2018 12:0...	Runtastic	iPhone X (GSM)	Hardware version: iPhone10,...	Running
28.08.2018 17:00:44 (U...)	28.08.2018 17...	28.08.2018 17:0...	Nike Run Club	iPhone X (GSM)	Hardware version: iPhone10...	Running

# APPLE WATCH HEALTH DATA SYNCED WITH THE CLOUD

- No Health data in iCloud backups
- Health data is synced into the cloud since iOS 11
- Starting with iOS 12, it is saved in secure container; 2FA is required
- ECG data is not synced
- The key to encrypted data is protected with iCloud Keychain
- iCloud Keychain can be accessed only by trusted devices
- To become trusted, one should know the passcode/password to one of existing trusted devices

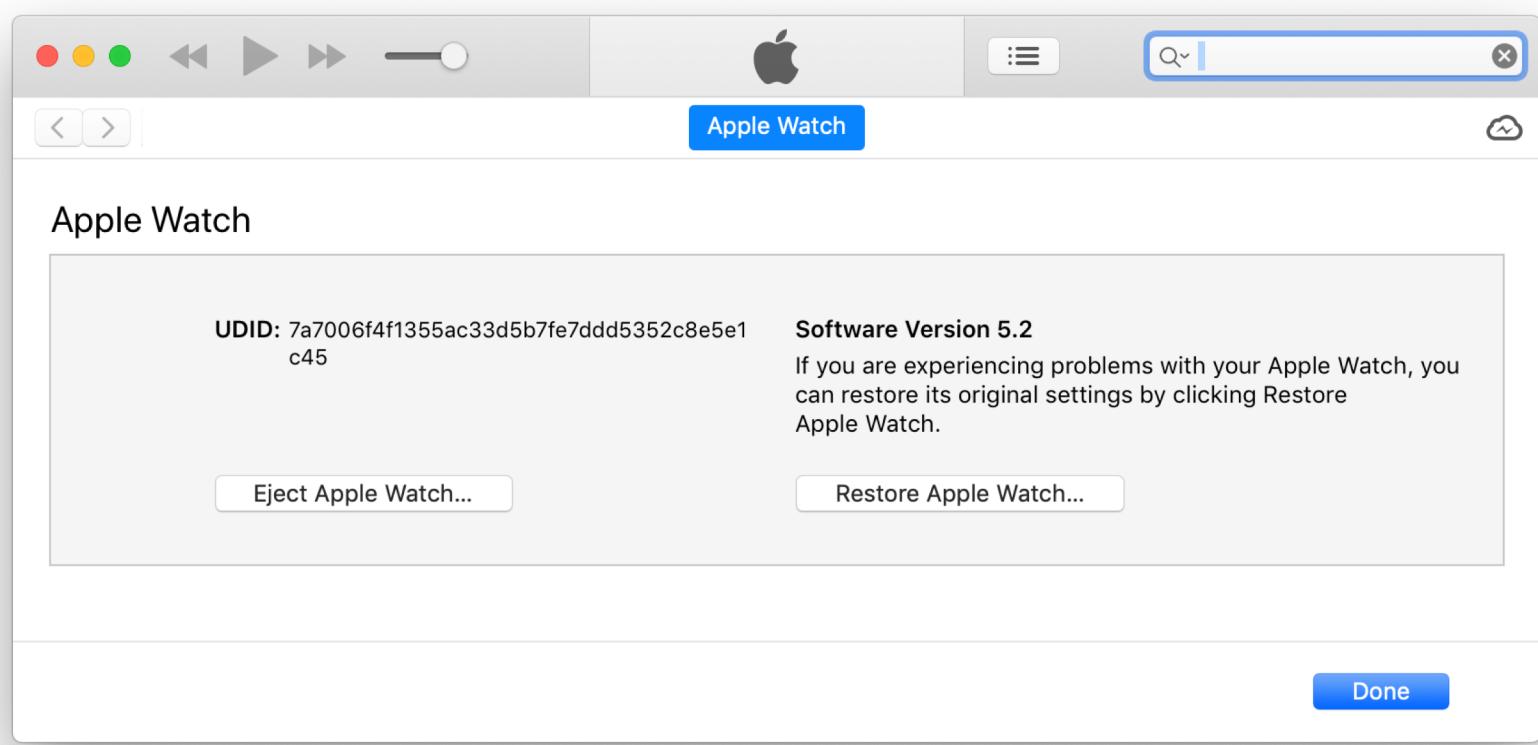
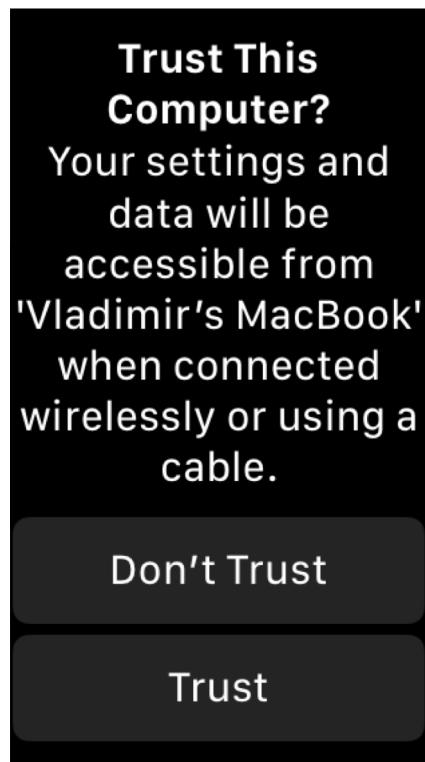


# APPLE WATCH CONNECTION WITH iBUS

[HTTPS://WWW.MFCBOX.COM/SHOP/CATEGORY/IBUS-TOOLS/](https://www.mfcbox.com/shop/category/ibus-tools/)

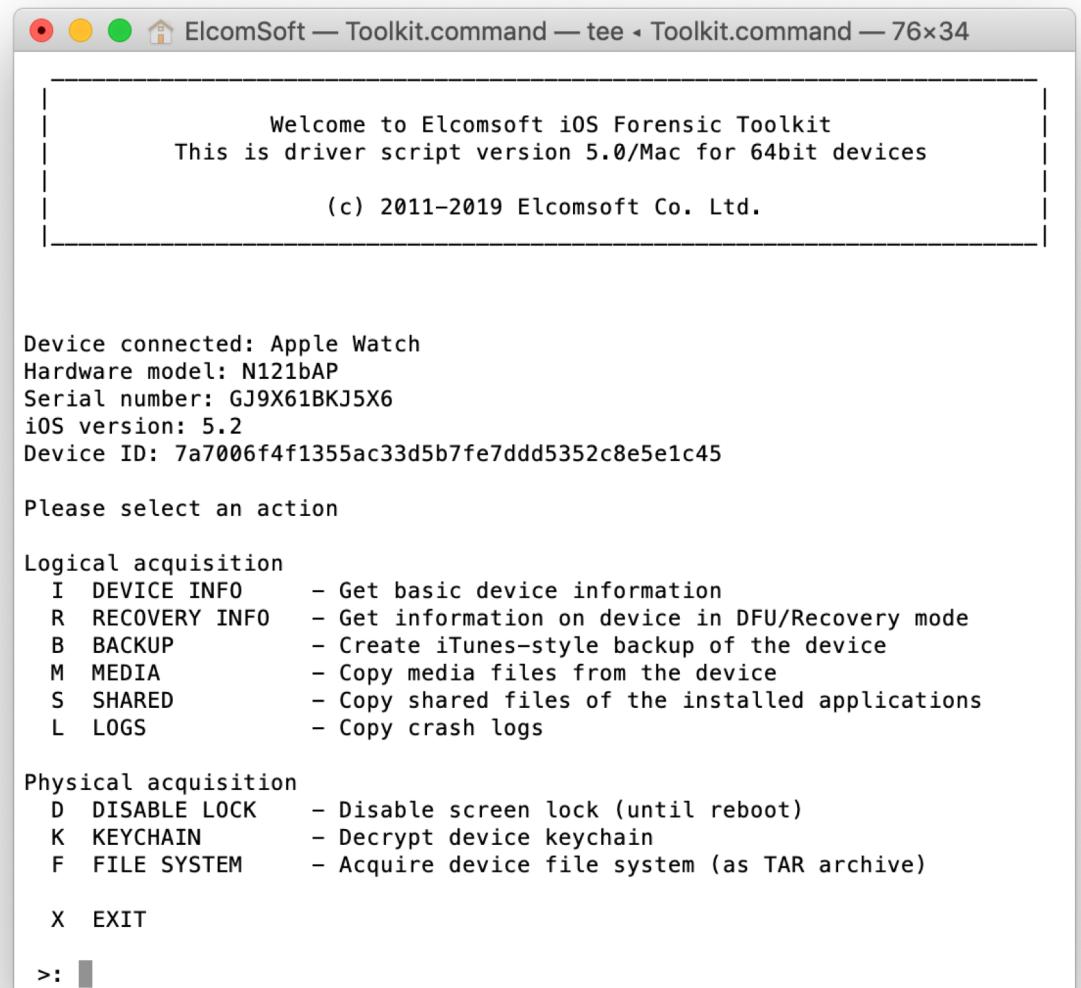


# APPLE WATCH PAIRING



# APPLE WATCH ACQUISITION OPTIONS

- Physical acquisition **might** be available with a jailbreak  
(e.g. *vortex* exploit for watchOS 3.0-4.1)
- **No backup service is running on watchOS**
- Device information is available
- List of installed applications can be obtained
- Shared files: *sometimes* work, but a very limited number of Watch apps use that
- AFC (Apple File Conduit) is the only reliable method
- Log files can also help!



Welcome to Elcomsoft iOS Forensic Toolkit  
This is driver script version 5.0/Mac for 64bit devices  
(c) 2011-2019 Elcomsoft Co. Ltd.

Device connected: Apple Watch  
Hardware model: N121bAP  
Serial number: GJ9X61BKJ5X6  
iOS version: 5.2  
Device ID: 7a7006f4f1355ac33d5b7fe7ddd5352c8e5e1c45

Please select an action

Logical acquisition

I DEVICE INFO	- Get basic device information
R RECOVERY INFO	- Get information on device in DFU/Recovery mode
B BACKUP	- Create iTunes-style backup of the device
M MEDIA	- Copy media files from the device
S SHARED	- Copy shared files of the installed applications
L LOGS	- Copy crash logs

Physical acquisition

D DISABLE LOCK	- Disable screen lock (until reboot)
K KEYCHAIN	- Decrypt device keychain
F FILE SYSTEM	- Acquire device file system (as TAR archive)

X EXIT

>:

# APPLE WATCH EXTRACT APP LIST

```
ElcomSoft — Toolkit.command — tee < Toolkit.command — 76x21

-----
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.0/Mac for 64bit devices

(c) 2011-2019 Elcomsoft Co. Ltd.

Device connected: Apple Watch
Hardware model: N121bAP
Serial number: GJ9X61BKJ5X6
iOS version: 5.2
Device ID: 7a7006f4f1355ac33d5b7fe7ddd5352c8e5e1c45

Device paired
[Write device info to file <ideviceinfo.plist>:  

[Write installed applications list to file <applications.txt>:  

[Write full installed applications info to file <applications.plist>: ]]
```

# APPLE WATCH EXTRACT LOGS

```
ElcomSoft — Toolkit.command — tee < Toolkit.command — 76x38

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.0/Mac for 64bit devices

(c) 2011-2019 Elcomsoft Co. Ltd.

Device connected: Apple Watch
Hardware model: N121bAP
Serial number: GJ9X61BKJ5X6
iOS version: 5.2
Device ID: 7a7006f4f1355ac33d5b7fe7ddd5352c8e5e1c45

Device paired
Write copied files to directory </Logs>:
Copy: WiFi/WiFiManager/wifi-buf-03-30-2019_15:09:13.517.log
Copy: WiFi/WiFiManager/wifi-buf-03-30-2019_17:05:44.236.log
Copy: WiFi/WiFiManager/wifi-buf-03-30-2019_17:05:44.219.log
Copy: WiFi/WiFiManager/wifi-buf-03-30-2019_15:09:13.590.log
Copy: DiagnosticLogs/sysdiagnose/IN_PROGRESS_sysdiagnose_2019.03.28_18-33-11
+0300_Watch_OS_Watch_16S535.tmp/ASPSnapshots/asptool_snapshot_timesensitive.
log
Copy: DiagnosticLogs/sysdiagnose/sysdiagnose_2019.03.30_15-08-48+0100_Watch_
OS_Watch_16T225.tar.gz
Copy: DiagnosticLogs/sysdiagnose/sysdiagnose_2019.03.30_17-05-20+0300_Watch_
OS_Watch_16T225.tar.gz
Copy: DiagnosticLogs/sysdiagnose/IN_PROGRESS_sysdiagnose_2019.03.28_18-33-11
+0300_Watch_OS_Watch_16S535.tar.gz
Copy: DiagnosticLogs/sysdiagnose/IN_PROGRESS_sysdiagnose_2019.03.28_18-33-11
+0300_Watch_OS_Watch_16S535-diagnostic_summary.log
Copy: DiagnosticLogs/Bridge-Pair-Performance-Report-575487600.907473.txt
Copy: ota_patch.txt
Done.
Press 'Enter' to continue
```

# APPLE WATCH MEDIA FILES

```
ElcomSoft — Toolkit.command — tee < Toolkit.command — 77x23

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.0/Mac for 64bit devices

(c) 2011-2019 Elcomsoft Co. Ltd.

Device connected: Apple Watch
Hardware model: N121bAP
Serial number: GJ9X61BKJ5X6
iOS version: 5.2
Device ID: 7a7006f4f1355ac33d5b7fe7ddd5352c8e5e1c45

Device paired
[Write copied files to directory <~/AFC>:
Copying file /DCIM/100APPLE/IMG_0017.JPG: OK
Copying file /DCIM/100APPLE/IMG_0003.JPG: OK
Copying file /DCIM/100APPLE/IMG_0002.JPG: OK
Copying file /DCIM/100APPLE/IMG_0016.JPG: OK
Copying file /DCIM/100APPLE/IMG_0028.JPG: OK
```

```
ElcomSoft — Toolkit.command — tee < Toolkit.command — 77x23

Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0024.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0030.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0018.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0019.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0031.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0025.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0033.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0027.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0026.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0032.JPG/5003.JPG: OK
Copying file /PhotoData/Photos.sqlite: OK
Copying file /PhotoData/MISC/DCIM_APPLE.plist: OK
Copying file /PhotoData/Photos.sqlite-wal: OK
Copying file /PhotoData/Photos.sqlite-shm: OK

Copying finished

Statistics:
    Total files: 235
    Copy OK: 235
    Copy FAILED: 0
Press 'Enter' to continue
```

# APPLE WATCH DEVICE INFO – ELCOMSOFT IOS FORENSIC TOOLKIT

Field name	Field value
Hardware Model	N121bAP
Serial Number	GJ9X86F2J5X4
Bluetooth Address	b8:41:a4:12:e6:b7
WiFi Address	b8:41:a4:14:37:df
UniqueDeviceID	2a9fbea1643728ce72f820abd21cf5e85424234
DeviceName	Apple Watch di Mattia
ProductType	Watch3,4
ProductVersion	5.1.1
BuildVersion	16R600
TimeZone	Europe/Rome
TimeZoneOffsetFromUTC	3600.000000
TimeIntervalSince1970	1544289361.799742 (Saturday 8 December 2018 17:16:01.799)
Language	IT

# APPLE WATCH INSTALLED APPLICATIONS – ELCOMSOFT IOS FORENSIC TOOLKIT

Field name	Field value
ApplicationDSID	1321761630
Path	/private/var/containers/Bundle/Application/83A3C4E9-F7A7-4813-AE28-311494787654/MessengerWatchAppBundle.app
CFBundleExecutable	MessengerWatchAppBundle
CFBundleName	Messenger
CFBundleVersion	133700421
LSRequiresiPhoneOS	True
WKCompanionAppBundleIdentifier	com.facebook.Messenger
Container	/private/var/mobile/Containers/Data/Application/1B9A093B-A9D6-4165-9396-47FC60C9F0F8

# APPLE WATCH LOGS

C:\Users\mattia\Desktop\iOS-Toolkit-5.0-Win\Logs\DiagnosticLogs\sysdiagnose\sysdiagnose\_2019.04.2

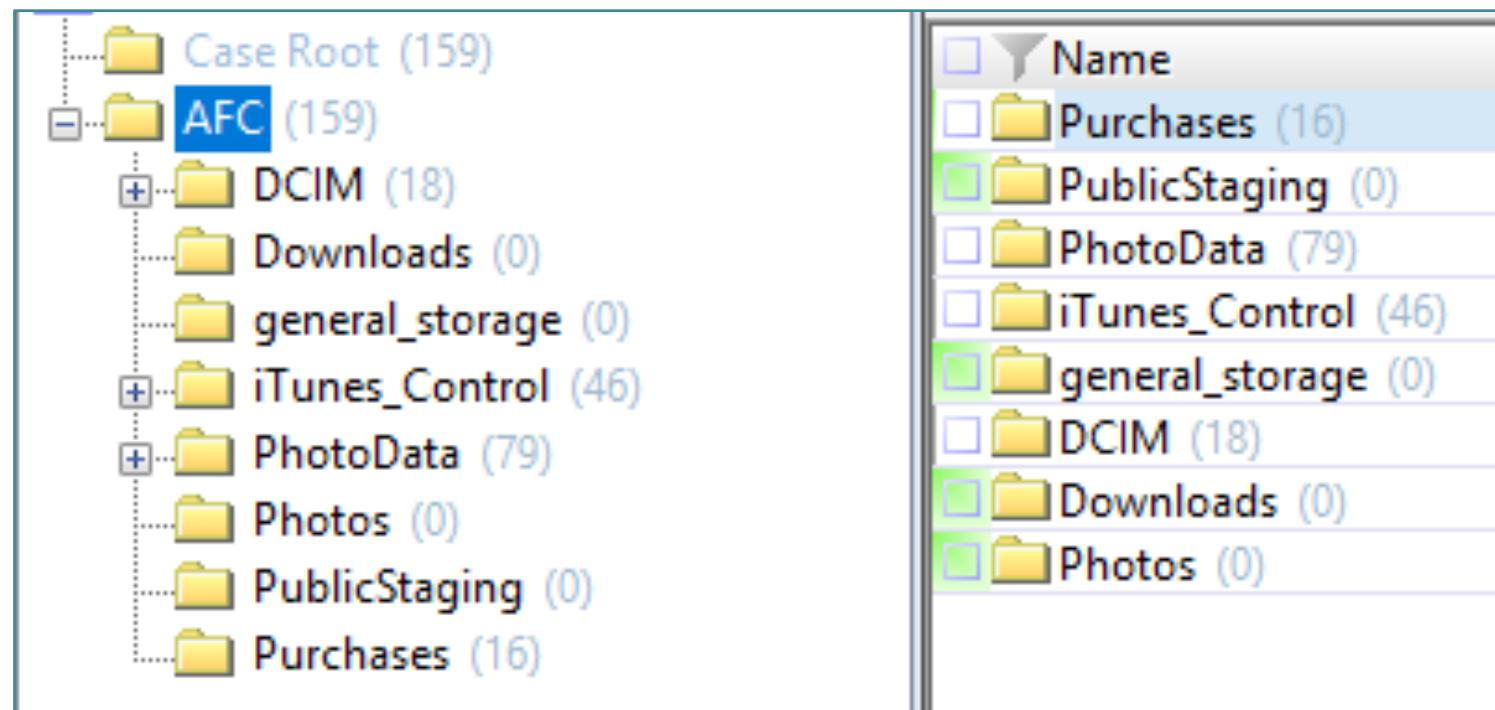
File Edit View Help

XML View List View

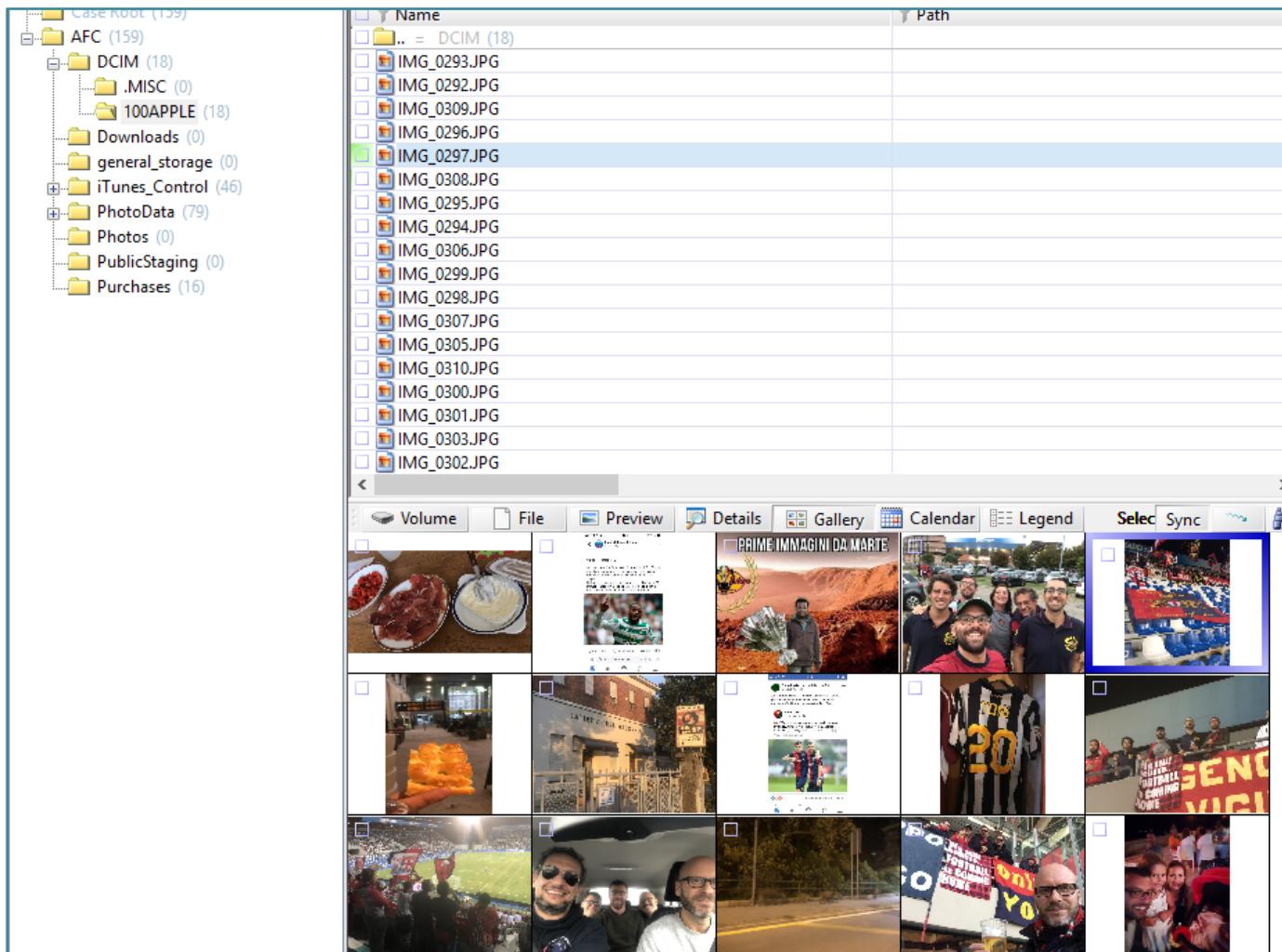
Key	Type	Value
CHANNEL	integer	6
+ RSN_IE	dict	
+ 80211D_IE	dict	
AGE	integer	20
FAST_ENTERPRISE_NET	boolean	true
lastAutoJoined	date	2019-04-25 13:17:51
CHANNEL_WIDTH	integer	20
IS_NETWORK_CUSTOM	boolean	false
AP_MODE	integer	2
WiFiManagerKnownNet	integer	3
SSID_STR	string	NHV25 Guest
IS_NETWORK_EAP	boolean	false
ORIG_AGE	integer	357
IS_NETWORK_CONFIGUI	boolean	false
GUESSED_2ghzBSSID1	string	28:6f:7f:58:ce:8e
SSID	data	...
- BSSID	string	28:6f:7f:8d:b2:0
IS_NETWORK_CAPTIVE	boolean	false
FT_ENABLED	boolean	true
GUESSED_2ghzBSSID2	string	28:6f:7f:58:ce:8d
RSSI	integer	-70
WEP	boolean	false
PHY_MODE	integer	16
UserDirected	boolean	false

+ FAST_ENTERPRISE_NET	dict	
CARPLAY_NETWORK	boolean	false
networkKnownBSSListKey	array	
knownBSSUpdatedDate	date	2019-04-24 20:37:41
lastUpdated	date	2019-04-24 11:51:59
enabled	boolean	true
GUESSED_2ghzBSSID3	string	28:6f:7f:58:ce:90
Strength	real	0.838376
CAPABILITIES	integer	4113
WiFiNetworksAutoJoin	boolean	true
CHANNEL_FLAGS	integer	10
lastJoined	date	2019-04-25 13:32:40
BEACON_INT	integer	100
SCAN_RESULT_FROM_PI	boolean	true
CaptiveNetwork	boolean	false
SHARE_MODE	integer	3
GUESSED_2ghzBSSID4	string	28:6f:7f:58:ce:91
+ RATES	array	
networkUsage	real	12776.997658
IS_NETWORK_EXPIRABLE	boolean	false
ScaledRate	real	1.000000
80211W_ENABLED	boolean	true
+ HT_CAPS_IE	dict	
ScaledRSSI	real	0.838376
+ QBSS_LOAD_IE	dict	
ASSOC_FLAGS	integer	1
+ +	dict	
+ +	dict	

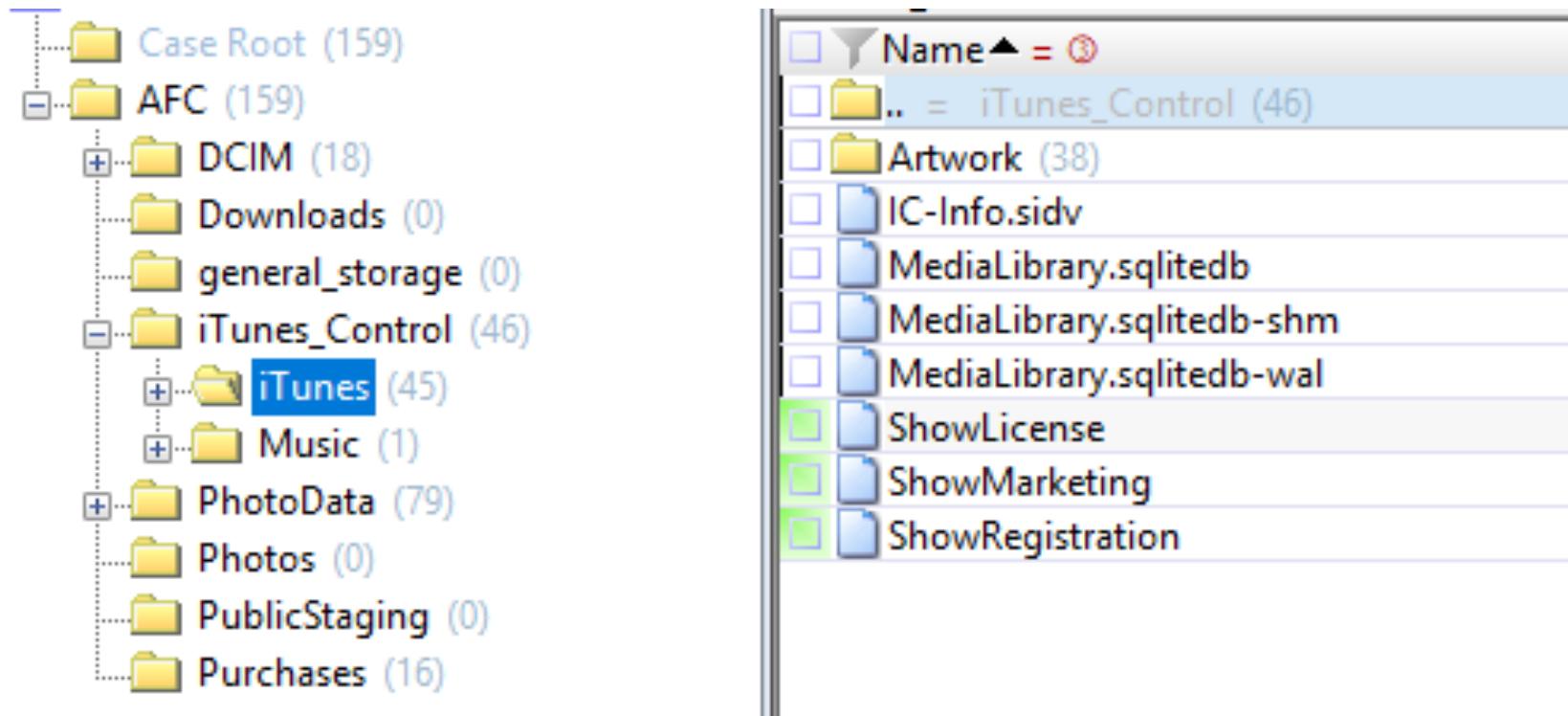
# APPLE WATCH AFC ACQUISITION



# APPLE WATCH AFC – DCIM FOLDER

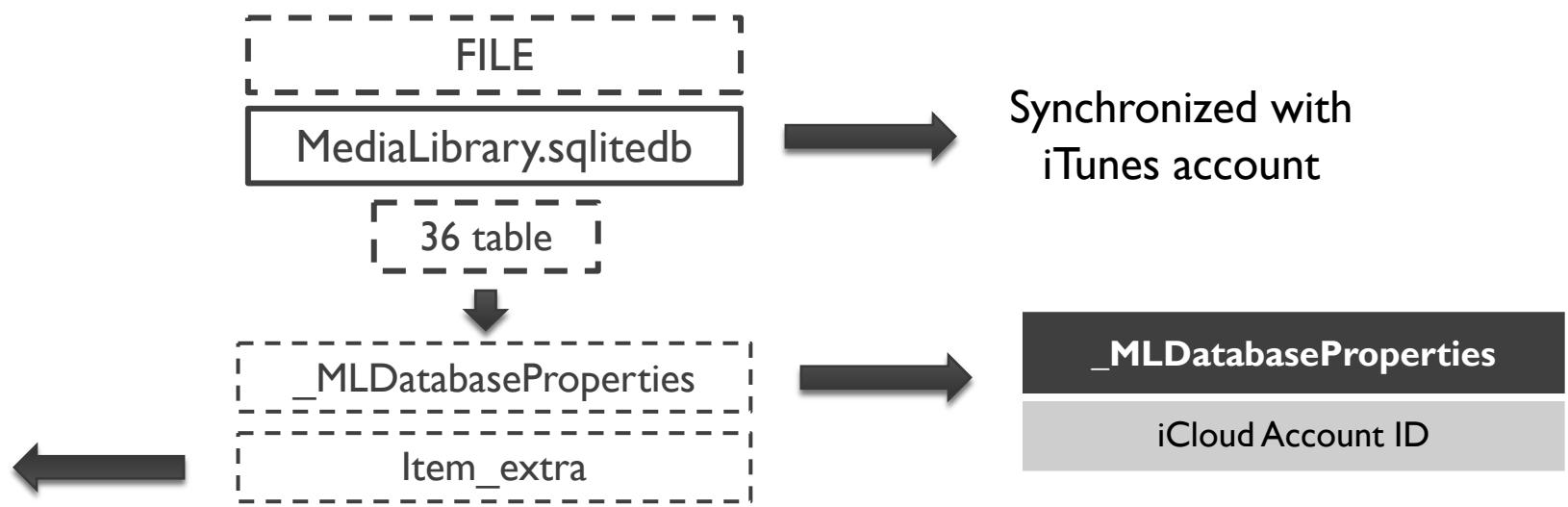


# APPLE WATCH AFC – ITUNES\_CONTROL/ITUNES



# APPLE WATCH AFC – ITUNES\_CONTROL/ITUNES/MEDIALIBRARY.SQLITEDB

item_extra	
media_kind	
0	Book
1	Music (mp3 format)
2	Film
33	Music (m4v format)



# APPLE WATCH AFC – ITUNES\_CONTROL/ITUNES/MEDIALIBRARY.SQLITEDB

item_extra	
	media_kind
0	Book
1	Music (mp3 format)
2	Film
33	Music (m4v format)



RecNo	key	value
Click here to define a filter		
1	_UUID	471A6E83-73B7-4D44-B6EE-96AFB88C25B1
2	MLCloudDatabaseUserVersion	380110
3	OrderingLanguage	it-IT
4	MLSortMapUnicodeVersion	備
5	MLSyncClientGenerationID	1894746158599307206
6	autoCreatedSmartPlaylistsDeleted	1
7	createdBuiltInSmartPlaylists	1
8	MLSyncLibraryID	D4E964E9-623A-41C7-B0C2-8B85765680BA
9	MLCloudDatabaseRevision	0
10	MLJaliscoAccountID	1321761630
11	MLStorefrontID	143450-7,35
12	MLJaliscoNeedsUpdateForTokens	0
13	MLJaliscoLastSupportedMediaKinds	4194304,1,65536,32
14	MLJaliscoDatabaseRevision	1504986125
15	MLCloudDatabasePreferredVideoQuality	-1

# APPLE WATCH

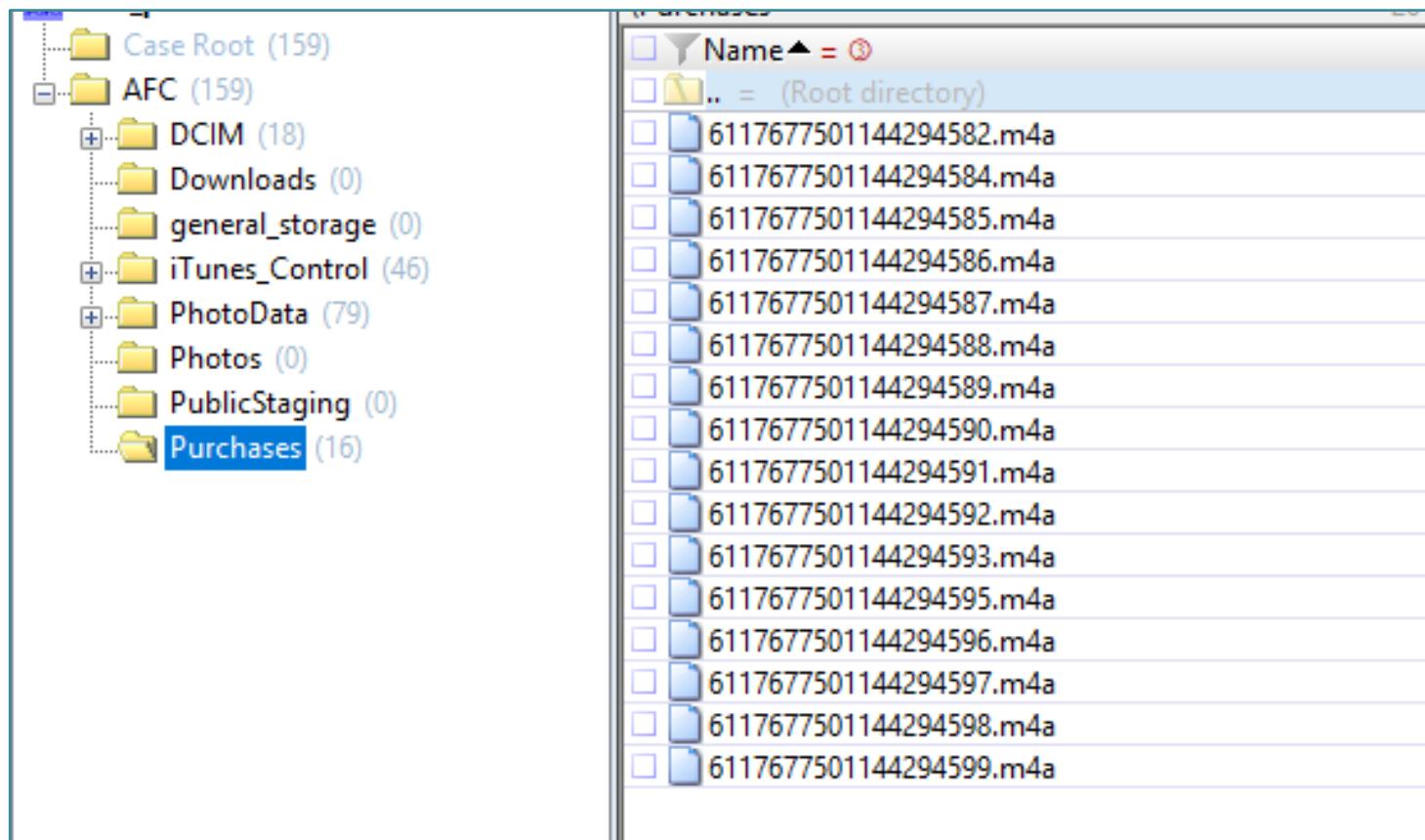
## AFC – ITUNES\_CONTROL/ITUNES/MEDIALIBRARY.SQLITEDB

```
1 select
2 ext.title AS "Title",
3 ext.media_kind AS "Media Type",
4 itep.format AS "File format",
5 ext.location AS "File",
6 ext.total_time_ms AS "Total time (ms)",
7 ext.file_size AS "File size",
8 ext.year AS "Year",
9 alb.album AS "Album Name",
10 alba.album_artist AS "Artist",
11 com.composer AS "Composer",
12 gen.genre AS "Genre",
13 art.artwork_token AS "Artwork",
14 itev.extended_content_rating AS "Content rating",
15 itev.movie_info AS "Movie information",
16 ext.description_long AS "Description",
17 ite.track_number AS "Track number",
18 sto.account_id AS "Account ID",
19 strftime('%d/%m/%Y %H:%M:%S', datetime(sto.date_purchased + 978397200,'unixepoch'))date_purchased,
20 sto.store_item_id AS "Item ID",
21 sto.purchase_history_id AS "Purchase History ID",
22 ext.copyright AS "Copyright"
23 from
24 item_extra ext
25 join item_store sto using (item_pid)
26 join item ite using (item_pid)
27 join item_stats ites using (item_pid)
28 join item_playback itep using (item_pid)
29 join item_video itev using (item_pid)
30 left join album alb on sto.item_pid=alb.representative_item_pid
31 left join album_artist alba on sto.item_pid=alba.representative_item_pid
32 left join composer com on sto.item_pid=com.representative_item_pid
33 left join genre gen on sto.item_pid=gen.representative_item_pid
34 left join item_artist itea on sto.item_pid=itea.representative_item_pid
35 left join artwork_token art on sto.item_pid=art.entity_pid
```

# APPLE WATCH AFC – ITUNES\_CONTROL/ITUNES/MEDIALIBRARY.SQLITEDB

Field name	Field value
Title	Prisencolinensinainciusol (Remix)
File format	m4a
File	<b>6117677501144294585.m4a</b>
Total time (ms)	320027
File size (bytes)	11034161
Year	2012
Album Name	Gift Clan 3 - Single
Artist	Adriano Celentano
Composer	Adriano Celentano
Genre	Pop
Artwork	us/r30/Music/64/1b/60/mzi.zlmopxmi.jpg
Track Number	2
iCloud Account ID	<b>1321761630</b>
Purchase date	<b>04/01/2012 02:28:06</b>
Item ID	483346952
Purchase History ID	230000997371840

# APPLE WATCH AFC – PURCHASES



# APPLE WATCH MANUAL ACQUISITION – SYNC TABLE

Application	Deletion on iPhone	Deletion on AppleWatch
Contacts	Deletion is propagated	Deletion is not possible
Call log	Deletion is propagated	Deletion is not possible
SMS/iMessage	<b>Deletion IS NOT PROPAGATED</b>	<b>Deletion IS NOT PROPAGATED</b>
Mail	Deletion is propagated	Deletion is propagated
Calendar	Deletion is propagated	Deletion is not possible
Wallet	Deletion is propagated	Deletion is not possible
Telegram	Deletion is propagated	Deletion is not possible
Facebook Messenger	Deletion is propagated	Deletion is not possible