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

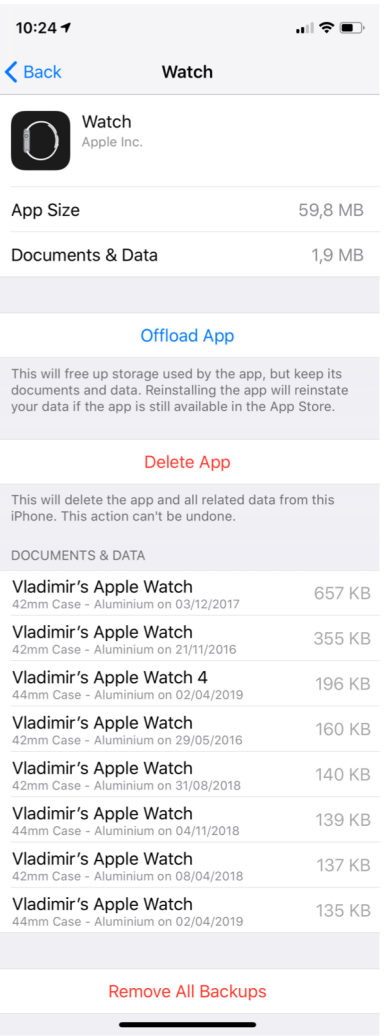
- Apple backs up Apple Watch data
- Comprehensive information at https://support.apple.com/en-us/HT204518
- Apple Watch content backs up automatically to your companion iPhone, so you can restore your Apple Watch from a backup.
- When you back up your iPhone to iCloud or iTunes, your iPhone backup will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

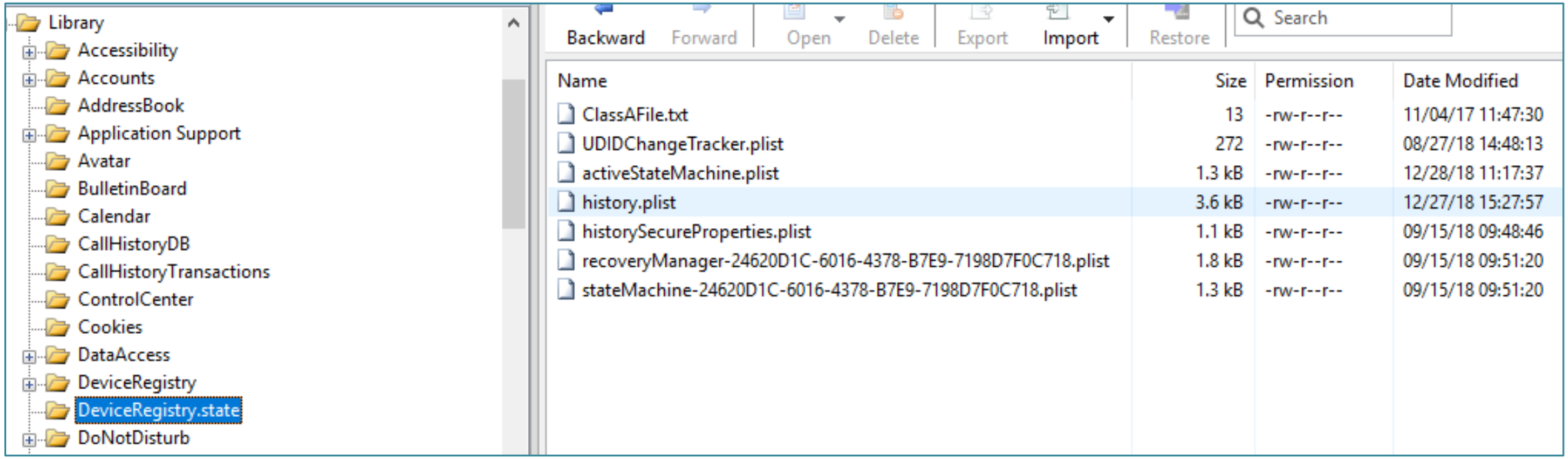
APPLE WATCH BACKUPS: WHAT'S **NOT** INCLUDED?

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

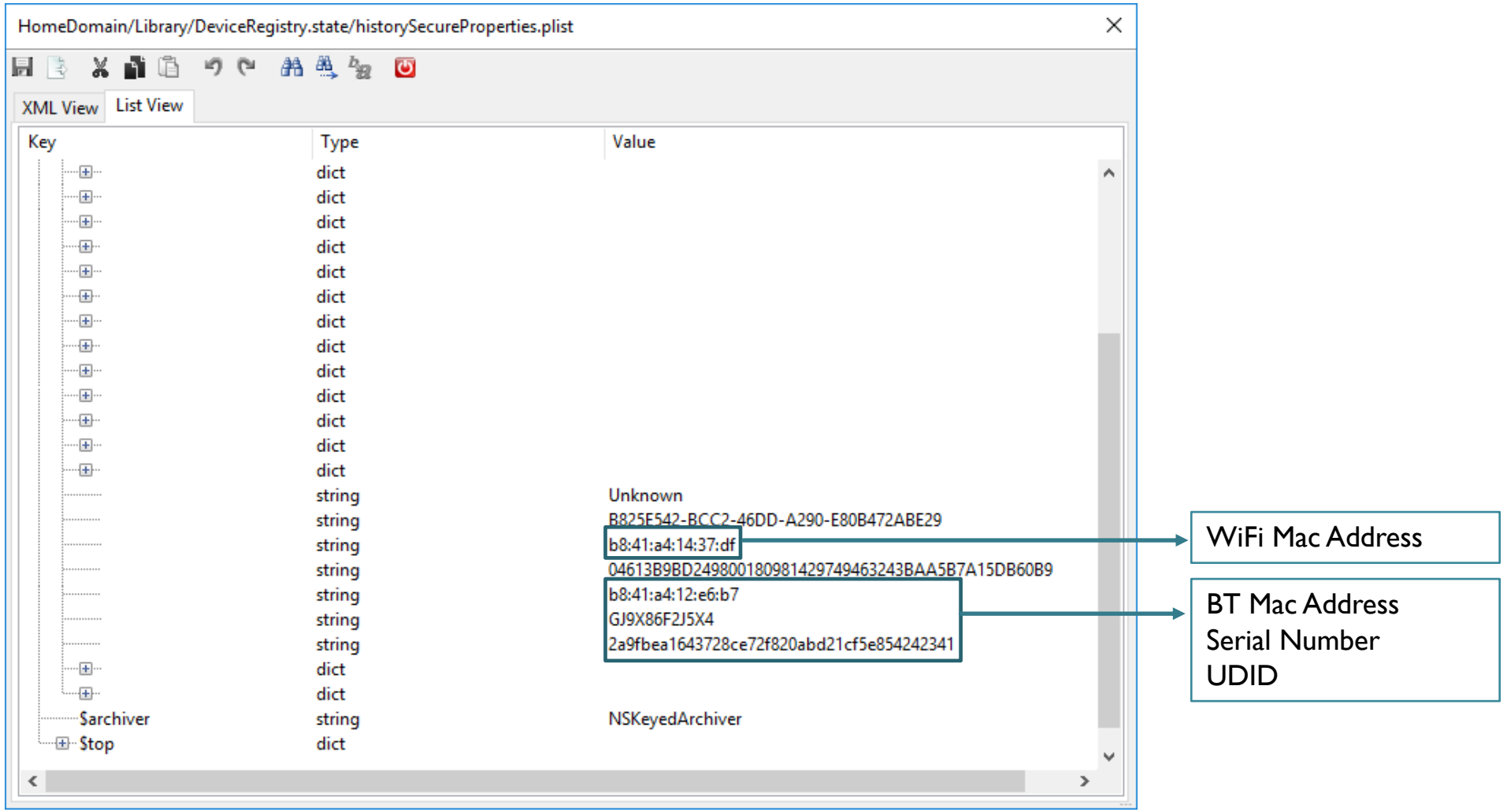
BACKUP EXTRACTION

- 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!**

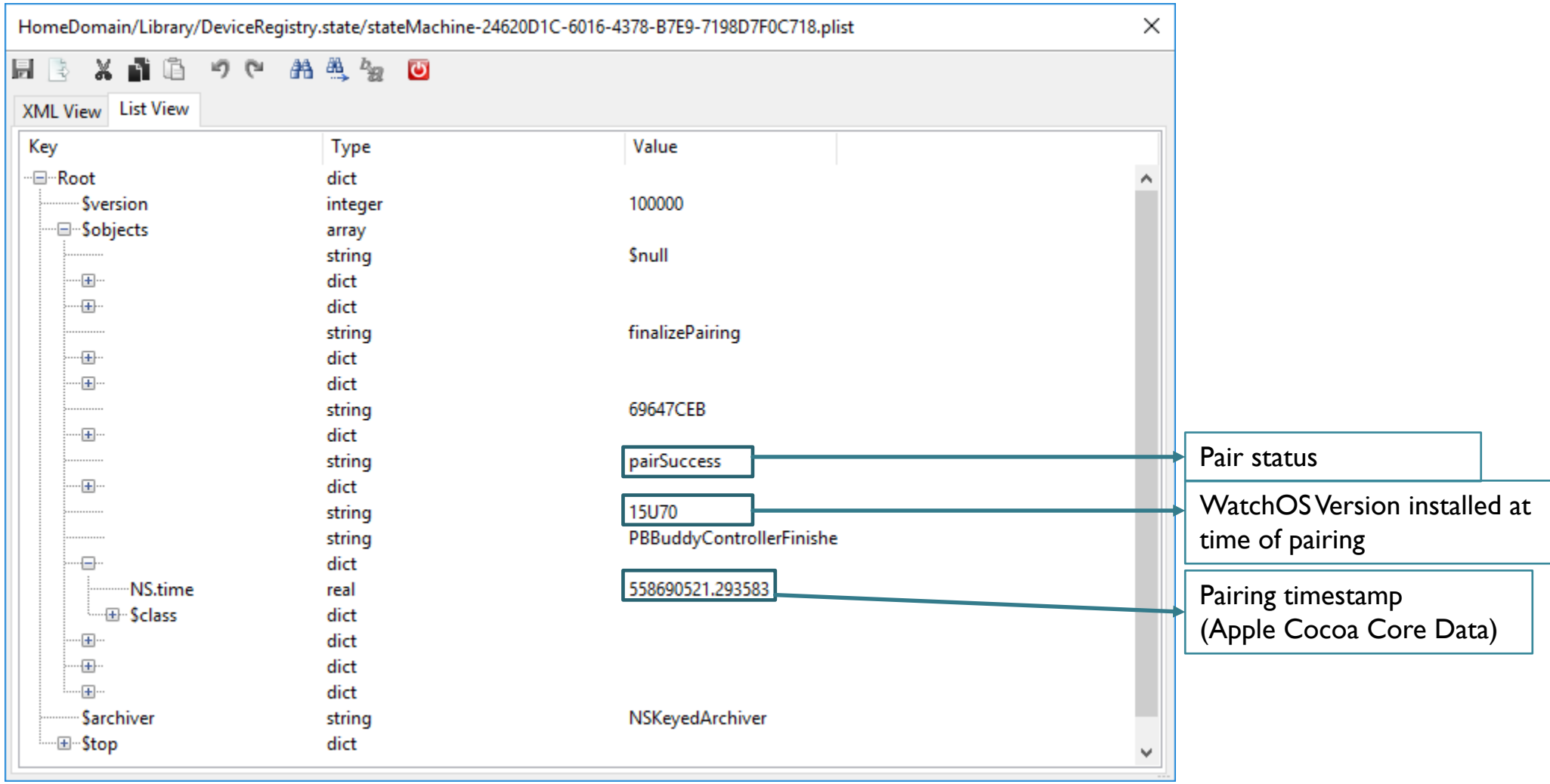
APPLE WATCH IOS BACKUP



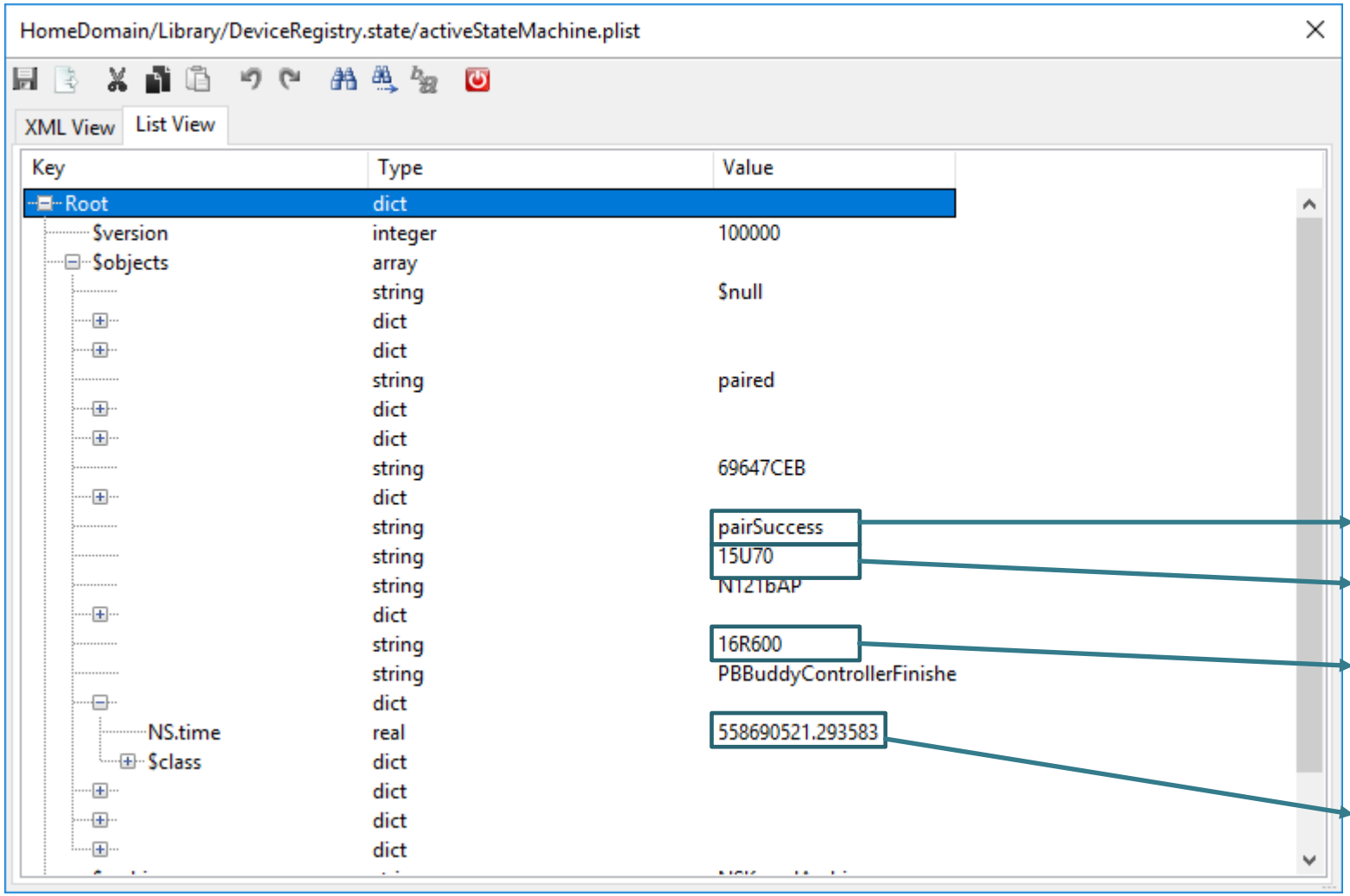
APPLE WATCH
IOS BACKUP – **HISTORYSECUREPROPERTIES.PLIST**



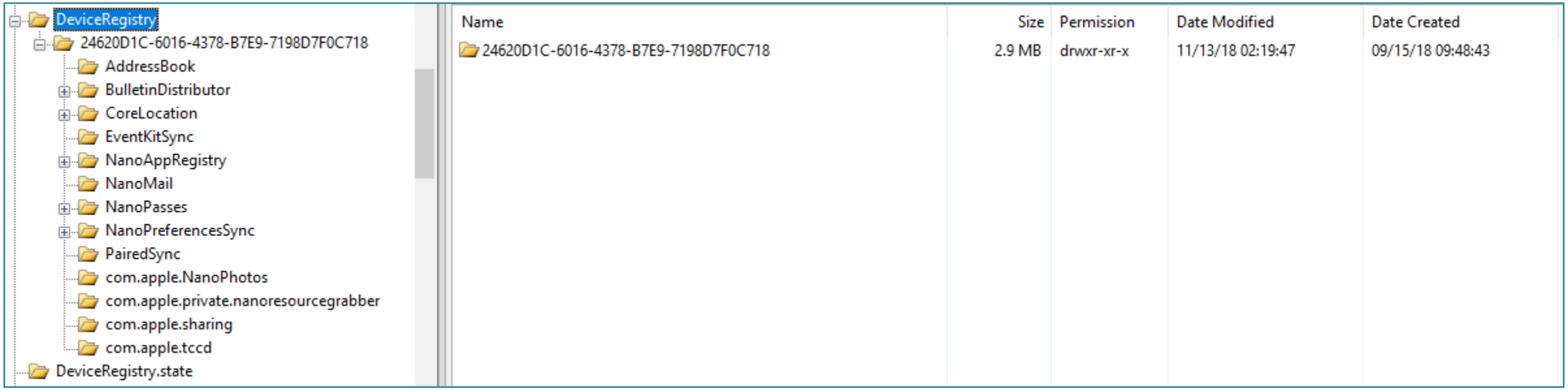
APPLE WATCH
IOS BACKUP – **STATEMACHINE-<GUID>.PLIST**



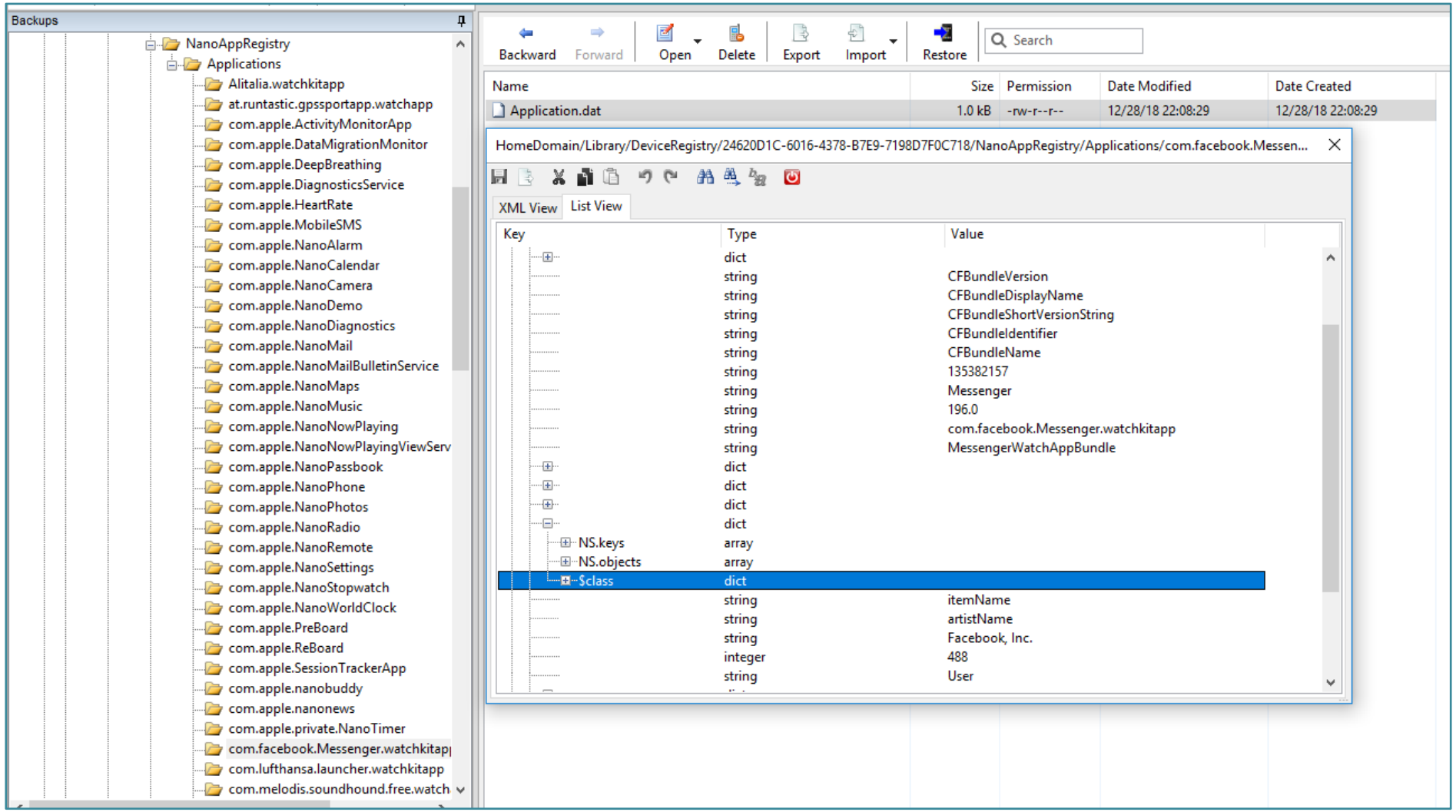
APPLE WATCH
IOS BACKUP – **ACTIVESTATEMACHINE.PLIST**



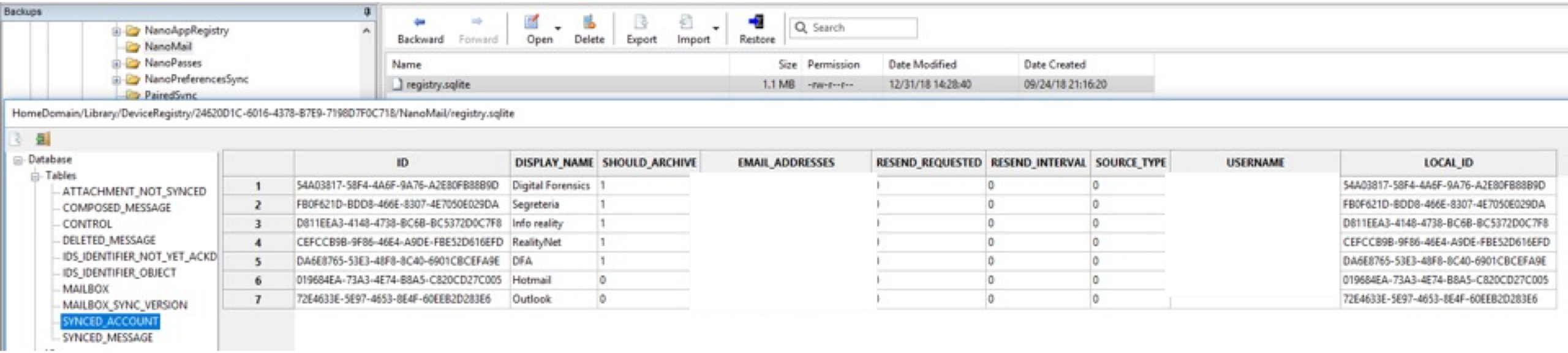
APPLE WATCH
IOS BACKUP – **DEVICEREGISTRY**



APPLE WATCH
IOS BACKUP – **NANOAPPREGISTRY**

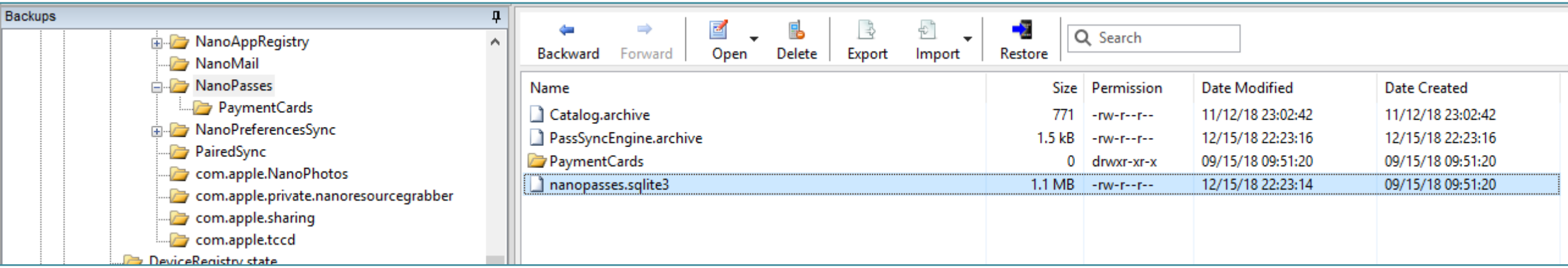


APPLE WATCH
IOS BACKUP – **NANOMAIL\REGISTRY.SQLITE**



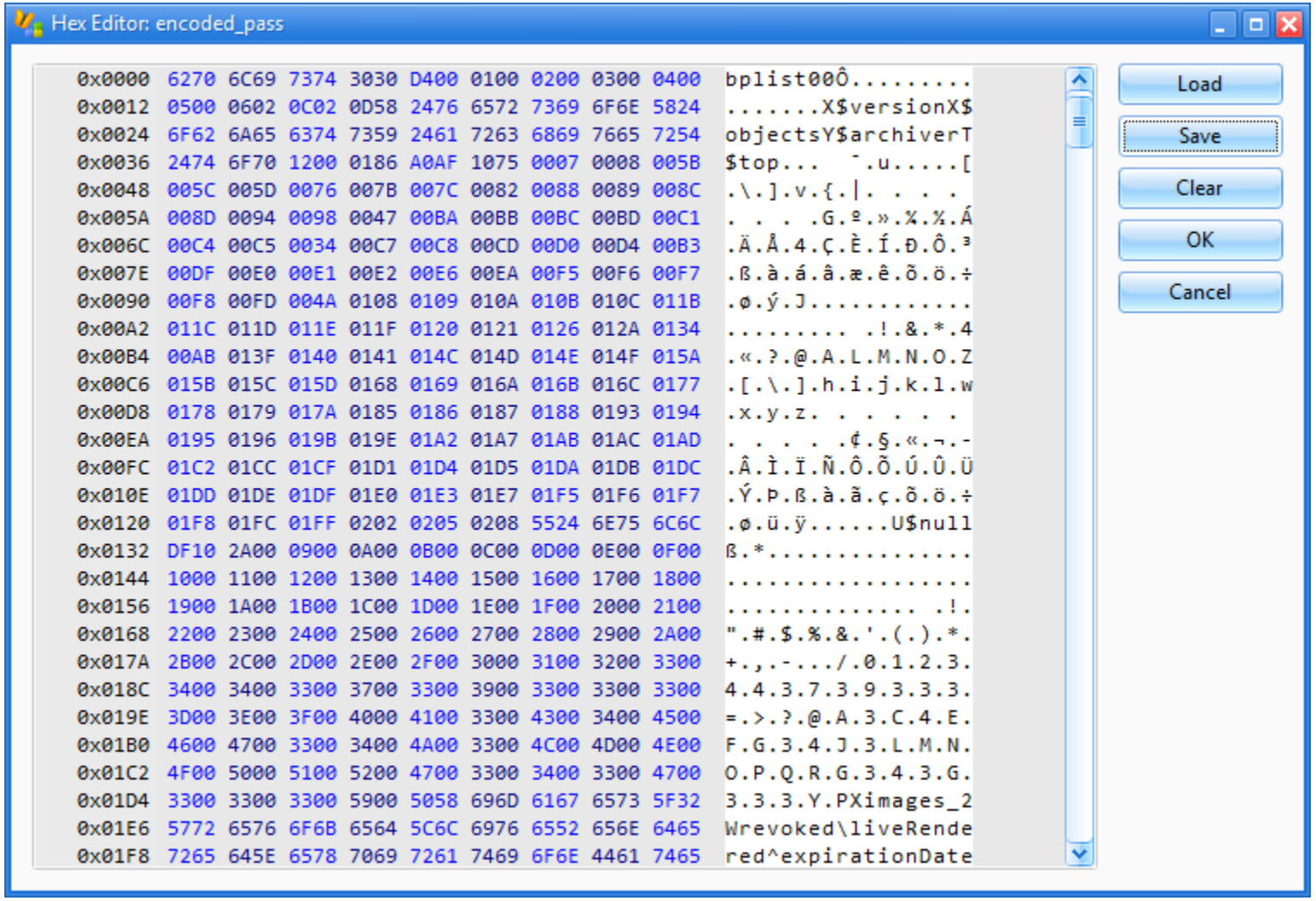
	ID	DISPLAY_NAME	SHOULD_ARCHIVE	EMAIL_ADDRESSES	RESEND_REQUESTED	RESEND_INTERVAL	SOURCE_TYPE	USERNAME	LOCAL_ID
1	54A03817-58F4-4A6F-9A76-A2E80FB88B9D	Digital Forensics	1			0	0		54A03817-58F4-4A6F-9A76-A2E80FB88B9D
2	FB0F621D-BDD8-466E-8307-4E7050E029DA	Segreteria	1			0	0		FB0F621D-BDD8-466E-8307-4E7050E029DA
3	D811EEA3-4148-4738-BC6B-BC5372D0C7F8	Info reality	1			0	0		D811EEA3-4148-4738-BC6B-BC5372D0C7F8
4	CEFCCB9B-9F86-46E4-A9DE-FBE52D616EFD	RealityNet	1			0	0		CEFCCB9B-9F86-46E4-A9DE-FBE52D616EFD
5	DA6E8765-53E3-48F8-8C40-6901CBCEFA9E	DFA	1			0	0		DA6E8765-53E3-48F8-8C40-6901CBCEFA9E
6	019684EA-73A3-4E74-B8A5-C820CD27C005	Hotmail	0			0	0		019684EA-73A3-4E74-B8A5-C820CD27C005
7	72E4633E-5E97-4653-8E4F-60EEB2D283E6	Outlook	0			0	0		72E4633E-5E97-4653-8E4F-60EEB2D283E6

APPLE WATCH
IOS BACKUP – **NANOPASSES\NANOPASSES.SQLITE3**

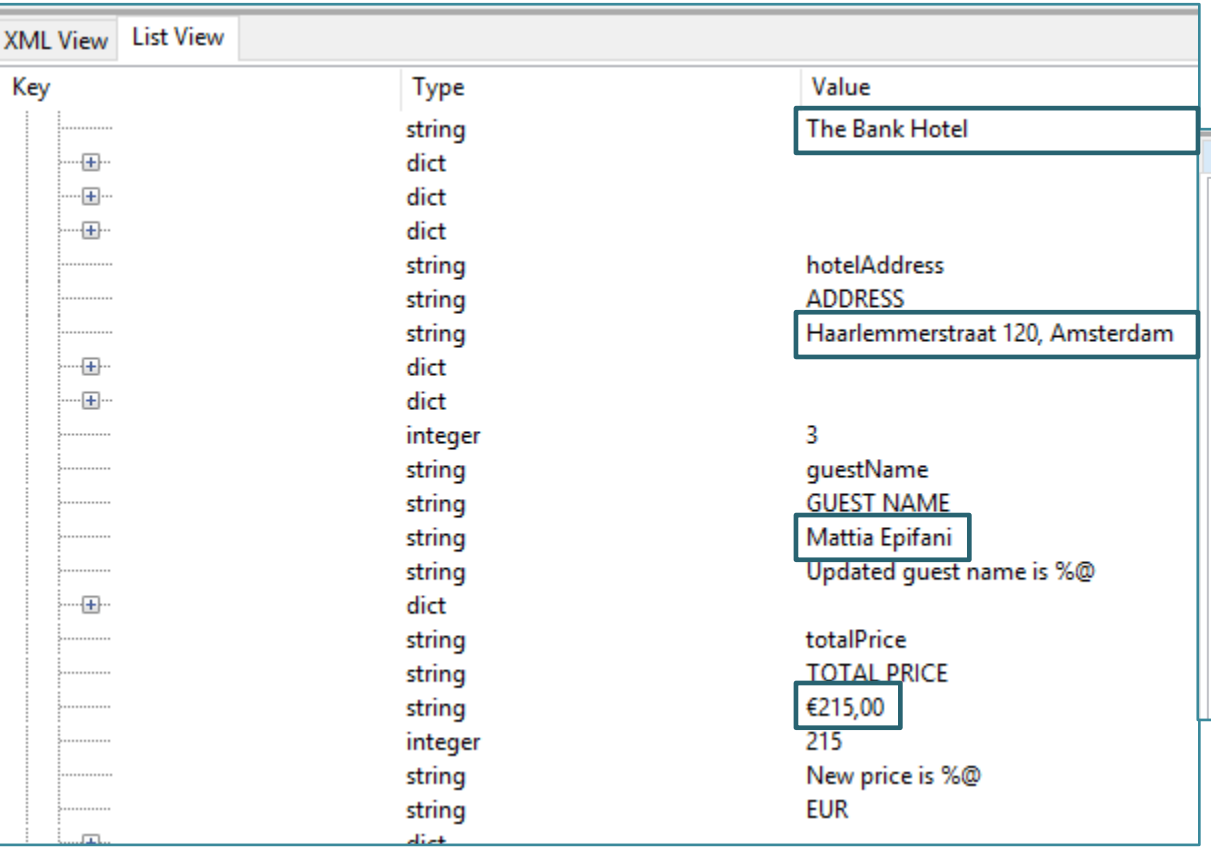


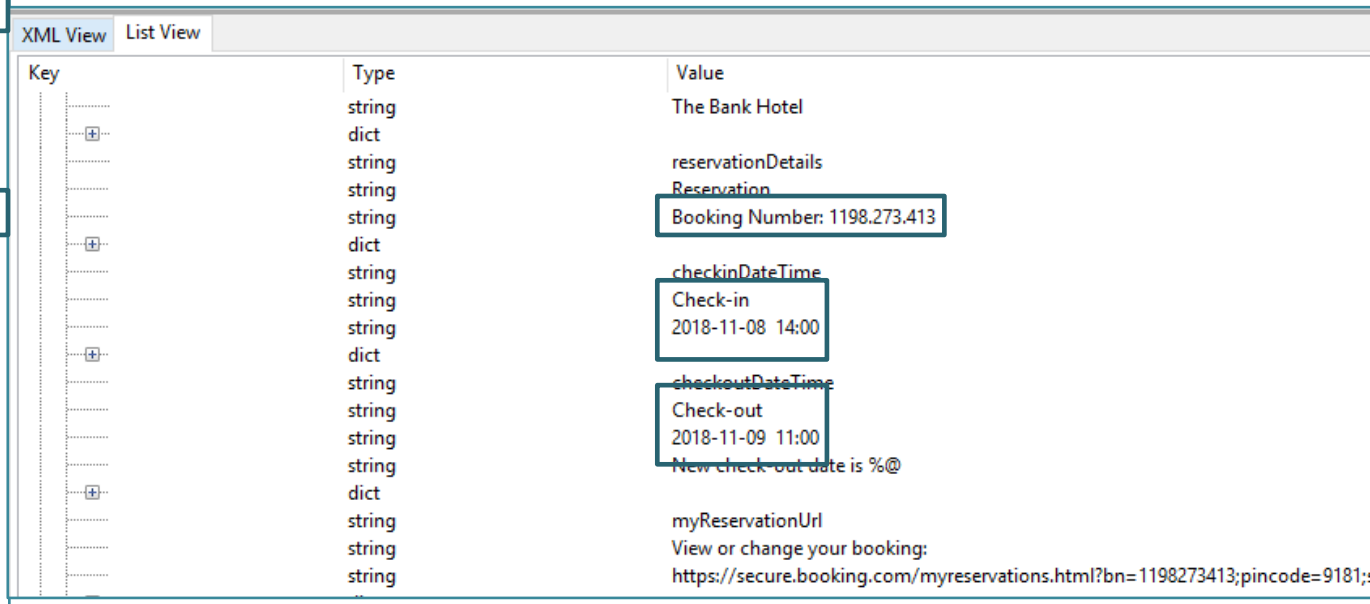
unique_id	type_id	organization_name	ingested_date	localized_description
Click here to define a filter				
Oc+NJo83fq3-17eDWmzVSyHPfzU=	pass.com.booking.reservation	Booking.com	563059511	Situato nel quartiere Jordaan di Amsterdam, il moderno Bank Hotel si trova nell'antico edificio di una ex banca sulla via Haarlemmerstraat, e offre eleganti camere con decorazioni sobrie, letti particolarmente lunghi e TV satellitare a schermo piatto. 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. 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.
IQx8nkFxkN4p+KDe8IZ0ViNJqag=	pass.com.bestwestern.rewards	Best Western Rewards®	558690775	Go. Get. Rewarded.

APPLE WATCH
IOS BACKUP – **NANOPASSES\NANOPASSES.SQLITE3**



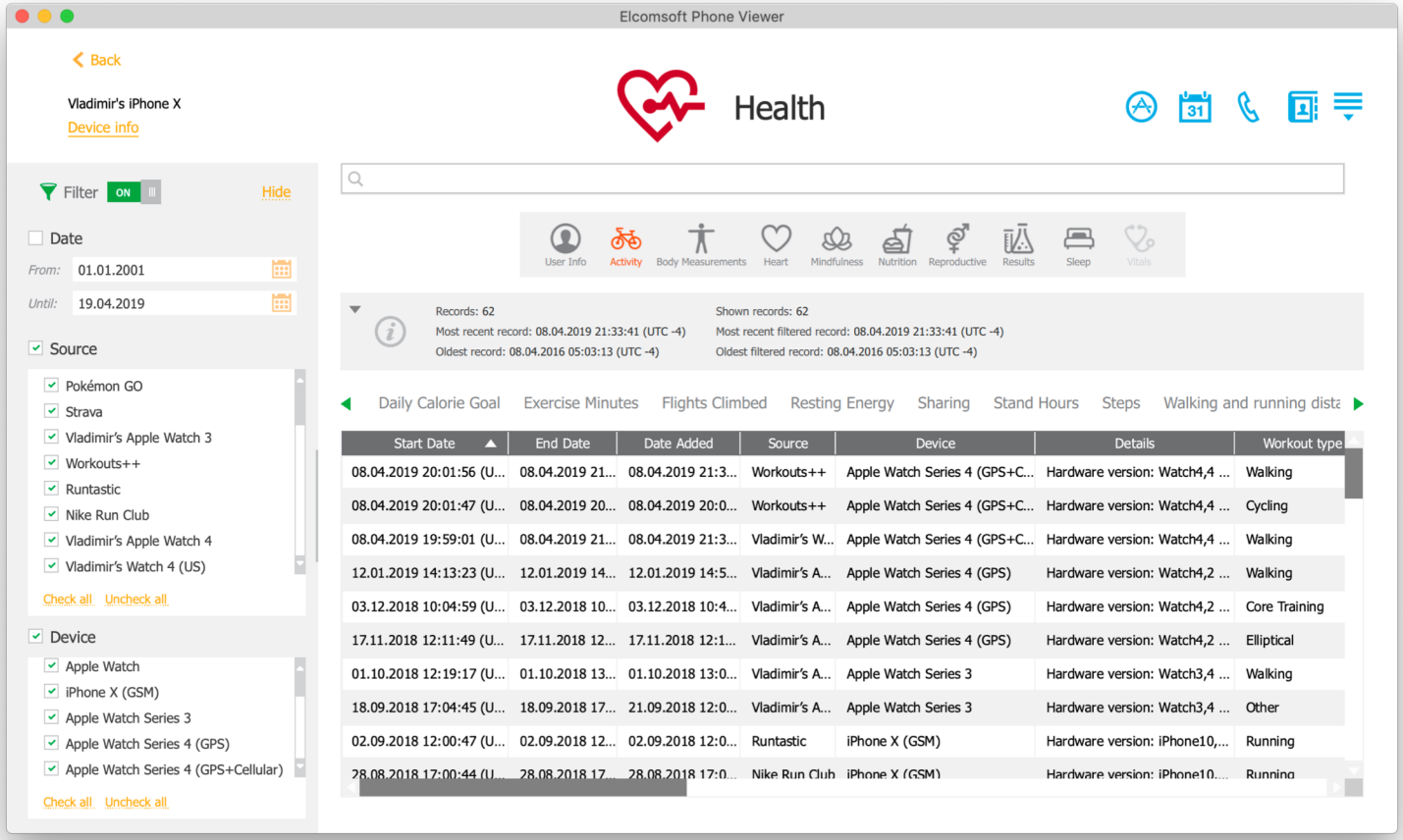
APPLE WATCH
IOS BACKUP – **NANOPASSES\NANOPASSES.SQLITE3**





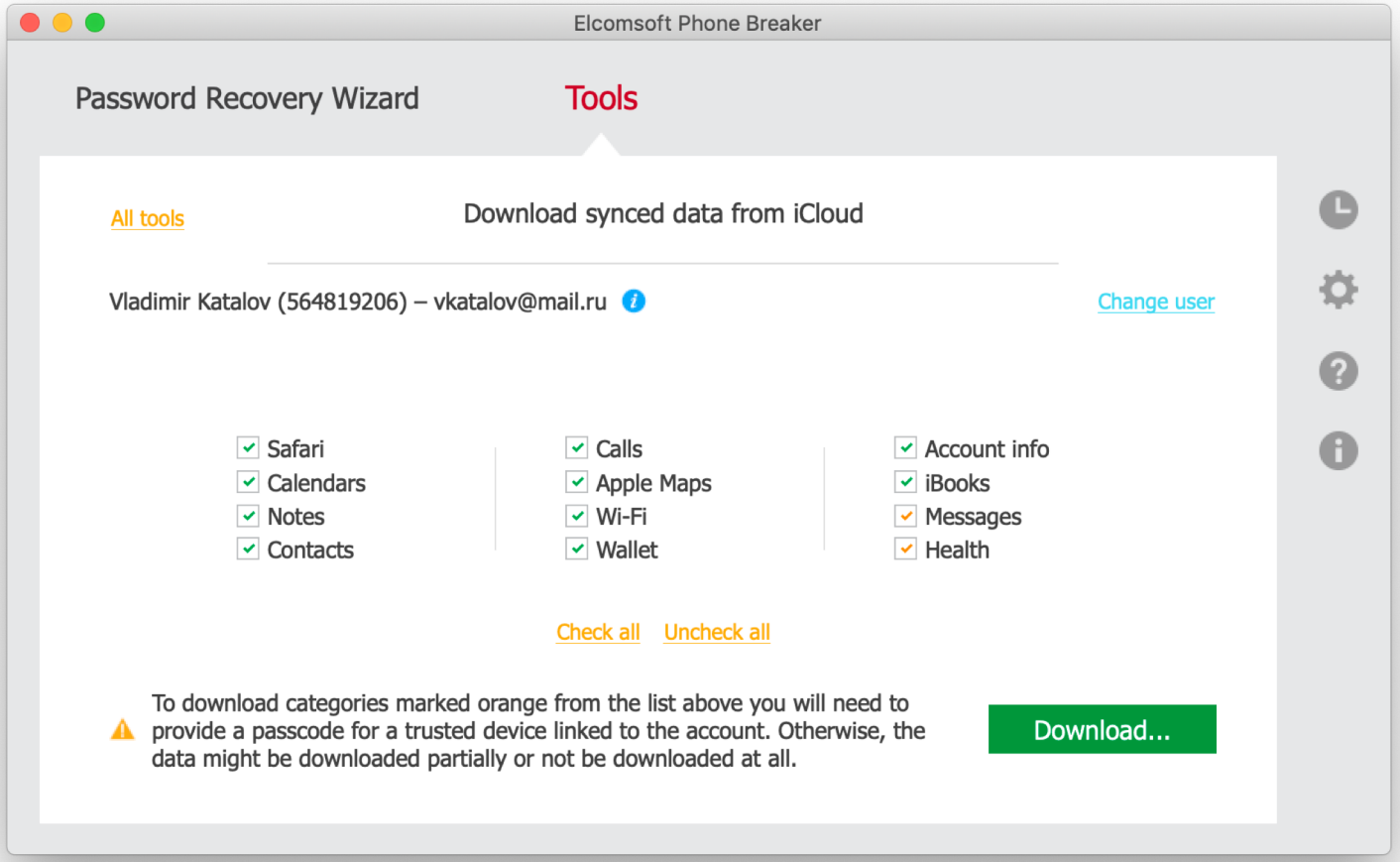
APPLE WATCH
HEALTH DATA IN LOCAL (ENCRYPTED) BACKUPS

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



APPLE WATCH
HEALTH DATA SYNCED WITH THE CLOUD

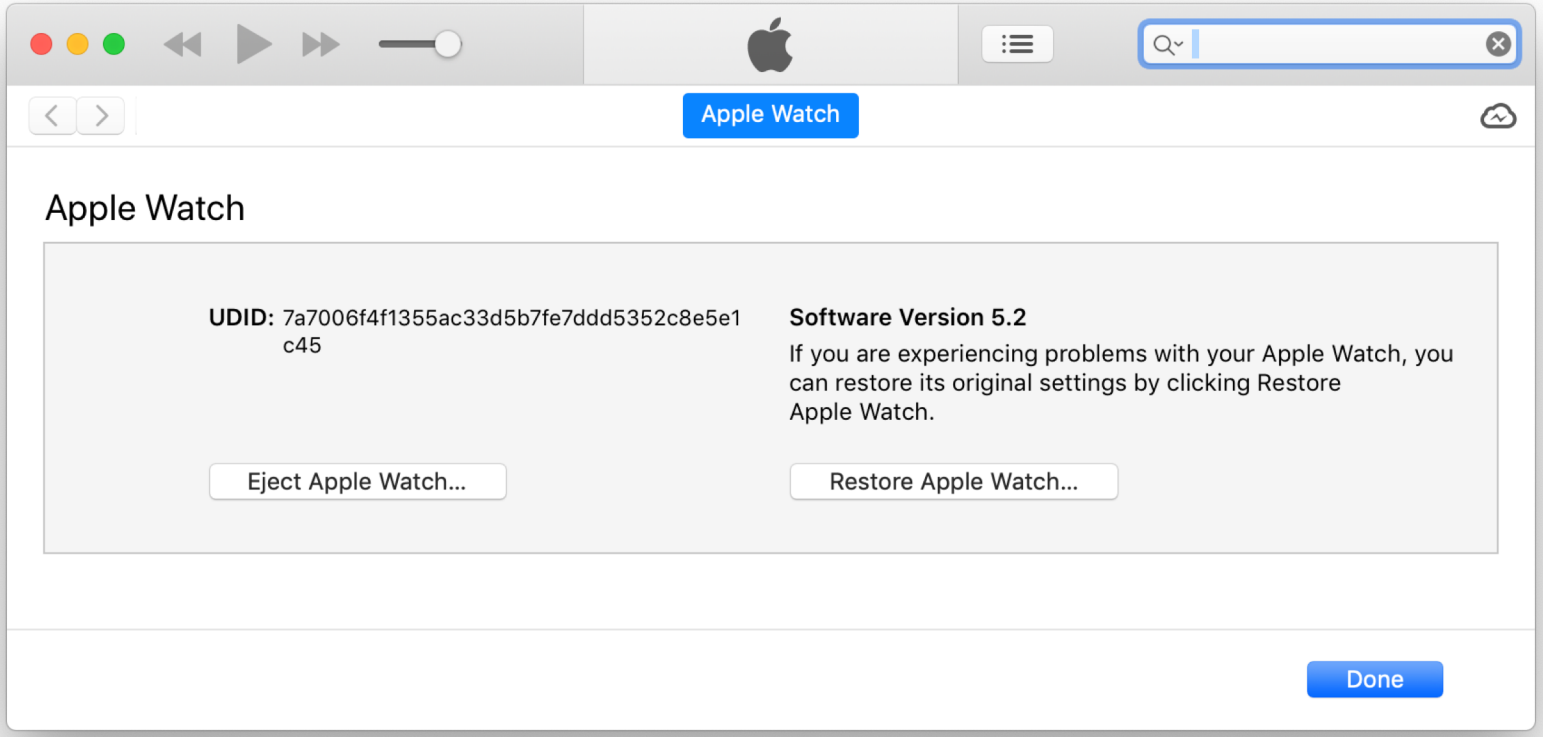
- No Health data in iCloud backups
- Health data is synced into the cloud since iOS 11
- Starting with iOS 12, it is saved in secure container; 2FA is required
- ECG data is not synced
- The key to encrypted data is protected with iCloud Keychain
- iCloud Keychain can be accessed only by trusted devices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



APPLE WATCH
CONNECTION WITH IBUS

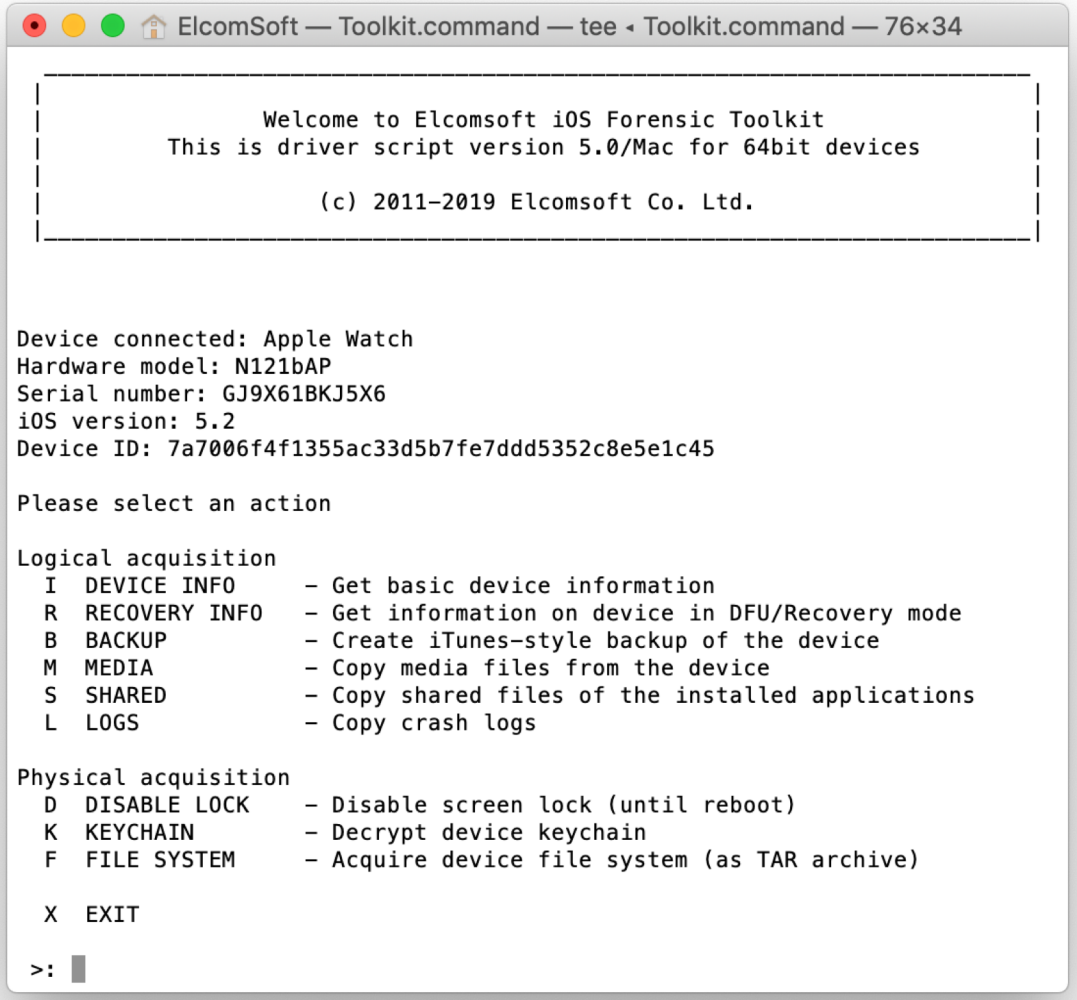
HTTPS://WWW.MFCBOX.COM/SHOP/CATEGORY/IBUS-TOOLS/

APPLE WATCH PAIRING

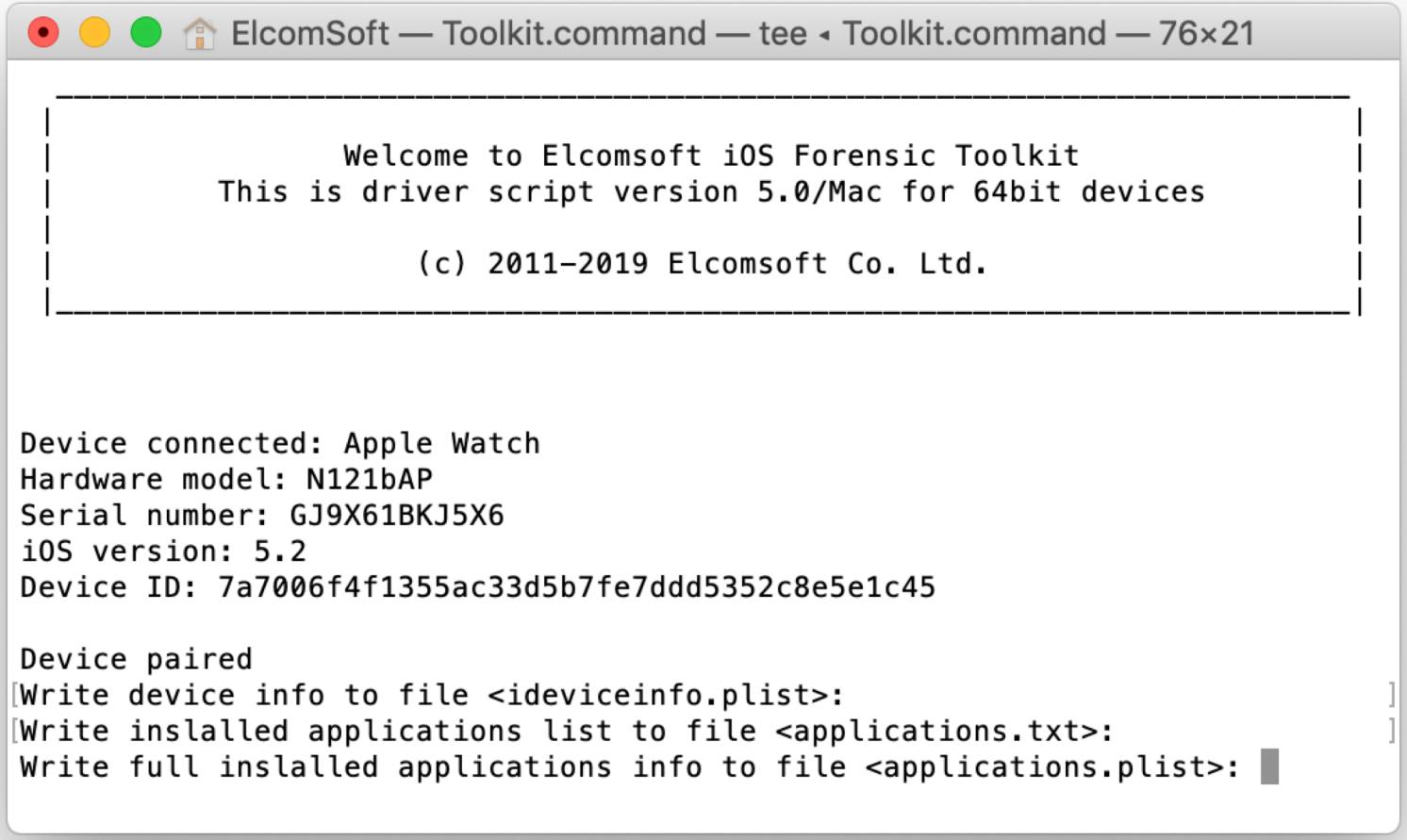


APPLE WATCH ACQUISITION OPTIONS

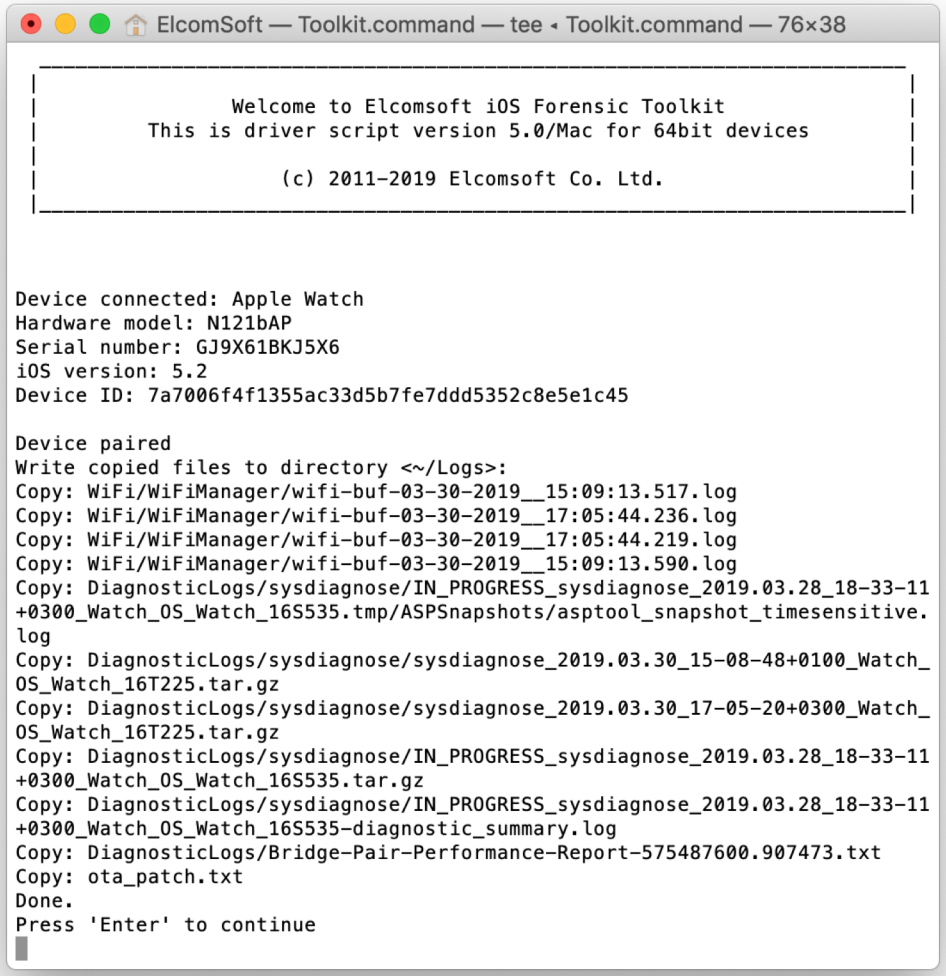
- Physical acquisition **might** be available with a jailbreak
  (e.g. *vortex* exploit for watchOS 3.0-4.1)
- **No backup service is running on watchOS**
- Device information is available
- List of installed applications can be obtained
- Shared files: *sometimes* work, but a very limited number of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



APPLE WATCH
EXTRACT APP LIST



APPLE WATCH EXTRACT LOGS



APPLE WATCH MEDIA FILES

ElcomSoft — Toolkit.command — tee ◂ Toolkit.command — 77×23

```
 _____________________________________________________________________________
|                                                                             |
|                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 — 77×23

```
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
```

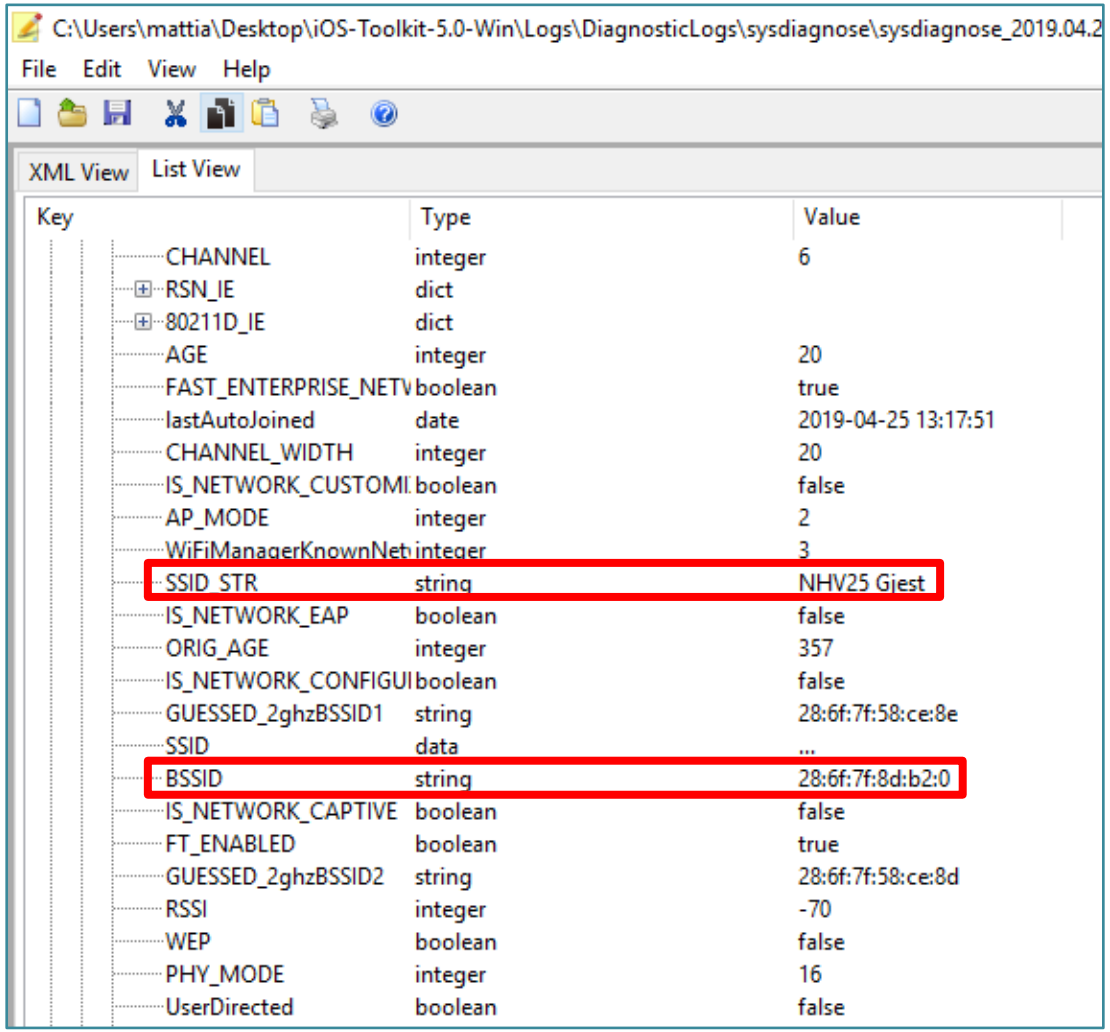
APPLE WATCH
DEVICE INFO – ELCOMSOFT IOS FORENSIC TOOLKIT

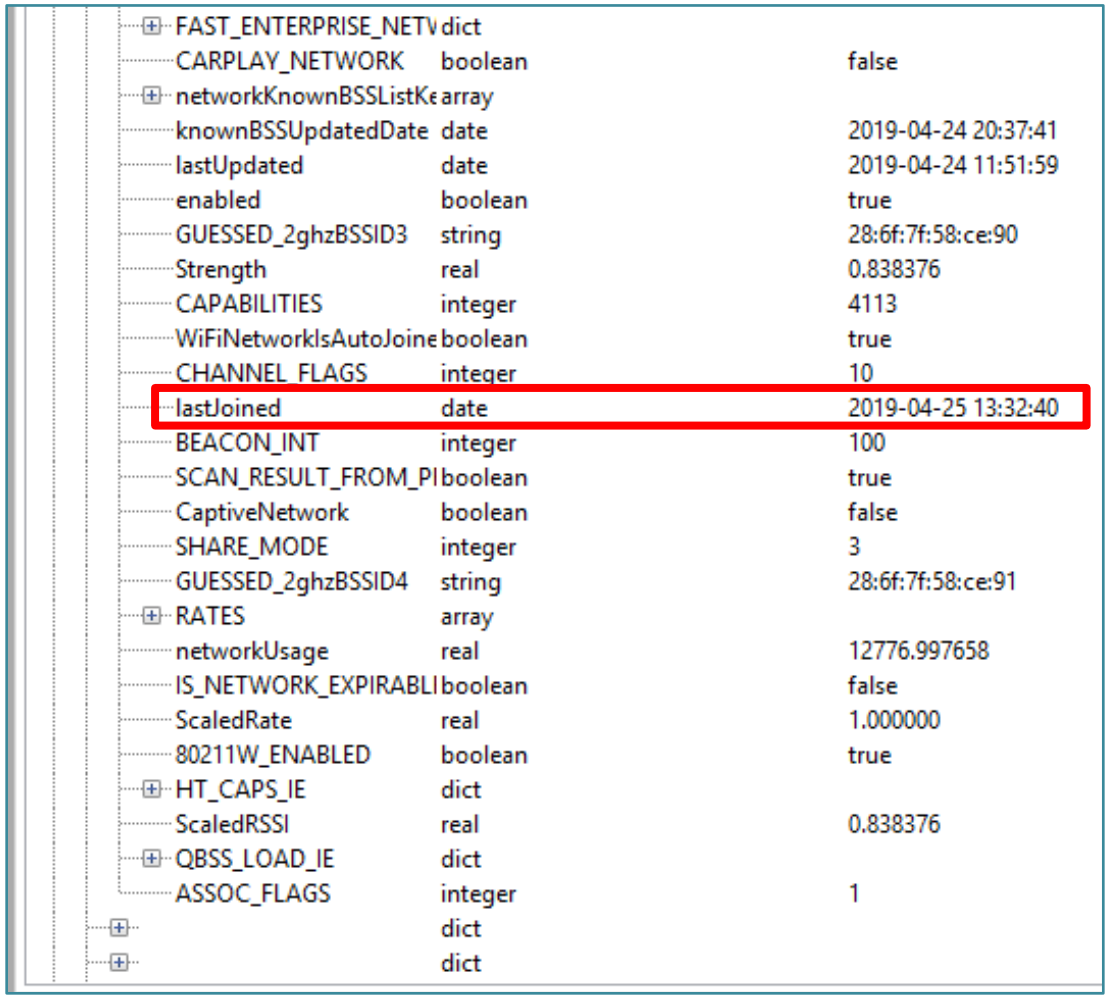
Field name	Field value
Hardware Model	N121bAP
Serial Number	GJ9X86F2J5X4
Bluetooth Address	b8:41:a4:12:e6:b7
WiFi Address	b8:41:a4:14:37:df
UniqueDeviceID	2a9fbea1643728ce72f820abd21cf5e85424234
DeviceName	Apple Watch di Mattia
ProductType	Watch3,4
ProductVersion	5.1.1
BuildVersion	16R600
TimeZone	Europe/Rome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

APPLE WATCH
INSTALLED APPLICATIONS – ELCOMSOFT IOS FORENSIC TOOLKIT

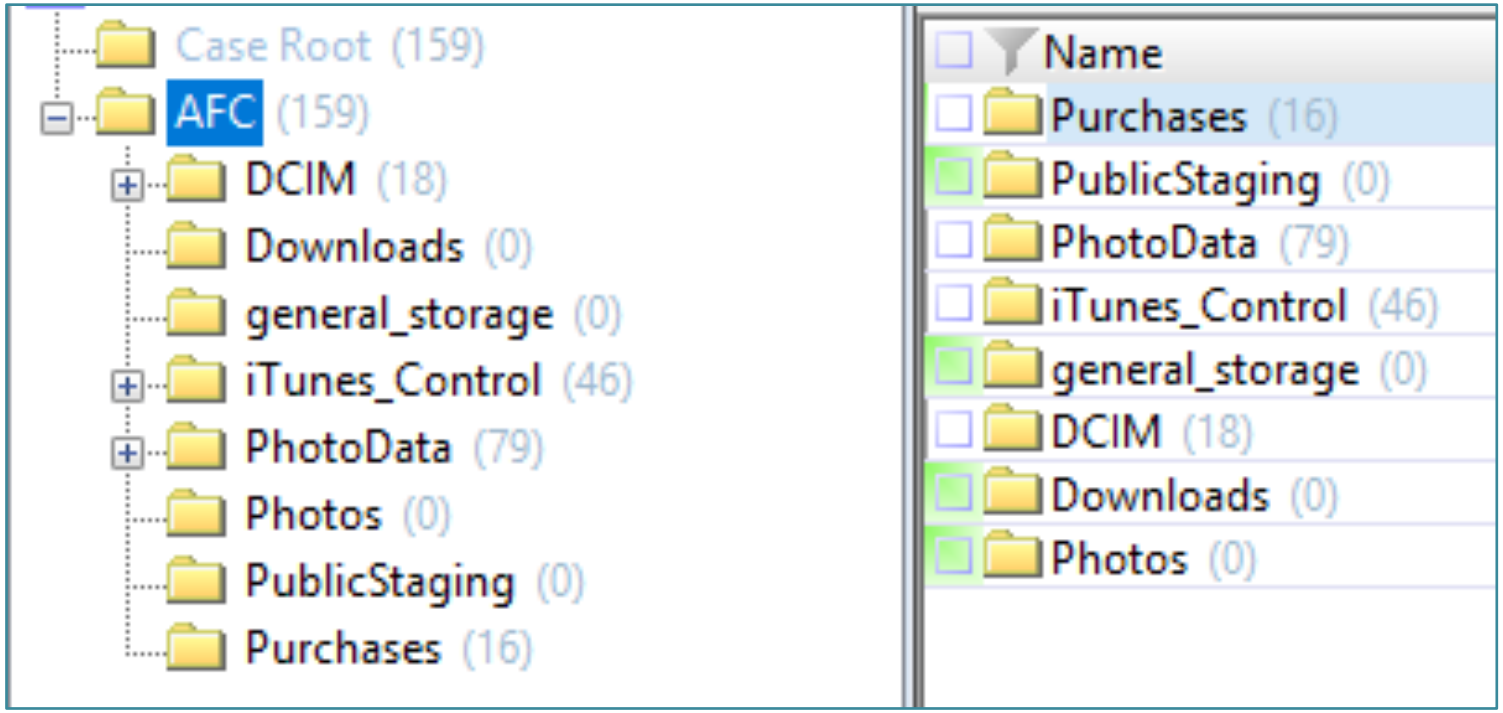
Field name	Field value
ApplicationDSID	1321761630
Path	/private/var/containers/Bundle/Application/83A3C4E9-F7A7-4813-AE28-311494787654/MessengerWatchAppBundle.app
CFBundleExecutable	MessengerWatchAppBundle
CFBundleName	Messenger
CFBundleVersion	133700421
LSRequiresIPhoneOS	True
WKCompanionAppBundleIdentifier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

APPLE WATCH LOGS

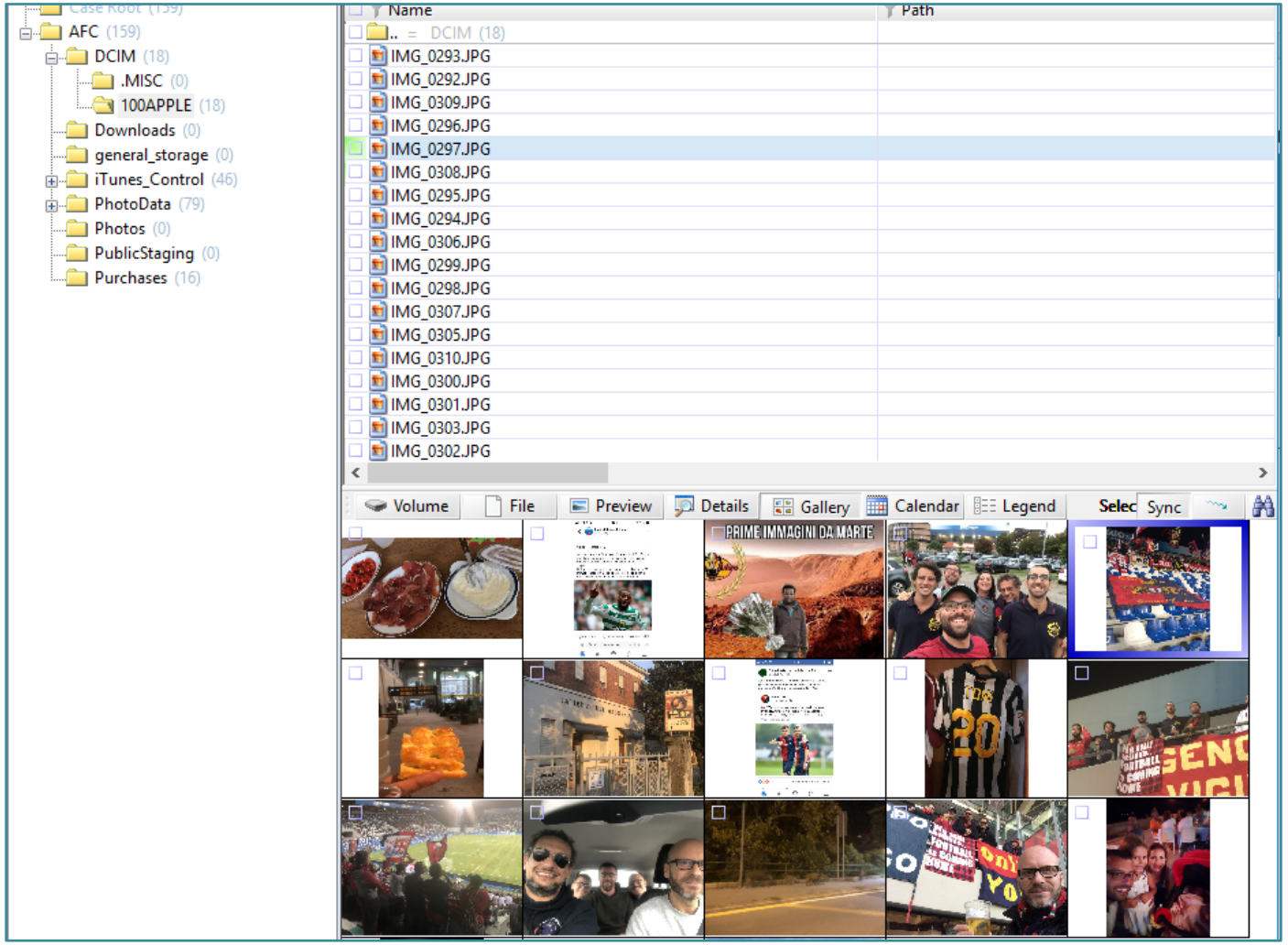




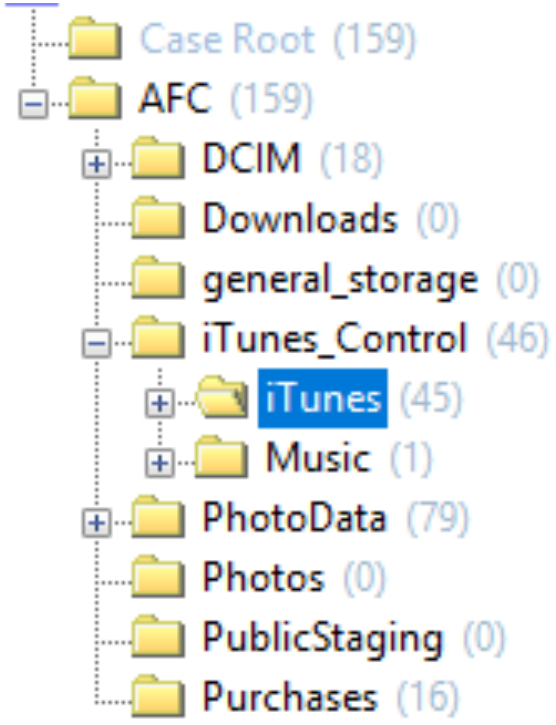
APPLE WATCH
AFC ACQUISITION

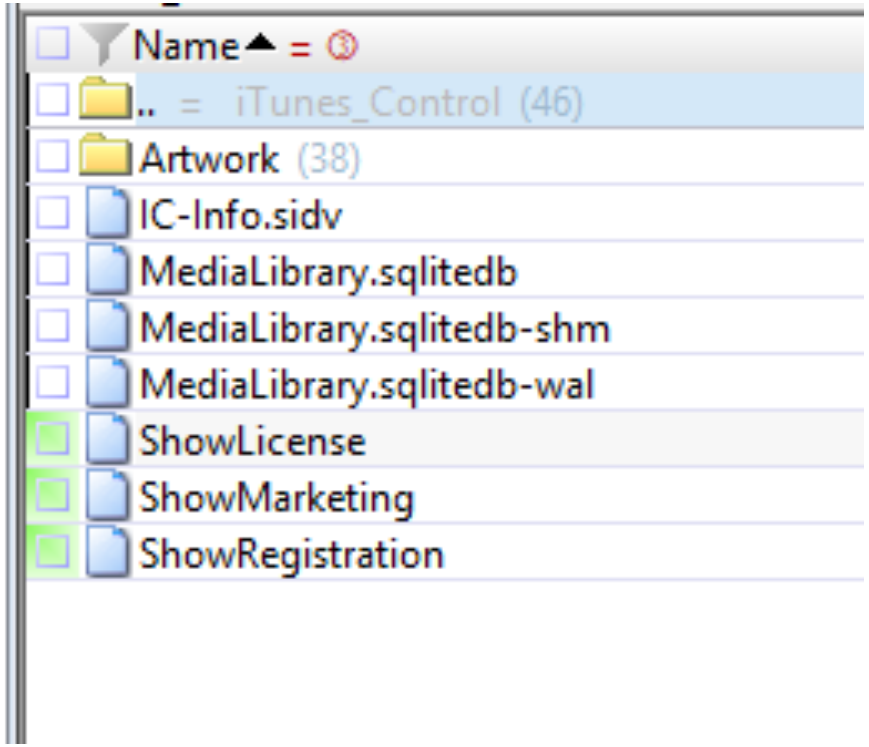


APPLE WATCH
AFC – **DCIM** FOLDER

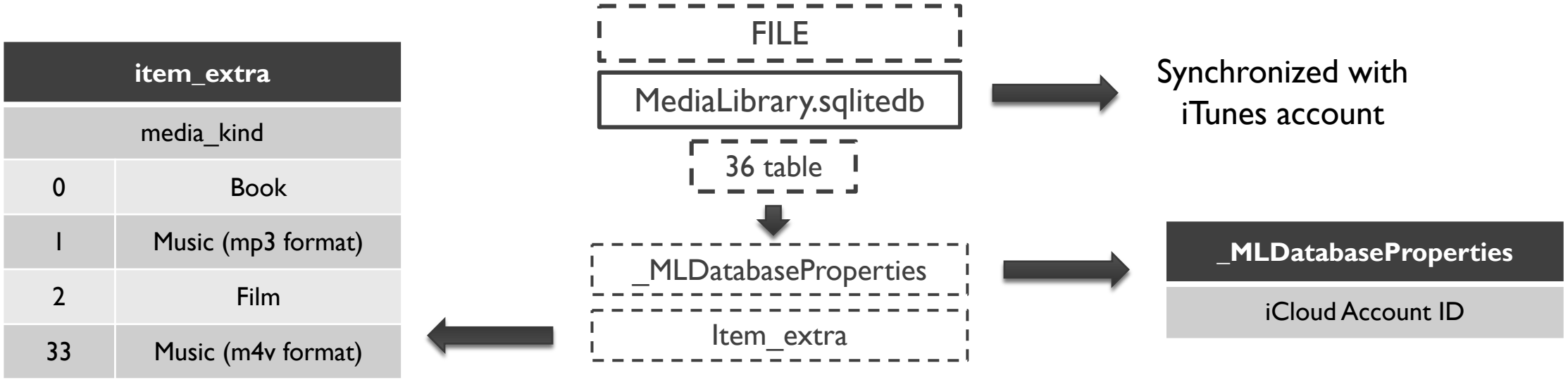


APPLE WATCH
AFC – **ITUNES_CONTROL/ITUNES**





APPLE WATCH
AFC – **ITUNES_CONTROL/ITUNES/MEDIALIBRARY.SQLITEDB**



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

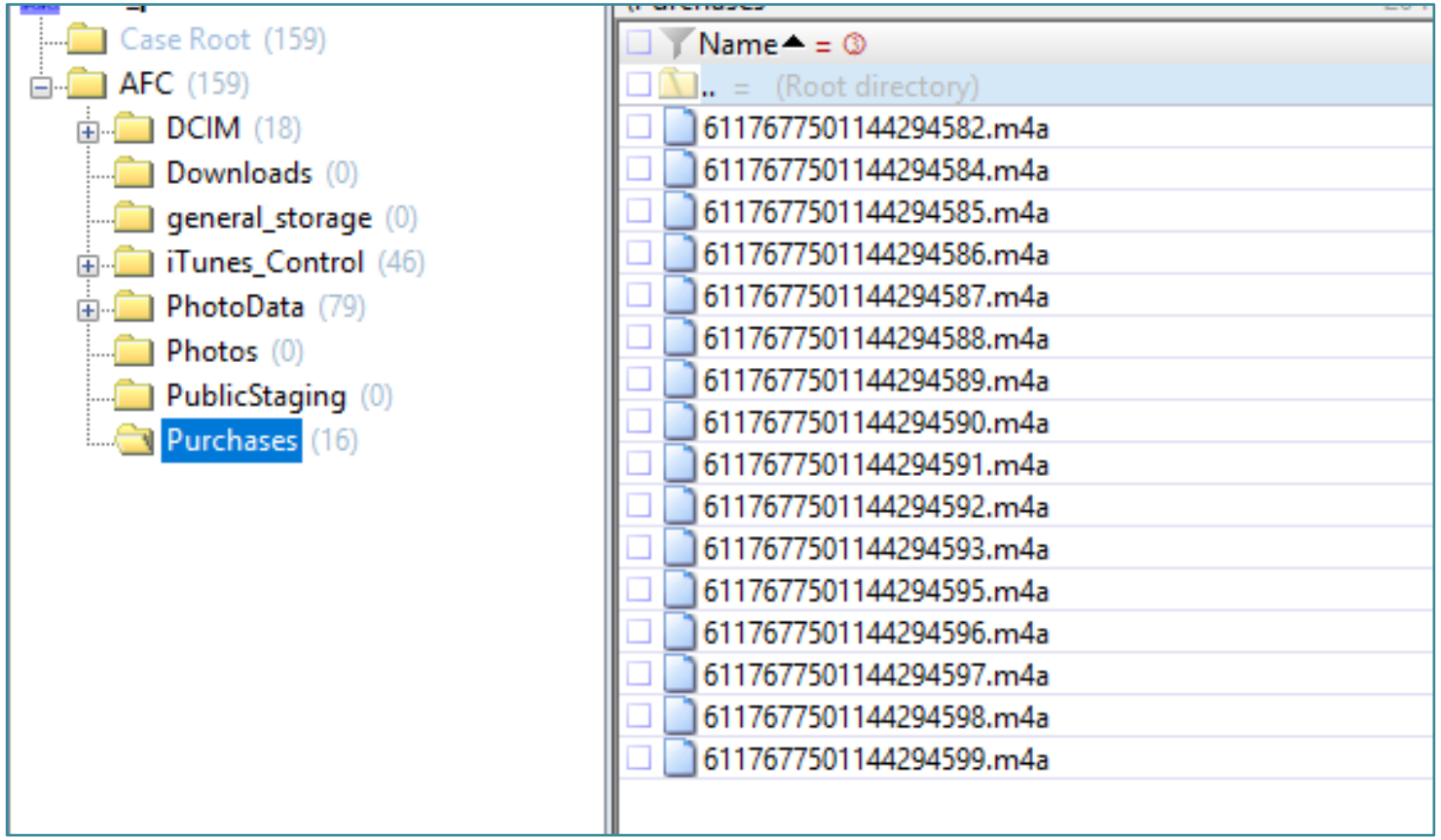
APPLE WATCH
AFC – ITUNES_CONTROL/ITUNES/MEDIALIBRARY.SQLITEDB

```
select
ext.title AS "Title",
ext.media_kind AS "Media Type",
itep.format AS "File format",
ext.location AS "File",
ext.total_time_ms AS "Total time (ms)",
ext.file_size AS "File size",
ext.year AS "Year",
alb.album AS "Album Name",
alba.album_artist AS "Artist",
com.composer AS "Composer",
gen.genre AS "Genre",
art.artwork_token AS "Artwork",
itev.extended_content_rating AS "Content rating",
itev.movie_info AS "Movie information",
ext.description_long AS "Description",
ite.track_number AS "Track number",
sto.account_id AS "Account ID",
strftime('%d/%m/%Y %H:%M:%S', datetime(sto.date_purchased + 978397200,'unixepoch'))date_purchased,
sto.store_item_id AS "Item ID",
sto.purchase_history_id AS "Purchase History ID",
ext.copyright AS "Copyright"
from
item_extra ext
join item_store sto using (item_pid)
join item ite using (item_pid)
join item_stats ites using (item_pid)
join item_playback itep using (item_pid)
join item_video itev using (item_pid)
left join album alb on sto.item_pid=alb.representative_item_pid
left join album_artist alba on sto.item_pid=alba.representative_item_pid
left join composer com on sto.item_pid=com.representative_item_pid
left join genre gen on sto.item_pid=gen.representative_item_pid
left join item_artist itea on sto.item_pid=itea.representative_item_pid
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	**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	Delation is not possible
Call log	Deletion is propagated	Delation is not possible
SMS/iMessage	**Deletion IS NOT PROPAGATED**	**Deletion IS NOT PROPAGATED**
Mail	Deletion is propagated	Deletion is propagated
Calendar	Deletion is propagated	Delation is not possible
Wallet	Deletion is propagated	Delation is not possible
Telegram	Deletion is propagated	Delation is not possible
Facebook Messenger	Deletion is propagated	Delation is not possible