



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

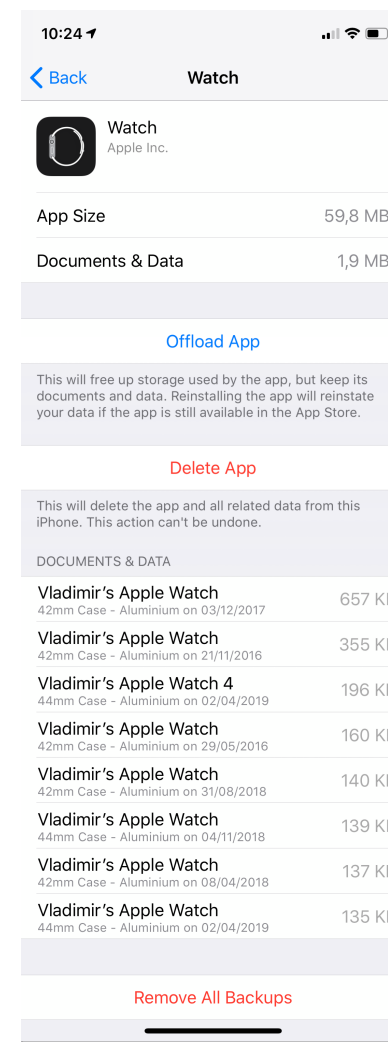
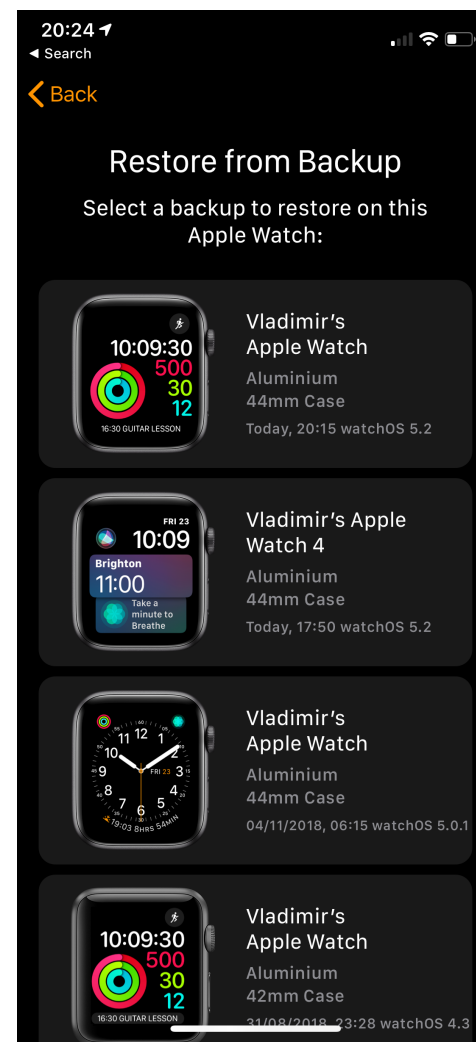
- Apple backs up Apple Watch data
- Comprehensive information at <https://support.apple.com/en-us/HT204518>
- Apple Watch content backs up automatically to your companion iPhone, so you can restore your Apple Watch from a backup.
- When you back up your iPhone to iCloud or iTunes, your iPhone backup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

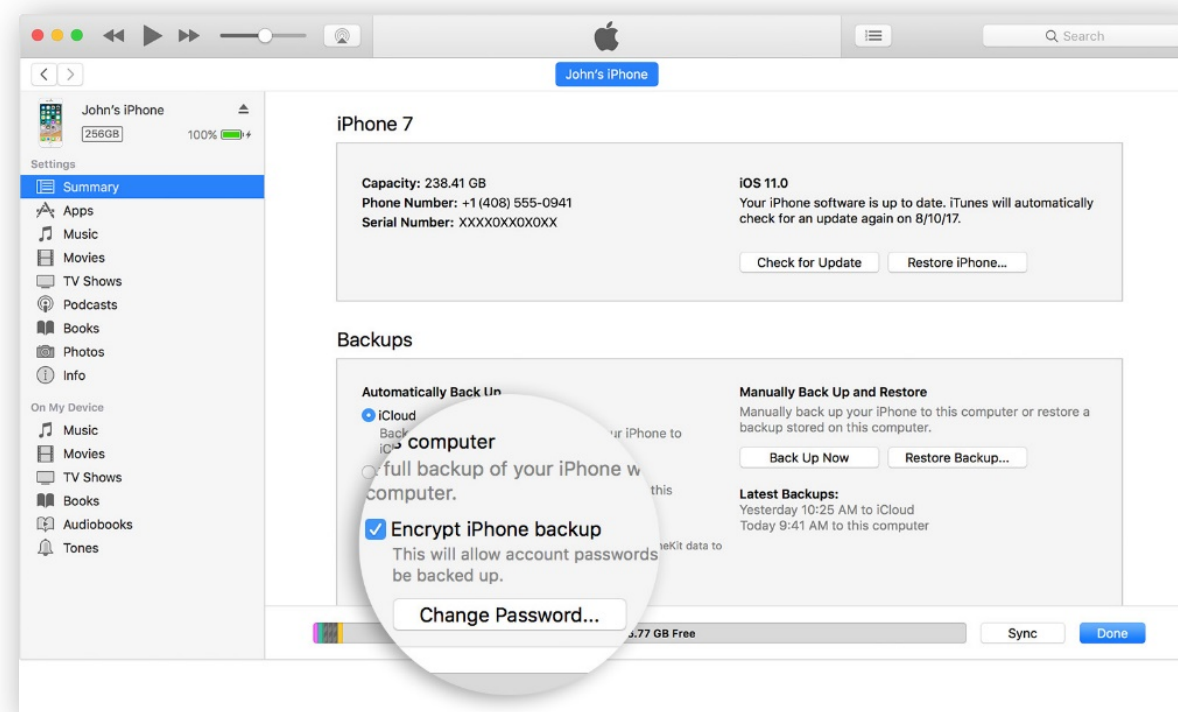
- Built-in apps: app data and settings
- Third-party apps: only settings
- Health and Fitness data: history, achievements, Workout and Activity calibration data, user-entered data
 - **To back up Health and Fitness data, you need to use iCloud or an encrypted iTunes backup.**
- App layout on Home screen
- 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 explorer window with a sidebar on the left and a main pane on the right. The sidebar displays a tree view of folders under 'Library', with 'DeviceRegistry.state' selected. The main pane shows a table of files with columns for Name, Size, Permission, and Date Modified. The file 'history.plist' is highlighted in the table.

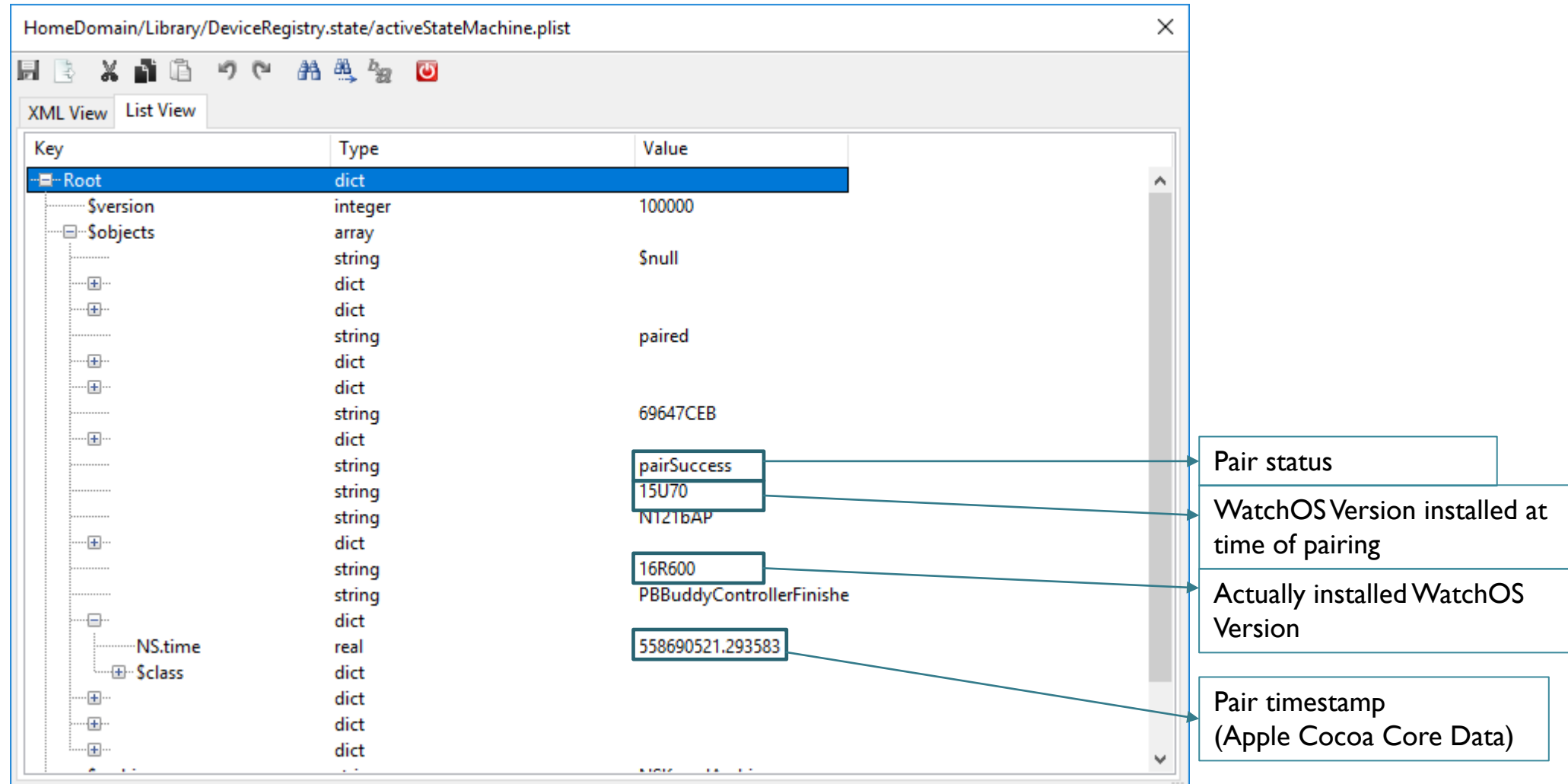
Name	Size	Permission	Date Modified
ClassAFile.txt	13	-rw-r--r--	11/04/17 11:47:30
UDIDChangeTracker.plist	272	-rw-r--r--	08/27/18 14:48:13
activeStateMachine.plist	1.3 kB	-rw-r--r--	12/28/18 11:17:37
history.plist	3.6 kB	-rw-r--r--	12/27/18 15:27:57
historySecureProperties.plist	1.1 kB	-rw-r--r--	09/15/18 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 – STATEMACHINE-<GUID>.PLIST

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

- 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
Subjects	array	
	string	\$null
	dict	
	dict	
	string	paired
	dict	
	dict	
	string	69647CEB
	dict	
	string	pairSuccess
	string	15U70
	string	NT21bAP
	dict	
	string	16R600
	string	PBBuddyControllerFinishe
	dict	
NS.time	real	558690521.293583
\$class	dict	
	dict	
	dict	
	dict	

Annotations:

- pairSuccess: Pair status
- 15U70: WatchOS Version installed at time of pairing
- 16R600: Actually installed WatchOS Version
- 558690521.293583: Pair timestamp (Apple Cocoa Core Data)

APPLE WATCH IOS BACKUP – DEVICEREGISTRY

Name	Size	Permission	Date Modified	Date Created
DeviceRegistry				
24620D1C-6016-4378-B7E9-7198D7F0C718	2.9 MB	drwxr-xr-x	11/13/18 02:19:47	09/15/18 09:48:43
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 image shows a file explorer window with a tree view on the left and a detailed view of a file on the right. The tree view shows a folder named 'NanoAppRegistry' containing an 'Applications' subfolder. Inside 'Applications', there are numerous subfolders representing different apps, including 'Alitalia.watchkitapp', 'at.runtastic.gpsportapp.watchapp', 'com.apple.ActivityMonitorApp', 'com.apple.DataMigrationMonitor', 'com.apple.DeepBreathing', 'com.apple.DiagnosticsService', 'com.apple.HeartRate', 'com.apple.MobileSMS', 'com.apple.NanoAlarm', 'com.apple.NanoCalendar', 'com.apple.NanoCamera', 'com.apple.NanoDemo', 'com.apple.NanoDiagnostics', 'com.apple.NanoMail', 'com.apple.NanoMailBulletinService', 'com.apple.NanoMaps', 'com.apple.NanoMusic', 'com.apple.NanoNowPlaying', 'com.apple.NanoNowPlayingViewServ', 'com.apple.NanoPassbook', 'com.apple.NanoPhone', 'com.apple.NanoPhotos', 'com.apple.NanoRadio', 'com.apple.NanoRemote', 'com.apple.NanoSettings', 'com.apple.NanoStopwatch', 'com.apple.NanoWorldClock', 'com.apple.PreBoard', 'com.apple.ReBoard', 'com.apple.SessionTrackerApp', 'com.apple.nanobuddy', 'com.apple.nanonews', 'com.apple.private.NanoTimer', 'com.facebook.Messenger.watchkitapp', 'com.lufthansa.launcher.watchkitapp', and 'com.melodis.soundhound.free.watch'.

The detailed view on the right shows the file 'Application.dat' (1.0 kB, -rw-r--r--, 12/28/18 22:08:29). Below the file list, there is a window titled 'HomeDomain/Library/DeviceRegistry/24620D1C-6016-4378-B7E9-7198D7F0C718/NanoAppRegistry/Applications/com.facebook.Messen...' with a search bar and a table view. The table has columns for 'Key', 'Type', and 'Value'. The 'NS.objects' array is expanded, showing a list of objects. The selected object is a dictionary with the following key-value pairs:

Key	Type	Value
CFBundleVersion	string	CFBundleVersion
CFBundleDisplayName	string	CFBundleDisplayName
CFBundleShortVersionString	string	CFBundleShortVersionString
CFBundleIdentifier	string	CFBundleIdentifier
CFBundleName	string	CFBundleName
135382157	string	135382157
Messenger	string	Messenger
196.0	string	196.0
com.facebook.Messenger.watchkitapp	string	com.facebook.Messenger.watchkitapp
MessengerWatchAppBundle	string	MessengerWatchAppBundle
NS.keys	array	
NS.objects	array	
-\$class	dict	
itemName	string	itemName
artistName	string	artistName
Facebook, Inc.	string	Facebook, Inc.
488	integer	488
User	string	User

APPLE WATCH IOS BACKUP – NANOMAIL\REGISTRY.SQLITE

Backups

- NanoAppRegistry
- NanoMail
- NanoPasses
- NanoPreferencesSync
- PairedSync

Backward Forward Open Delete Export Import Restore Search

Name	Size	Permission	Date Modified	Date Created
registry.sqlite	1.1 MB	-rw-r--r--	12/31/18 14:28:40	09/24/18 21:16:20

HomeDomain/Library/DeviceRegistry/24620D1C-6016-4378-B7E9-7198D7F0C718/NanoMail/registry.sqlite

Database

- Tables
 - ATTACHMENT_NOT_SYNCED
 - COMPOSED_MESSAGE
 - CONTROL
 - DELETED_MESSAGE
 - IDS_IDENTIFIER_NOT_YET_ACKD
 - IDS_IDENTIFIER_OBJECT
 - MAILBOX
 - MAILBOX_SYNC_VERSION
 - SYNCED_ACCOUNT
 - SYNCED_MESSAGE

	ID	DISPLAY_NAME	SHOULD_ARCHIVE	EMAIL_ADDRESSES	RESEND_REQUESTED	RESEND_INTERVAL	SOURCE_TYPE	USERNAME	LOCAL_ID
1	54A03817-58F4-4A6F-9A76-A2E80FB88B9D	Digital Forensics	1	mattia.epifani@digital-forensics.it	0	0	0	mattia.epifani@digital-forensics.it	54A03817-58F4-4A6F-9A76-A2E80FB88B9D
2	FB0F621D-BDD8-466E-8307-4E7050E029DA	Segreteria	1	segreteria@realitynet.it	0	0	0	segreteria@realitynet.it	FB0F621D-BDD8-466E-8307-4E7050E029DA
3	D811EEA3-4148-4738-BC6B-BC5372D0C7F8	Info reality	1	info@realitynet.it	0	0	0	info@realitynet.it	D811EEA3-4148-4738-BC6B-BC5372D0C7F8
4	CEFCB9B-9F86-46E4-A9DE-FBE52D616EFD	RealityNet	1	mattia.epifani@realitynet.it	0	0	0	mattia.epifani@realitynet.it	CEFCB9B-9F86-46E4-A9DE-FBE52D616EFD
5	DA6E8765-53E3-48F8-8C40-6901CBCEFA9E	DFA	1	info@perfezionisti.it	0	0	0	info@perfezionisti.it	DA6E8765-53E3-48F8-8C40-6901CBCEFA9E
6	019684EA-73A3-4E74-B8A5-C820CD27C005	Hotmail	0	mattiaep@hotmail.it	0	0	0		019684EA-73A3-4E74-B8A5-C820CD27C005
7	72E4633E-5E97-4653-8E4F-60EEB2D283E6	Outlook	0	rmdataserver@hotmail.com	0	0	0		72E4633E-5E97-4653-8E4F-60EEB2D283E6

APPLE WATCH IOS BACKUP – NANOMAIL\REGISTRY.SQLITE

Backups

- NanoApp
- NanoMail
- NanoPass
- NanoPref
- PairedSvr

HomeDomain/Library/DeviceRegistry

Database

- Tables
 - ATTACHMENT_NOT_SYNCED
 - COMPOSED_MESSAGE
 - CONTROL
 - DELETED_MESSAGE
 - IDS_IDENTIFIER_NOT_YET_SYNCED
 - IDS_IDENTIFIER_OBJECT
 - MAILBOX
 - MAILBOX_SYNC_VERSION
 - SYNCED_ACCOUNT**
 - SYNCED_MESSAGE

DISPLAY_NAME	SHOULD_ARCHIVE	EMAIL_ADDRESSES
Digital Forensics	1	mattia.epifani@digital-forensics.it
Segreteria	1	segreteria@realitynet.it
Info reality	1	info@realitynet.it
RealityNet	1	mattia.epifani@realitynet.it
DFA	1	info@perfezionisti.it
Hotmail	0	mattiaep@hotmail.it
Outlook	0	rndataserver@hotmail.com

LOCAL_ID
17-58F4-4A6F-9A76-A2E80FB88B9D
1D-BDD8-466E-8307-4E7050E029DA
A3-4148-4738-BC6B-BC5372D0C7F8
89B-9F86-46E4-A9DE-FBE52D616EFD
65-53E3-48F8-8C40-6901CBCEFA9E
EA-73A3-4E74-B8A5-C820CD27C005
8E-5E97-4653-8E4F-60EEB2D283E6

APPLE WATCH IOS BACKUP – NANOMAIL\REGISTRY.SQLITE

The screenshot shows a file explorer window with the following elements:

- Backups folder:** Contains NanoAppRegistry, NanoMail, NanoPasses, NanoPreferencesSync, and PairedSync.
- File Properties:** registry.sqlite, 1.1 MB, Permission: -rw-r--r--, Date Modified: 12/31/18 14:28:40, Date Created: 09/24/18 21:16:20.
- File Path:** HomeDomain/Library/DeviceRegistry/24620D1C-6016-4378-B7E9-7198D7F0C718/NanoMail/registry.sqlite
- Database Structure:**
 - Database: Tables
 - ATTACHMENT_NOT_SYNCED
 - COMPOSED_MESSAGE
 - CONTROL
 - DELETED_MESSAGE
 - IDS_IDENTIFIER_NOT_YET_ACTIVATED
 - IDS_IDENTIFIER_OBJECT
 - MAILBOX** (highlighted)
 - MAILBOX_SYNC_VERSION
 - SYNCED_ACCOUNT
 - SYNCED_MESSAGE
- Table Data:**

	ACCOUNT_ID	FILTER_TYPE	TYPE	URL	CUSTOM_NAME
9	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/nordata	nordata
10	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/Banca	Banca
11	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/Fabio	Fabio
12	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/Fra	Fra
13	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/Marco	Marco
14	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/Mattia	Mattia
15	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/nordata	nordata
16	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/Ontrack	Ontrack
17	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/Perna	Perna
18	FB0F621D-BDD8-466E-8307-4E7050E029DA	0	0	imap://FB0F621D-BDD8-466E-8307-4E7050E029DA/INBOX/Salvo	Salvo

APPLE WATCH IOS BACKUP – NANOPASSES\NANOPASSES.SQLITE3

The screenshot shows a file explorer window with a left sidebar containing a tree view of folders: NanoAppRegistry, NanoMail, NanoPasses (expanded), PaymentCards, NanoPreferencesSync, PairedSync, com.apple.NanoPhotos, com.apple.private.nanoresourcegrabber, com.apple.sharing, com.apple.tccd, and DeviceRegistry.state. The main pane shows a list of files and folders:

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>
IQx8nkFxn4p+KDe8IZ0ViNJqag=	pass.com.bestwestern.rewards	Best Western Rewards®	558690775	Go. Get. Rewarded.

APPLE WATCH

IOS BACKUP – NANOPASSES\NANOPASSES.SQLITE3

```
Hex Editor: encoded_pass

0x0000 6270 6C69 7374 3030 D400 0100 0200 0300 0400 bplist00 .....
0x0012 0500 0602 0C02 0D58 2476 6572 7369 6F6E 5824 .....X$versionX$
0x0024 6F62 6A65 6374 7359 2461 7263 6869 7665 7254 objectsY$archiverT
0x0036 2474 6F70 1200 0186 A0AF 1075 0007 0008 005B $stop... ^.u.....[
0x0048 005C 005D 0076 007B 007C 0082 0088 0089 008C .\].v.{.|. . . .
0x005A 008D 0094 0098 0047 00BA 00BB 00BC 00BD 00C1 . . . .G.º.».%.%.Á
0x006C 00C4 00C5 0034 00C7 00C8 00CD 00D0 00D4 00B3 .Ä.Å.4.ç.È.Í.Ð.Ï.º
0x007E 00DF 00E0 00E1 00E2 00E6 00EA 00F5 00F6 00F7 .ß.à.á.â.ã.ä.å.ö.÷
0x0090 00F8 00FD 004A 0108 0109 010A 010B 010C 011B .ø.ý.J.....
0x00A2 011C 011D 011E 011F 0120 0121 0126 012A 0134 ..... .!.&.*.4
0x00B4 00AB 013F 0140 0141 014C 014D 014E 014F 015A .«.?.@.A.L.M.N.O.Z
0x00C6 015B 015C 015D 0168 0169 016A 016B 016C 0177 .[\.].h.i.j.k.l.w
0x00D8 0178 0179 017A 0185 0186 0187 0188 0193 0194 .x.y.z. . . . .
0x00EA 0195 0196 019B 019E 01A2 01A7 01AB 01AC 01AD . . . . .ç.¸.«.¸.-
0x00FC 01C2 01CC 01CF 01D1 01D4 01D5 01DA 01DB 01DC .Â.Ë.Ï.Ñ.Ò.Ó.Ô.Õ.Ü
0x010E 01DD 01DE 01DF 01E0 01E3 01E7 01F5 01F6 01F7 .Ý.Þ.ß.à.ã.ä.å.ö.÷
0x0120 01F8 01FC 01FF 0202 0205 0208 5524 6E75 6C6C .ø.ü.ý.....U$null
0x0132 DF10 2A00 0900 0A00 0B00 0C00 0D00 0E00 0F00 ß.*.....
0x0144 1000 1100 1200 1300 1400 1500 1600 1700 1800 .....
0x0156 1900 1A00 1B00 1C00 1D00 1E00 1F00 2000 2100 .....
0x0168 2200 2300 2400 2500 2600 2700 2800 2900 2A00 ".#.$.%.&.'.(.)*.
0x017A 2B00 2C00 2D00 2E00 2F00 3000 3100 3200 3300 +.,.-.../.0.1.2.3.
0x018C 3400 3400 3300 3700 3300 3900 3300 3300 3300 4.4.3.7.3.9.3.3.3.
0x019E 3D00 3E00 3F00 4000 4100 3300 4300 3400 4500 =.>.>@.A.3.C.4.E.
0x01B0 4600 4700 3300 3400 4A00 3300 4C00 4D00 4E00 F.G.3.4.J.3.L.M.N.
0x01C2 4F00 5000 5100 5200 4700 3300 3400 3300 4700 O.P.Q.R.G.3.4.3.G.
0x01D4 3300 3300 3300 5900 5058 696D 6167 6573 5F32 3.3.3.Y.PXimages_2
0x01E6 5772 6576 6F6B 6564 5C6C 6976 6552 656E 6465 Wrevoked\liveRende
0x01F8 7265 645E 6578 7069 7261 7469 6F6E 4461 7465 red^expirationDate
```

APPLE WATCH IOS BACKUP – NANOPASSES\NANOPASSES.SQLITE3

Key	Type	Value
	string	The Bank Hotel
	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	https://secure.booking.com/myreservations.html?bn=1198273413;pincode=9181;

APPLE WATCH HEALTH DATA IN LOCAL (ENCRYPTED) BACKUPS

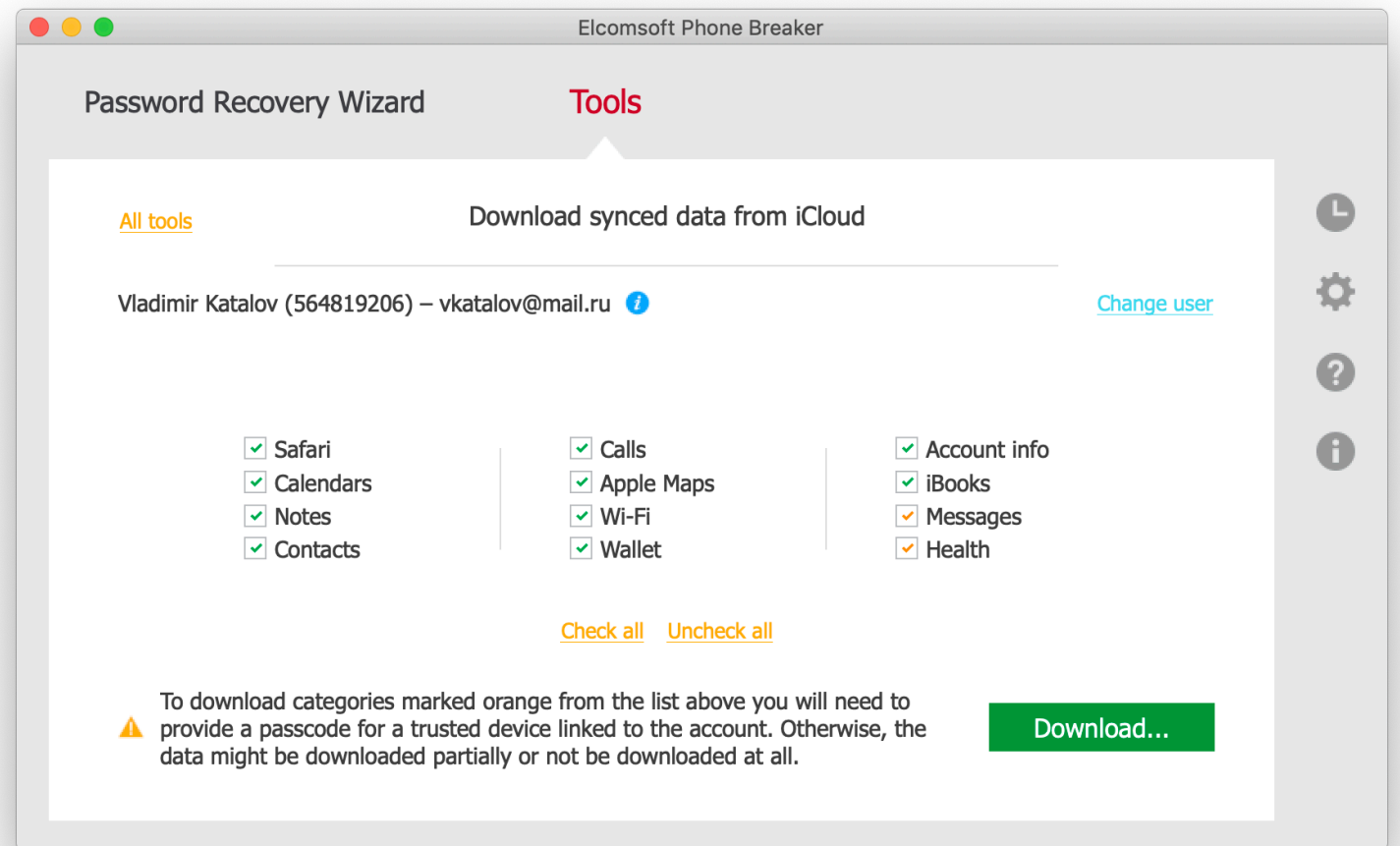
- Most data comes into *Activity* category
- GPS locations are available in *Workouts* category only
- Other useful categories: *Steps*, *Walking/running distance*, *Mindfulness*, *Heart rate*
- No *Sleep* data comes from Watch
- We have not found ECG data yet, sorry

The screenshot shows the 'Health' app interface within the Elcomsoft Phone Viewer. The app is titled 'Vladimir's iPhone X' and displays a list of activity records. The left sidebar shows a filter menu with 'Source' and 'Device' sections. The main area shows a table of records with columns for Start Date, End Date, Date Added, Source, Device, Details, and Workout type.

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/)



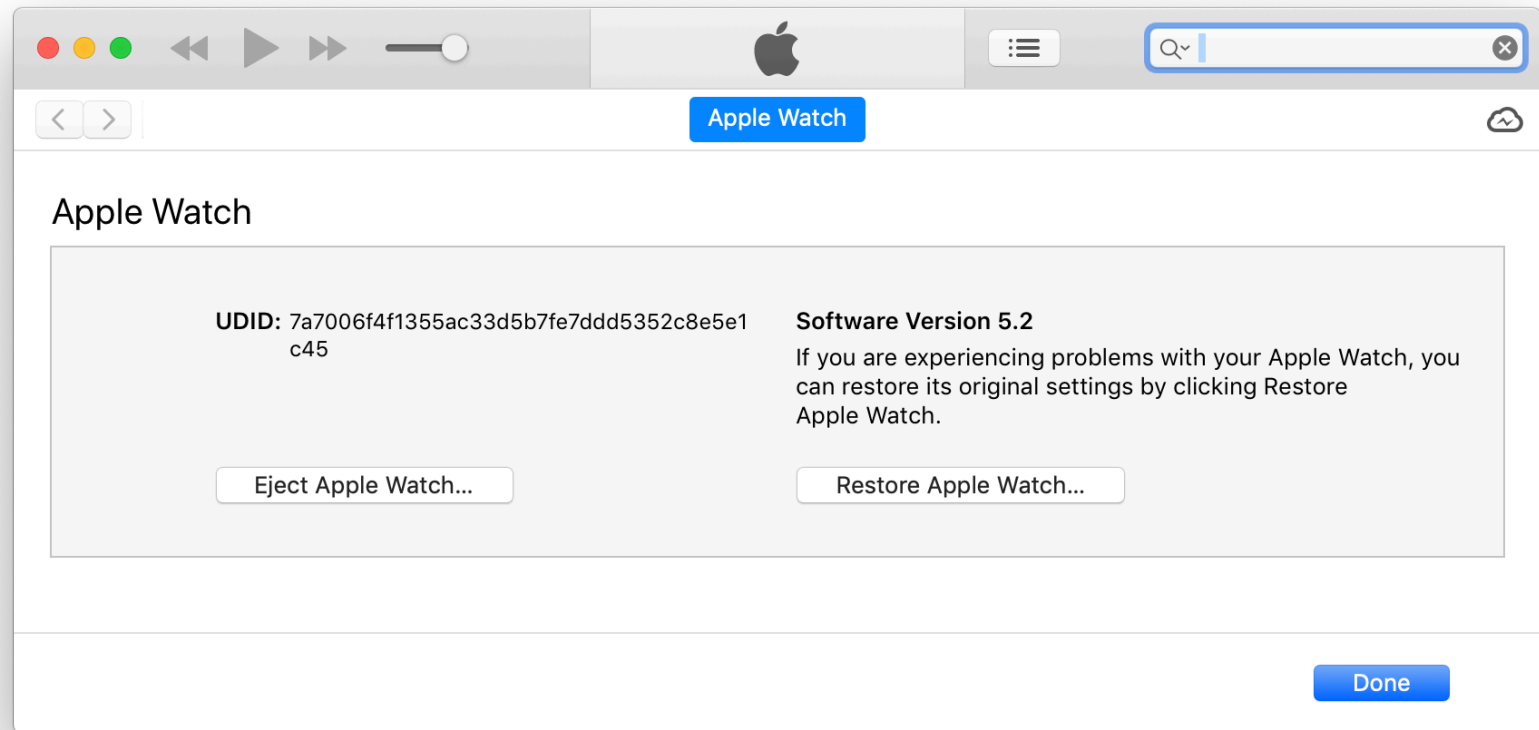
APPLE WATCH PAIRING

Trust This Computer?

Your settings and
data will be
accessible from
'Vladimir's MacBook'
when connected
wirelessly or using a
cable.

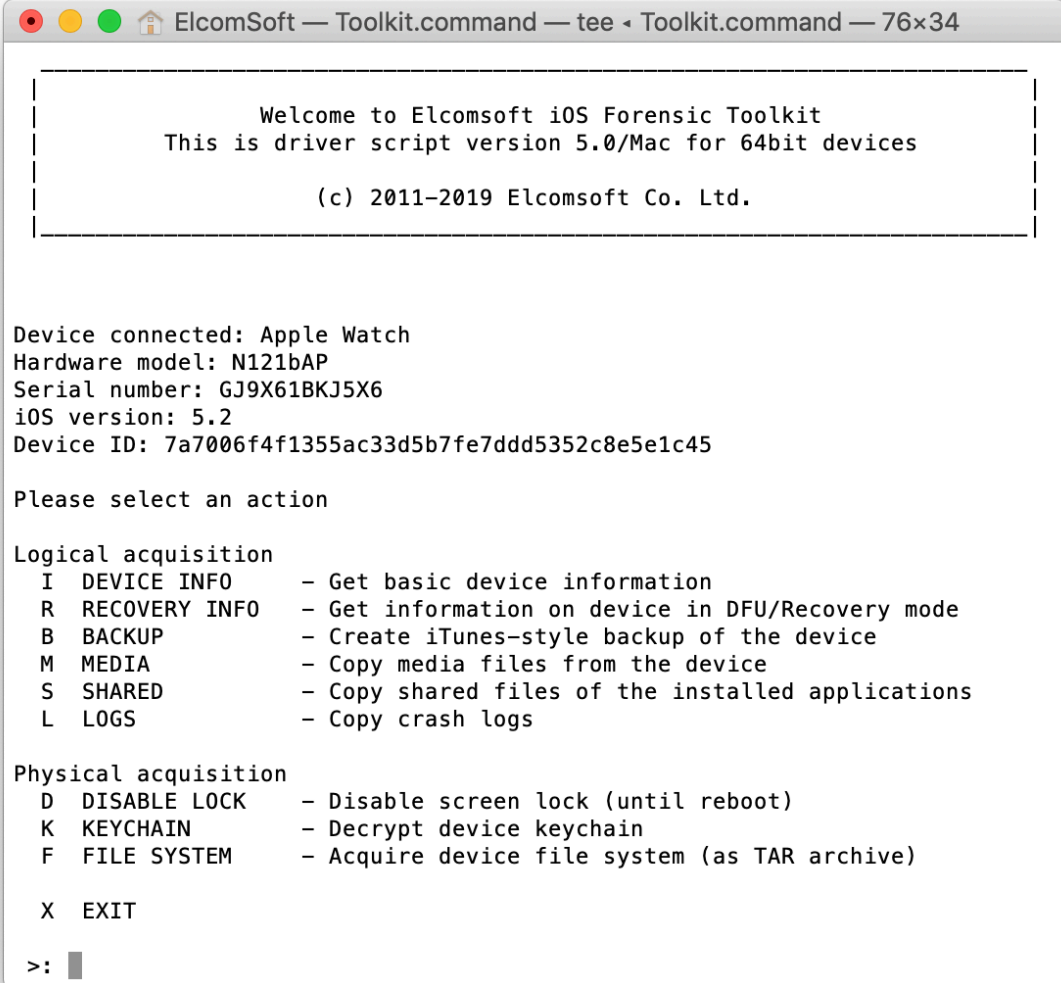
Don't Trust

Trust



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!



```
ElcomSoft — Toolkit.command — tee ◀ Toolkit.command — 76x34

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	2a9fbeat643728ce72f820abd21cf5e85424234
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

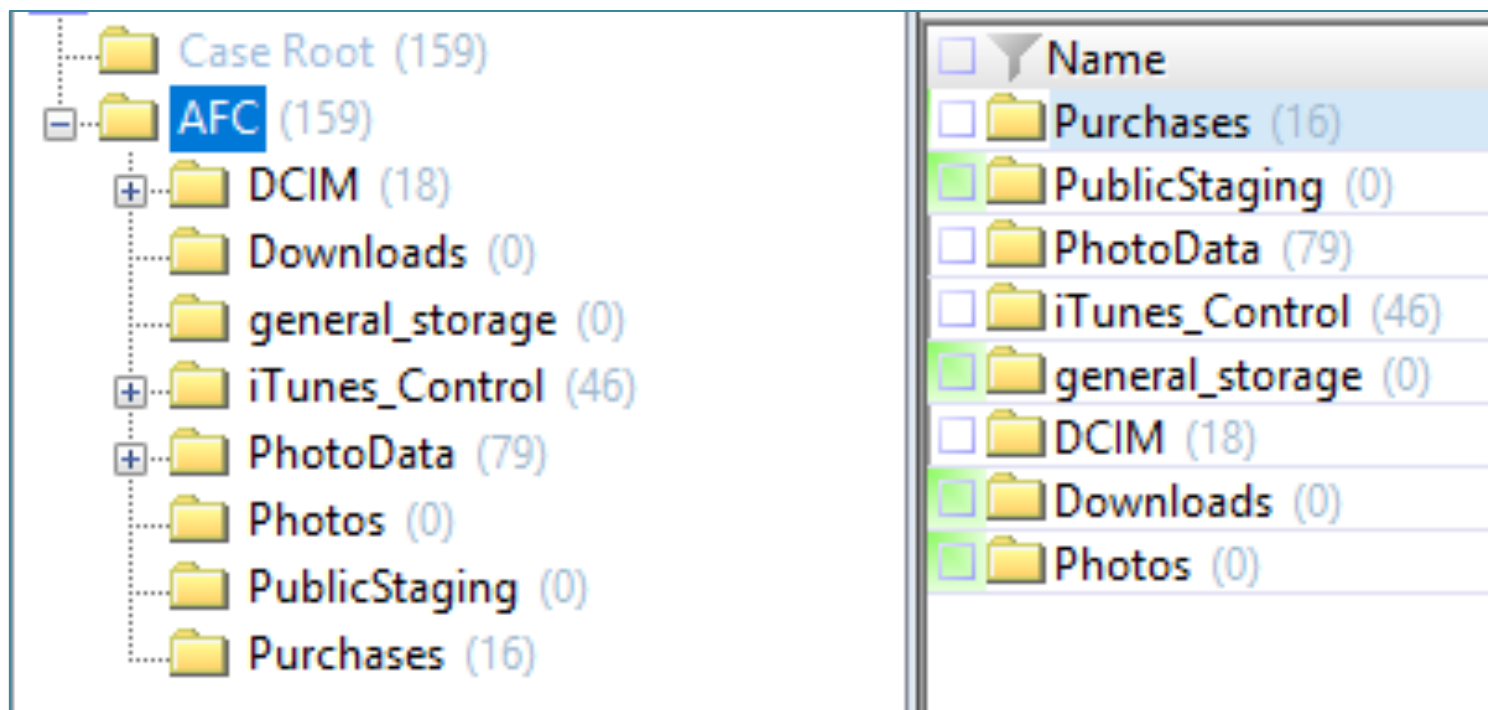
File Edit View Help

XML View List View

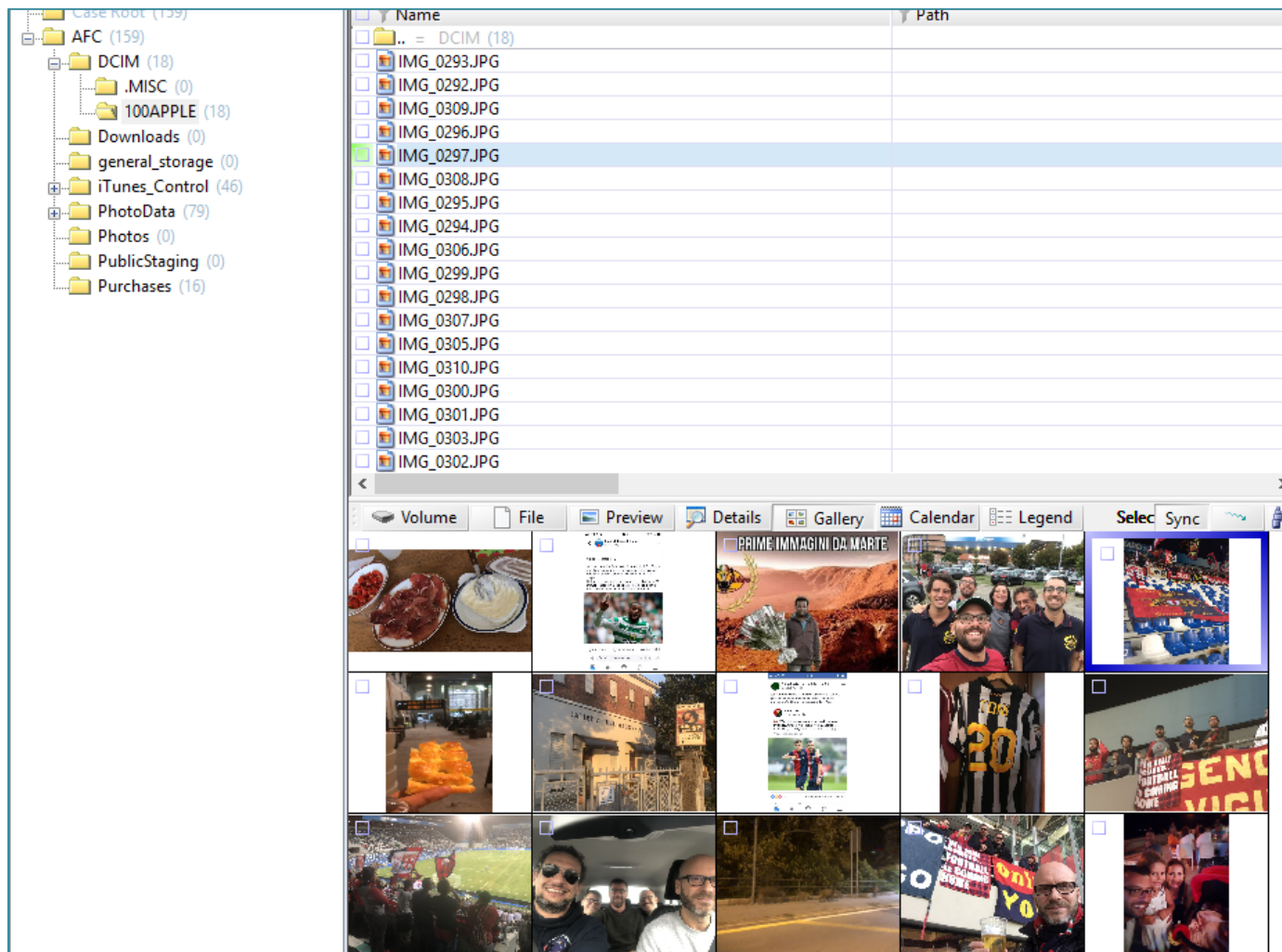
Key	Type	Value
CHANNEL	integer	6
RSN_IE	dict	
80211D_IE	dict	
AGE	integer	20
FAST_ENTERPRISE_NETWORK	boolean	true
lastAutoJoined	date	2019-04-25 13:17:51
CHANNEL_WIDTH	integer	20
IS_NETWORK_CUSTOMIZED	boolean	false
AP_MODE	integer	2
WiFiManagerKnownNetworks	integer	3
SSID_STR	string	NHV25 Giest
IS_NETWORK_EAP	boolean	false
ORIG_AGE	integer	357
IS_NETWORK_CONFIGURED	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_NETWORK	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
WiFiNetworkIsAutoJoined	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

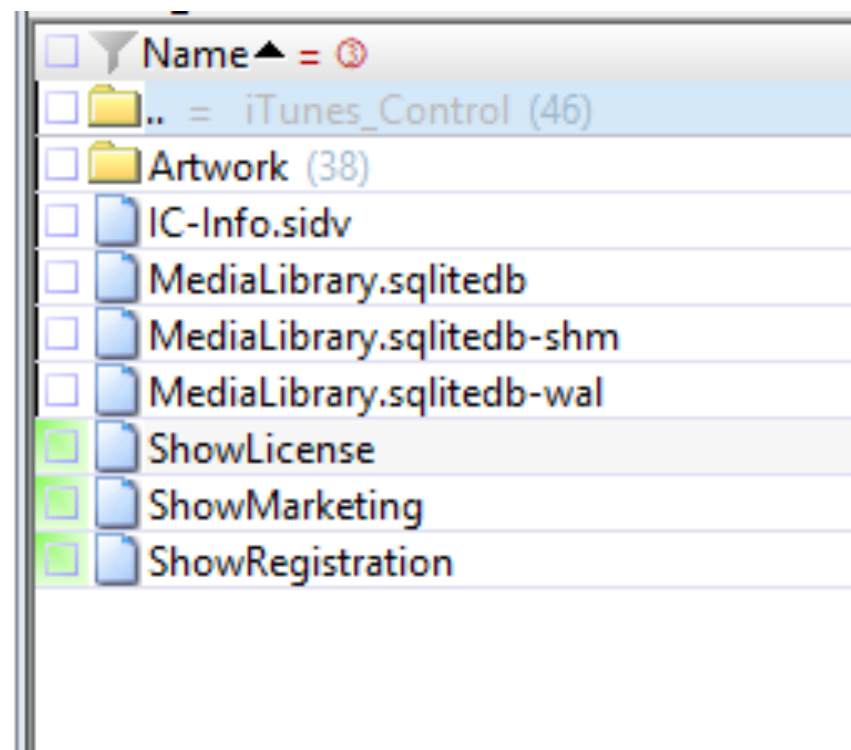
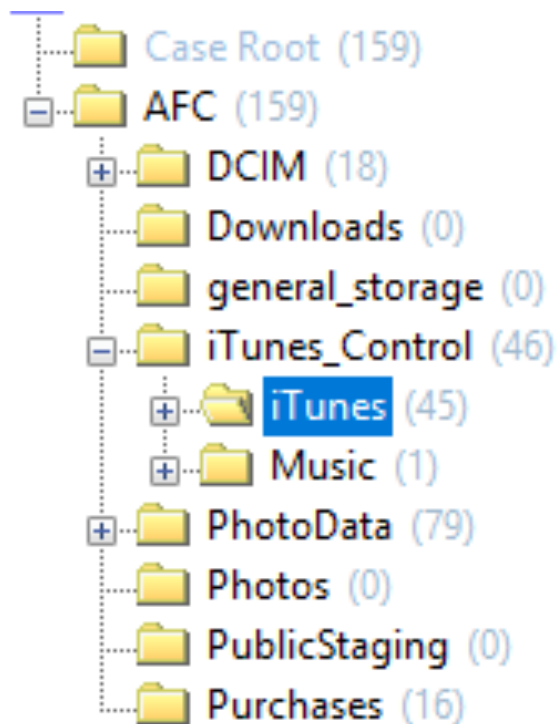


APPLE WATCH AFC – DCIM FOLDER



APPLE WATCH

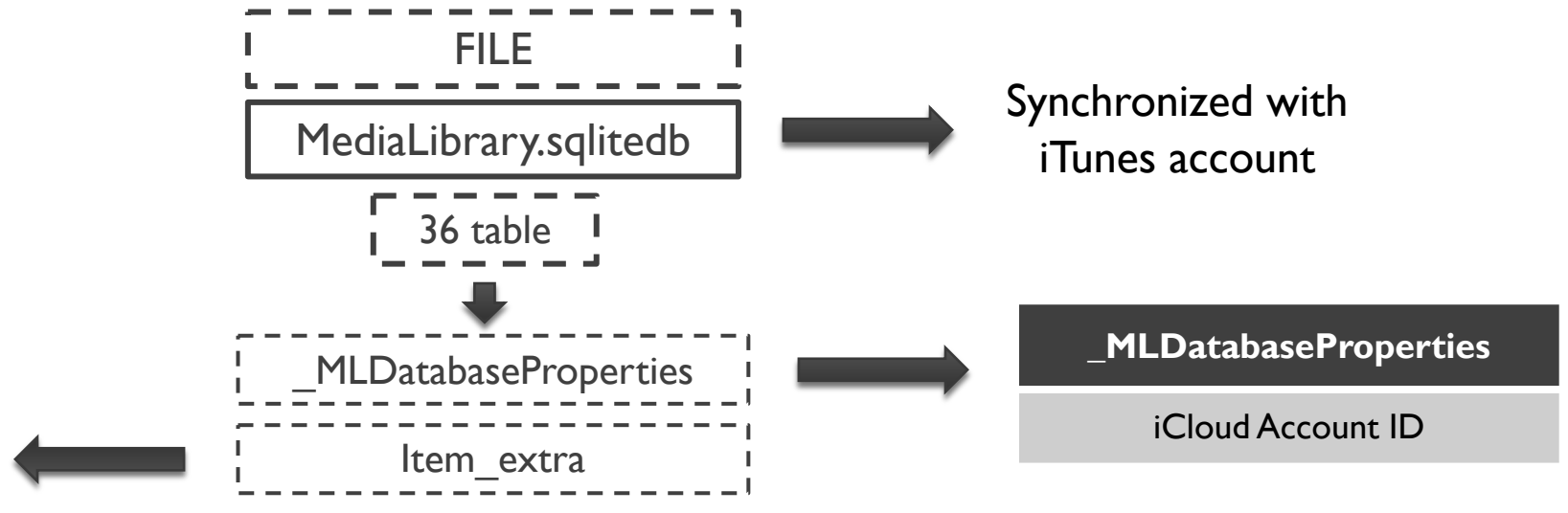
AFC – ITUNES_CONTROL/ITUNES



APPLE WATCH

AFC – ITUNES_CONTROL/ITUNES/MEDIA LIBRARY.SQLITEDB

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



APPLE WATCH

AFC – ITUNES_CONTROL/ITUNES/MEDIA/LIBRARY.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/MEDIA/LIBRARY.SQLITEDB

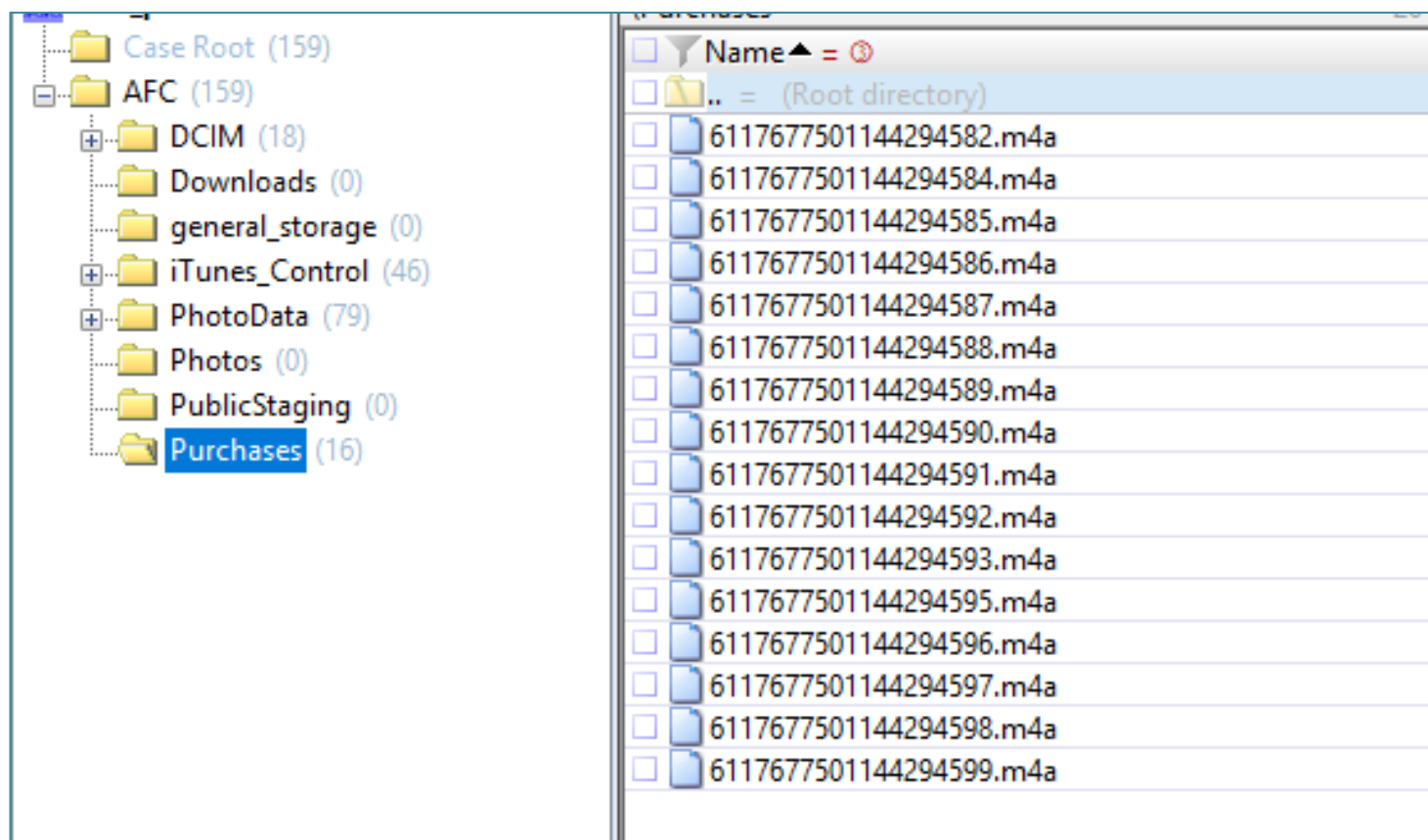
```
1 select
2 ext.title AS "Title",
3 ext.media_kind AS "Media Type",
4 itep.format AS "File format",
5 ext.location AS "File",
6 ext.total_time_ms AS "Total time (ms)",
7 ext.file_size AS "File size",
8 ext.year AS "Year",
9 alb.album AS "Album Name",
10 alba.album_artist AS "Artist",
11 com.composer 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/MEDIA/LIBRARY.SQLITEDB

Field name	Field value
Title	Prisencolinensinainciusol (Remix)
File format	m4a
File	6117677501144294585.m4a
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	1321761630
Purchase date	04/01/2012 02:28:06
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	Deletion IS NOT PROPAGATED	Deletion IS NOT PROPAGATED
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