APPLE WATCH FORENSICS

MATTIA EPIFANI – FRANCESCO PICASSO

SANS DFIR EU SUMMIT

PRAGUE, 29 SEPTEMBER 2019

APPLE WATCH

- **Apple Watch** is a line of **smartwatches** designed and marketed by Apple Inc.
- It incorporates **fitness tracking** and **health-oriented capabilities**
- It works in **integration with an iPhone**
- As of September 2019, **4 models were produced**

APPLE WATCH IDENTIFICATION

HTTPS://SUPPORT.APPLE.COM/EN-US/HT204507

Model number	Generation
A1553 (38mm) / A1554 (42mm)	Apple Watch 1st Generation
A1802 (38mm) / A1803 (42mm)	Apple Watch Series 1
A1757 (38mm) / A1758 (42mm) A1816 (38mm) / A1817 (42mm)	Apple Watch Series 2
A1858 (38mm) / A1859 (42mm)	Apple Watch Series 3 (GPS)
America A1860 (38mm) / A1861(42mm) **Europe and Asia** A1889 (38mm) / A1891(42mm) **China** A1890 (38mm) / A1892 (42mm)	Apple Watch Series 3 (GPS+Cellular)
A1977 (38mm) / A1978 (42mm)	Apple Watch Series 4 (GPS)
America A1975 (38mm) / A1976 (42mm) **Europe,Asia and China** A2007 (38mm) / A2008 (42mm)	Apple Watch Series 4 (GPS+Cellular)

APPLE WATCH IDENTIFICATION

HTTPS://SUPPORT.APPLE.COM/EN-US/HT204507

1° Generation	Apple Watch 1	Apple Watch 2	App
			

APPLE WATCH ACQUISITION

- **Three options** for data acquisition:
  - Device
    - Direct connection
    - Manual acquisition
  - Synced iPhone
  - Cloud (iPhone backup and synced Health data)

APPLE WATCH FORENSICS – DEVICE ACQUISITION

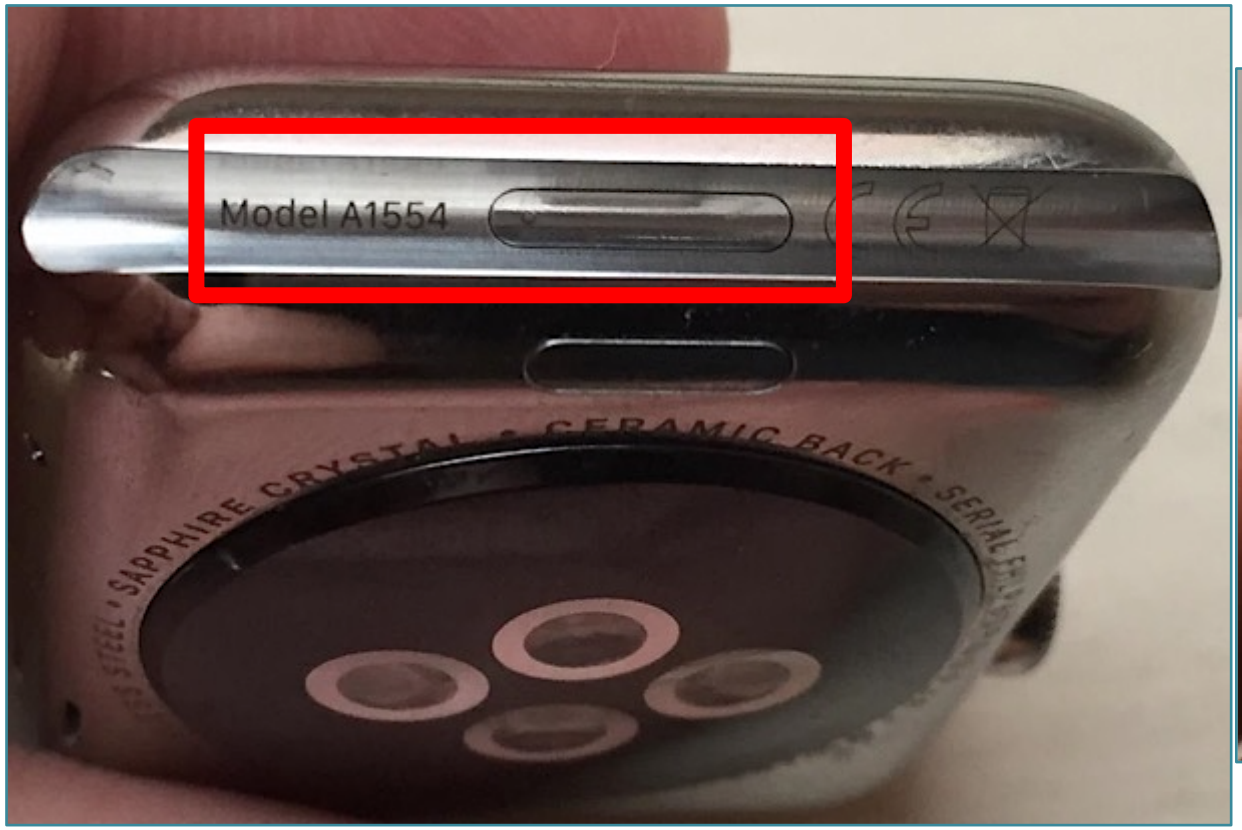
MATTIA EPIFANI – FRANCESCO PICASSO

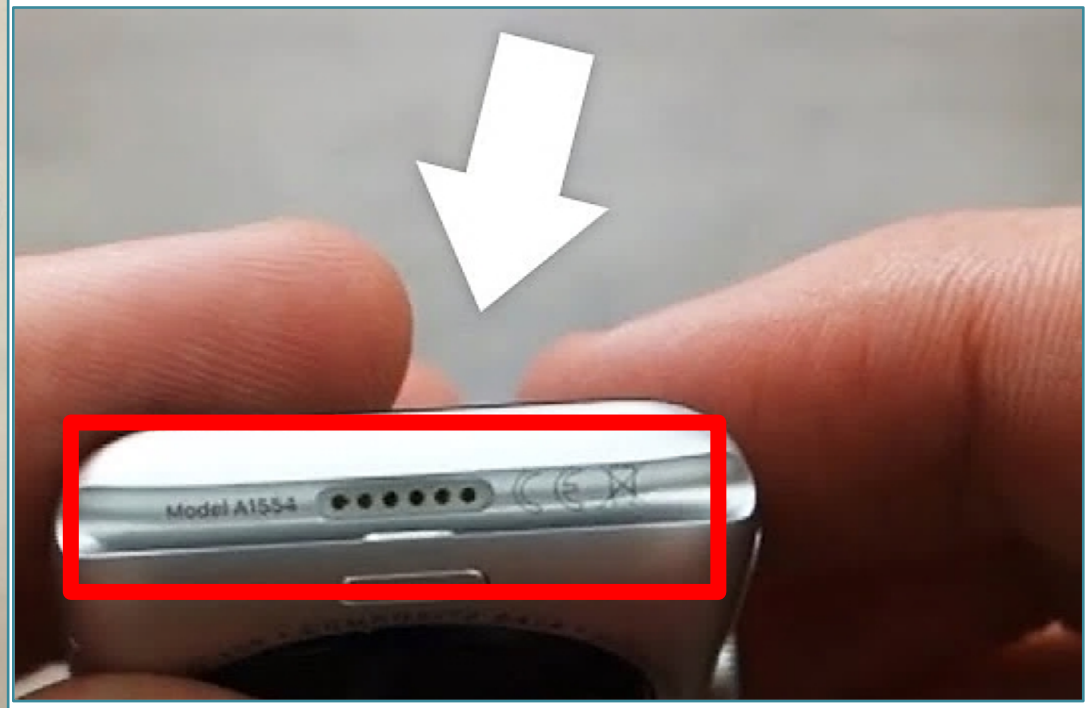
SANS DFIR EU SUMMIT

PRAGUE, 29 SEPTEMBER 2019

APPLE WATCH
THE "SECRET" (DIAGNOSTIC) PORT!

HTTPS://WWW.IDOWNLOADBLOG.COM/2015/04/13/APPLE-WATCH-DIAGNOSTIC-PORT/

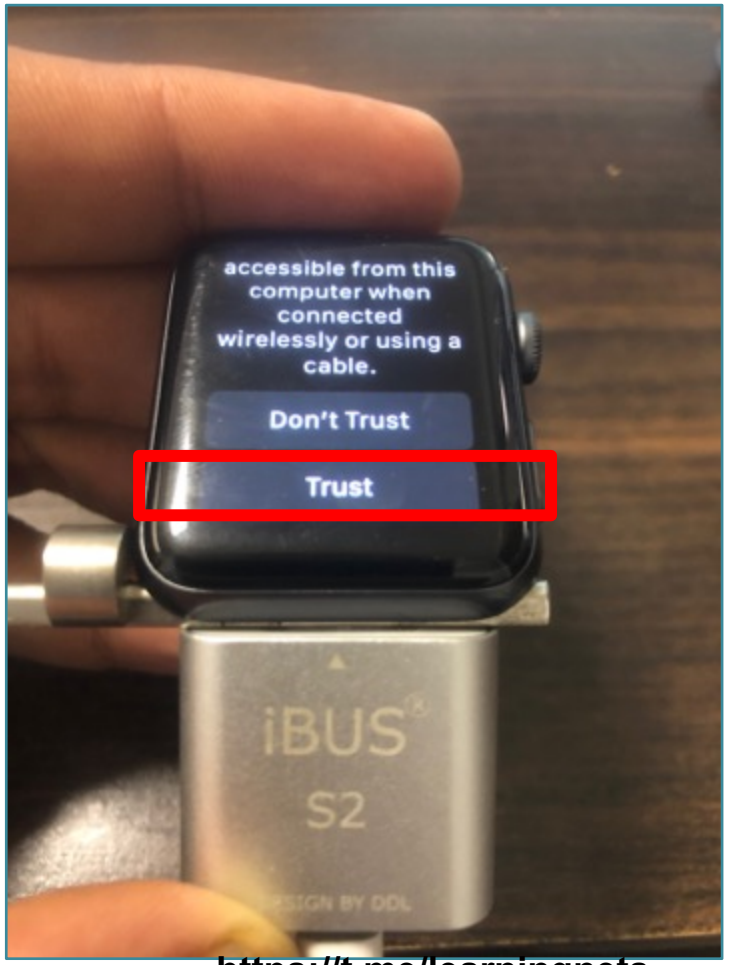


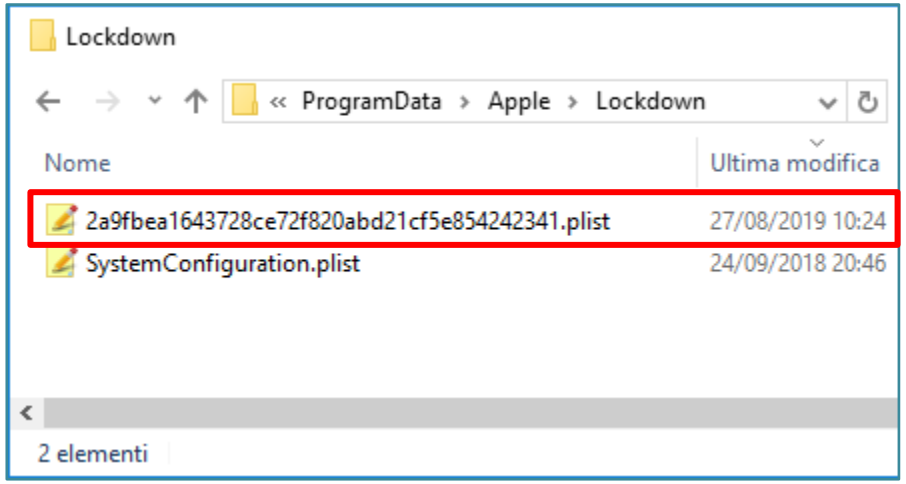


APPLE WATCH CONNECTION WITH IBUS

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

APPLE WATCH PAIRING



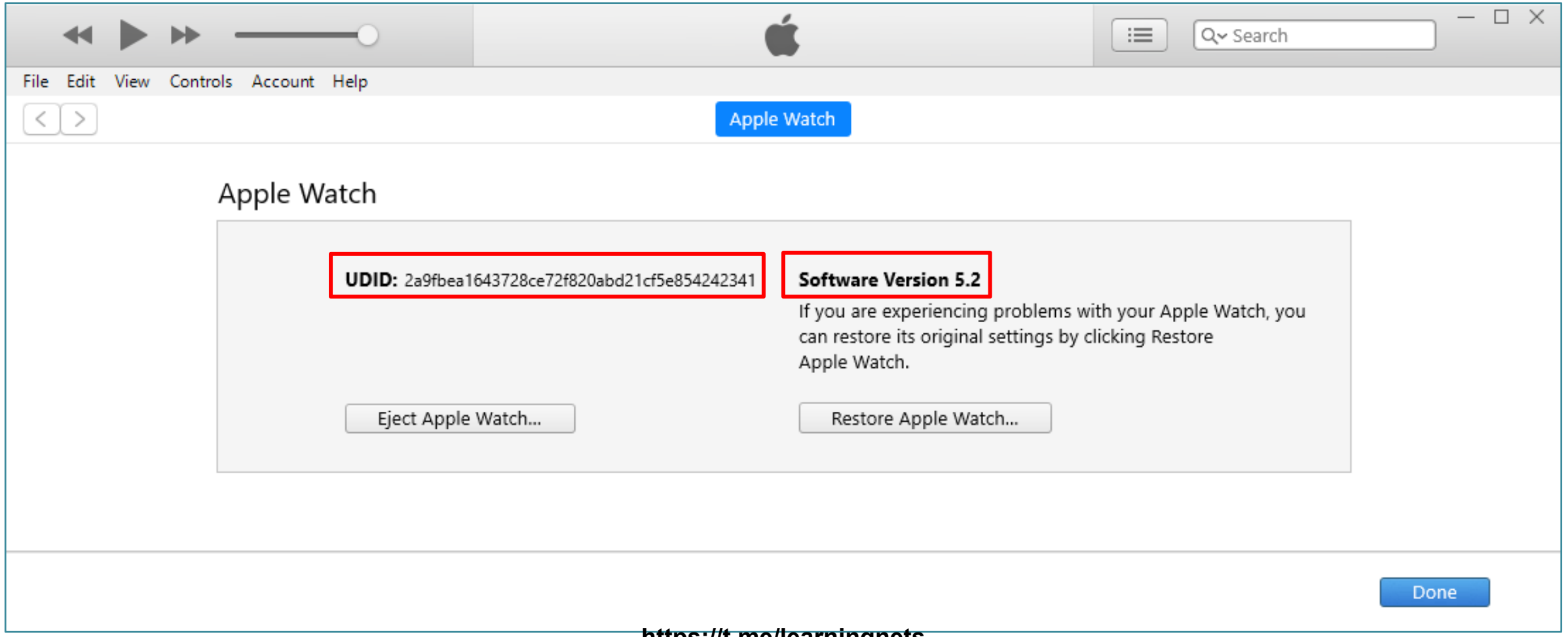


APPLE WATCH DEVICE ACQUISITION

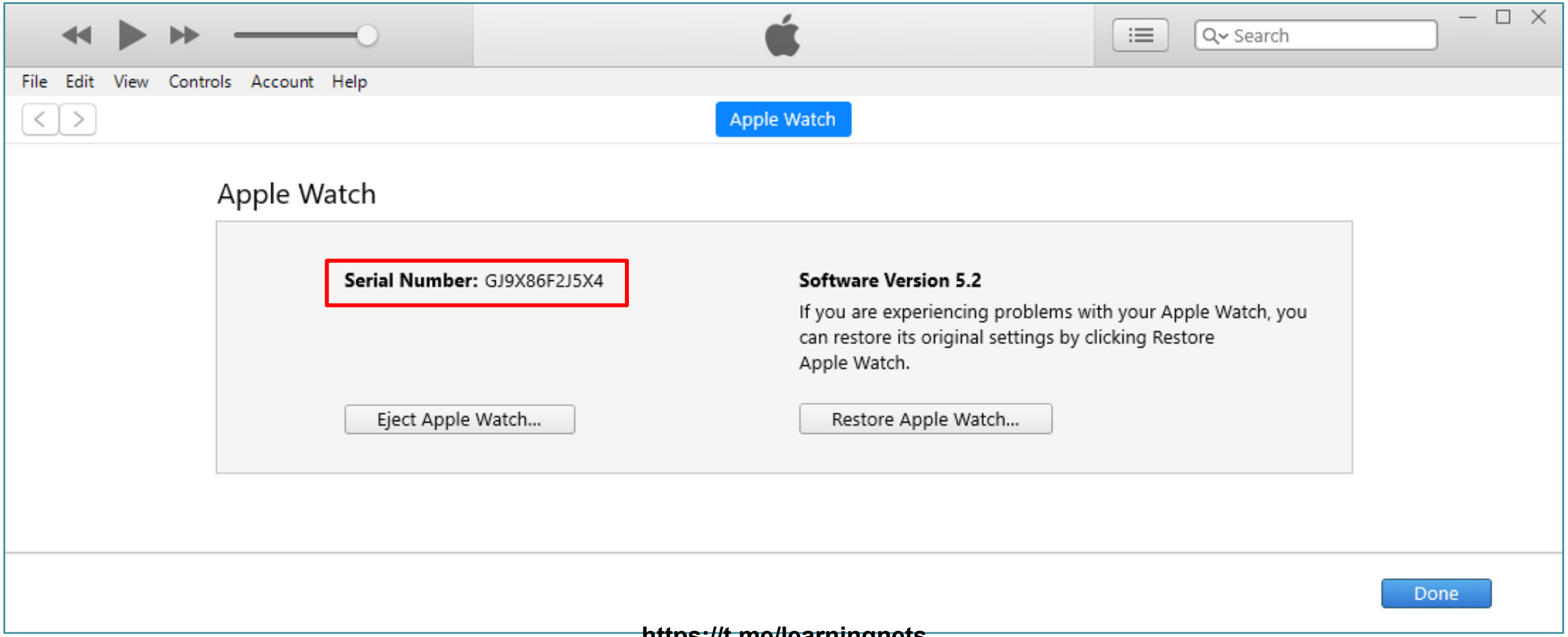
- **No backup service is running on watchOS**
- Possible acquisitions:
  - Device information and list of installed applications
  - AFC protocol (Apple File Conduit)
  - Crash logs (and sysdiagnose!)

- Full file system acquisition **might** be available with a jailbreak
  - **jelbrekTime watchOS 4.1** https://github.com/tihmstar/jelbrekTime
  - **Brenbreak watchOS 4.0 – 5.1.2** https://please.brenbreak.today/

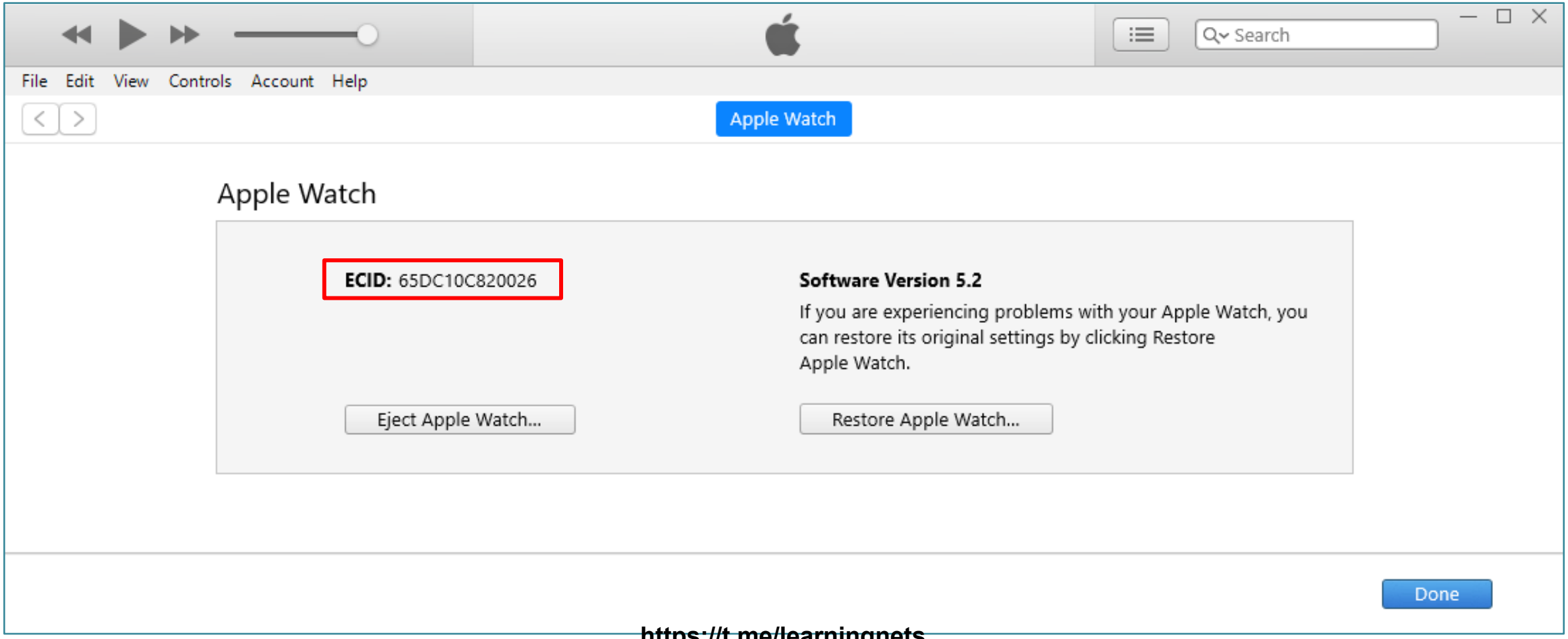
APPLE WATCH
EXTRACTING BASIC DEVICE INFORMATION



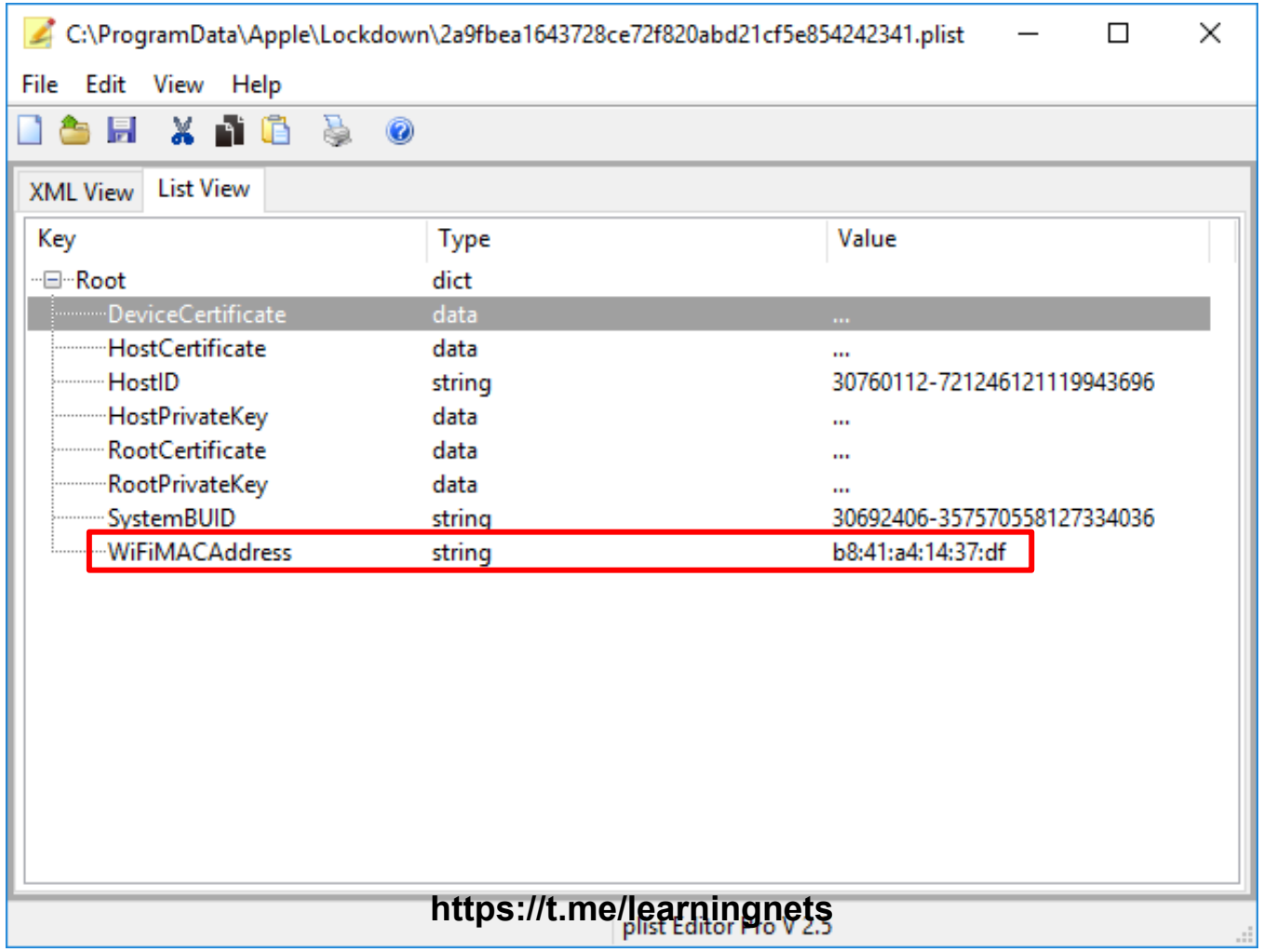
APPLE WATCH
EXTRACTING BASIC DEVICE INFORMATION



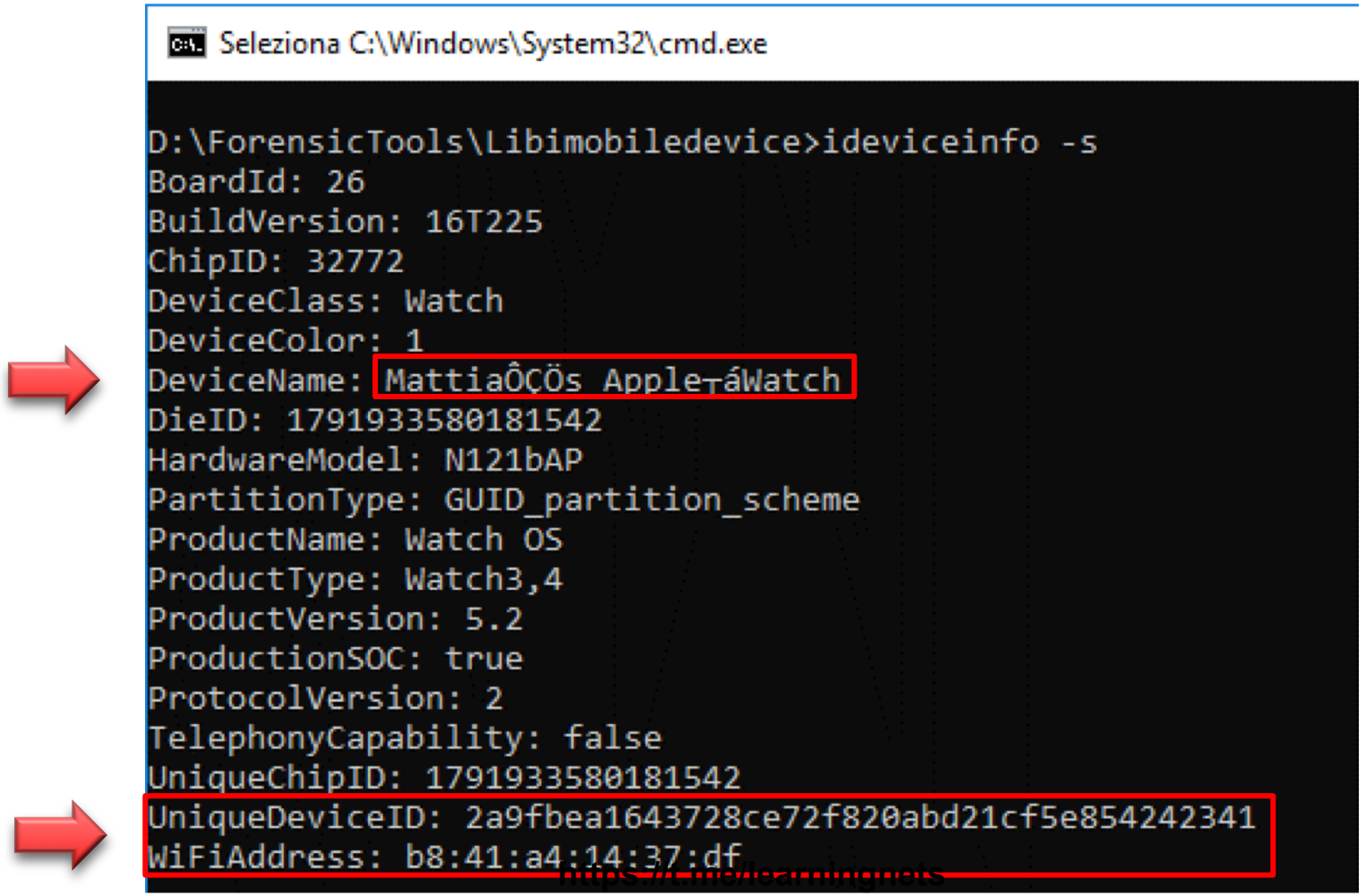
APPLE WATCH
EXTRACTING BASIC DEVICE INFORMATION



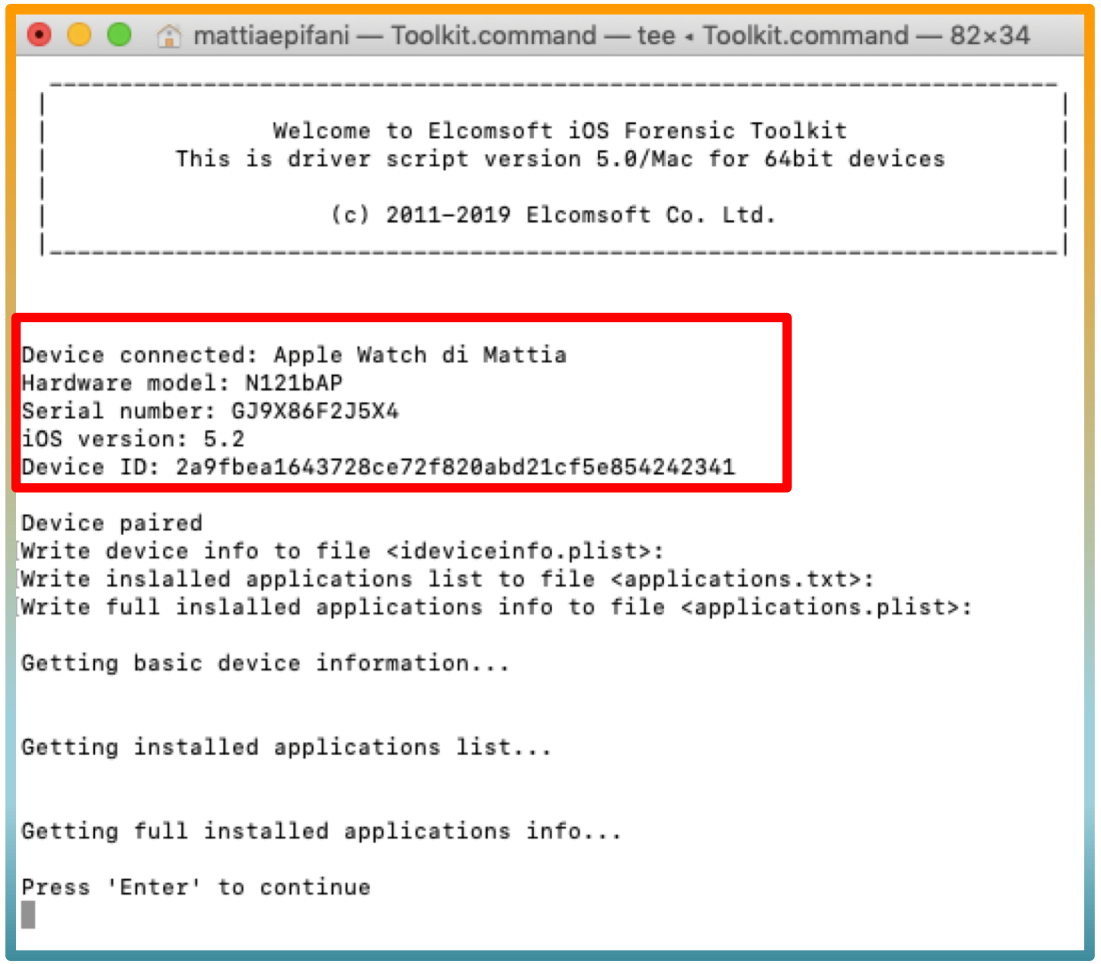
APPLE WATCH
EXTRACTING BASIC DEVICE INFORMATION



APPLE WATCH
EXTRACTING BASIC DEVICE INFORMATION



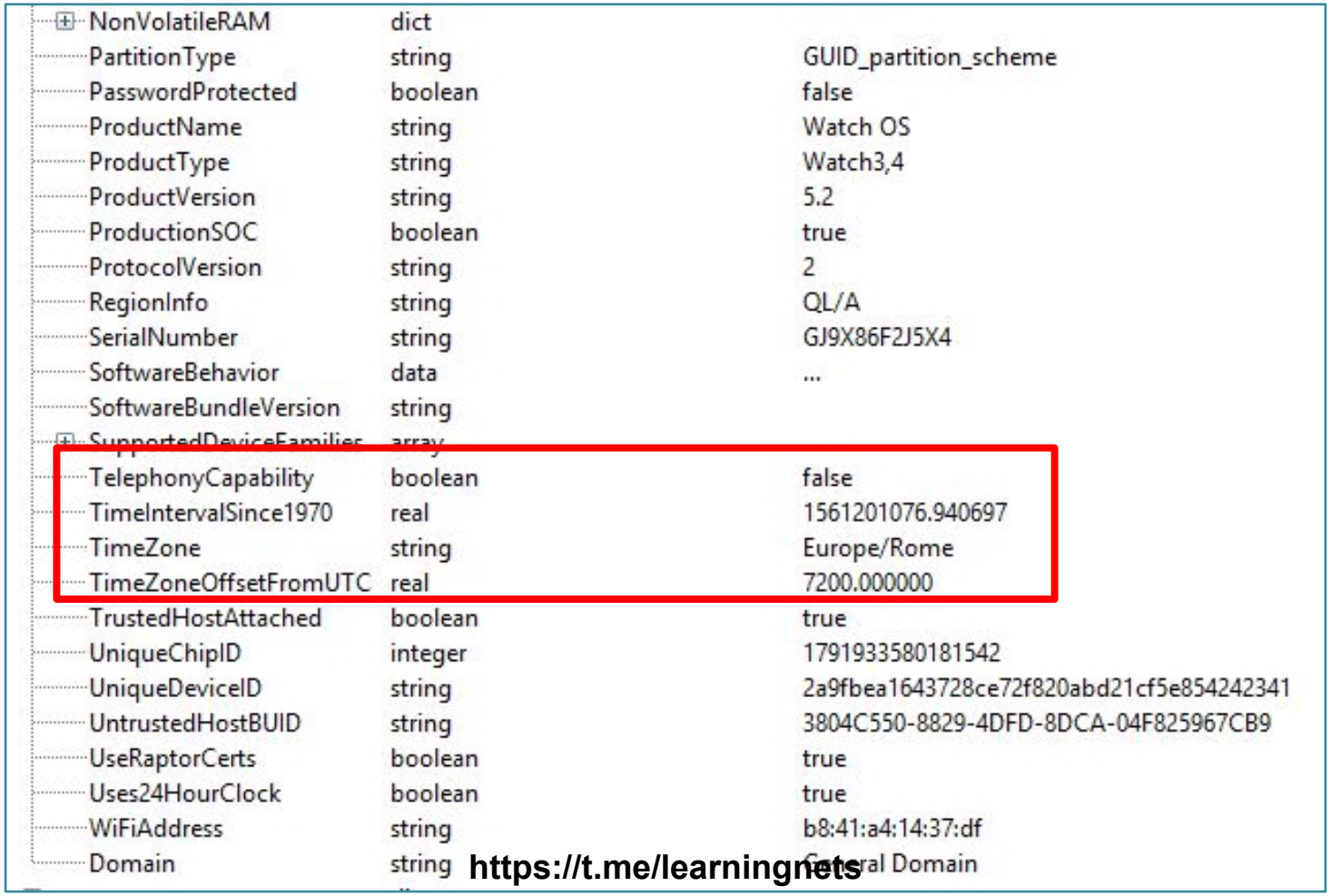
APPLE WATCH
DEVICE INFORMATION (ELCOMSOFT)



APPLE WATCH
DEVICE INFORMATION (ELCOMSOFT)

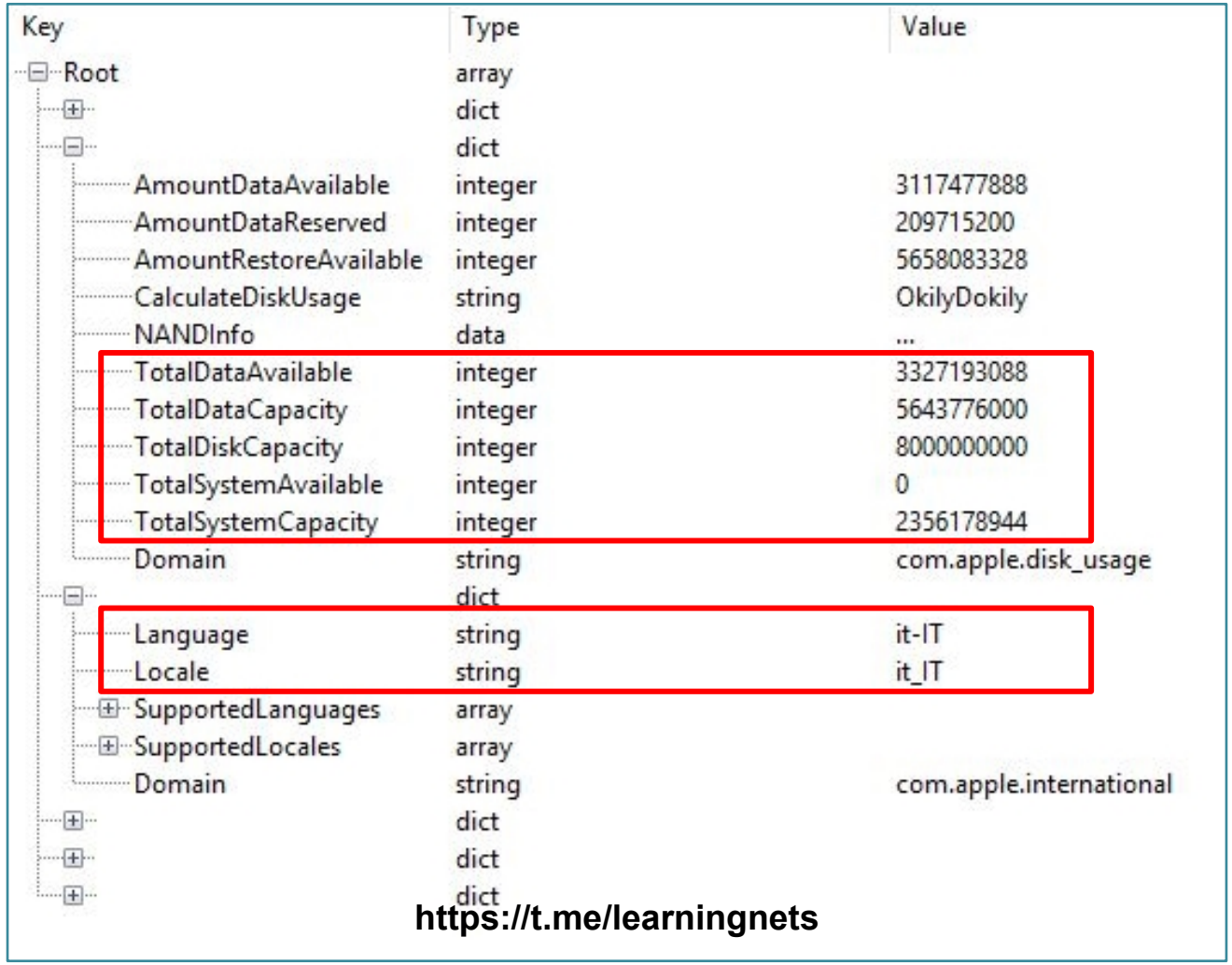
Key	Type	Value
Root	array	
	dict	
ActivationState	string	Activated
BasebandStatus	string	NoTelephonyCapabilty
BluetoothAddress	string	b8:41:a4:12:e6:b7
BoardId	integer	26
BrickState	boolean	false
BuildVersion	string	16T225
CPUArchitecture	string	armv7k
ChipID	integer	32772
DeviceClass	string	Watch
DeviceColor	string	1
DeviceName	string	Apple Watch di Mattia
DieID	integer	1791933580181542
EthernetAddress	string	b8:41:a4:19:16:11
FirmwareVersion	string	iBoot-4513.250.287
HardwareModel	string	N121bAP
HardwarePlatform	string	t8004
HostAttached	boolean	true
MLBSerialNumber	string	GJP829208PSJ0Y34S
ModelNumber	string	MQL12

APPLE WATCH
DEVICE INFORMATION (ELCOMSOFT)



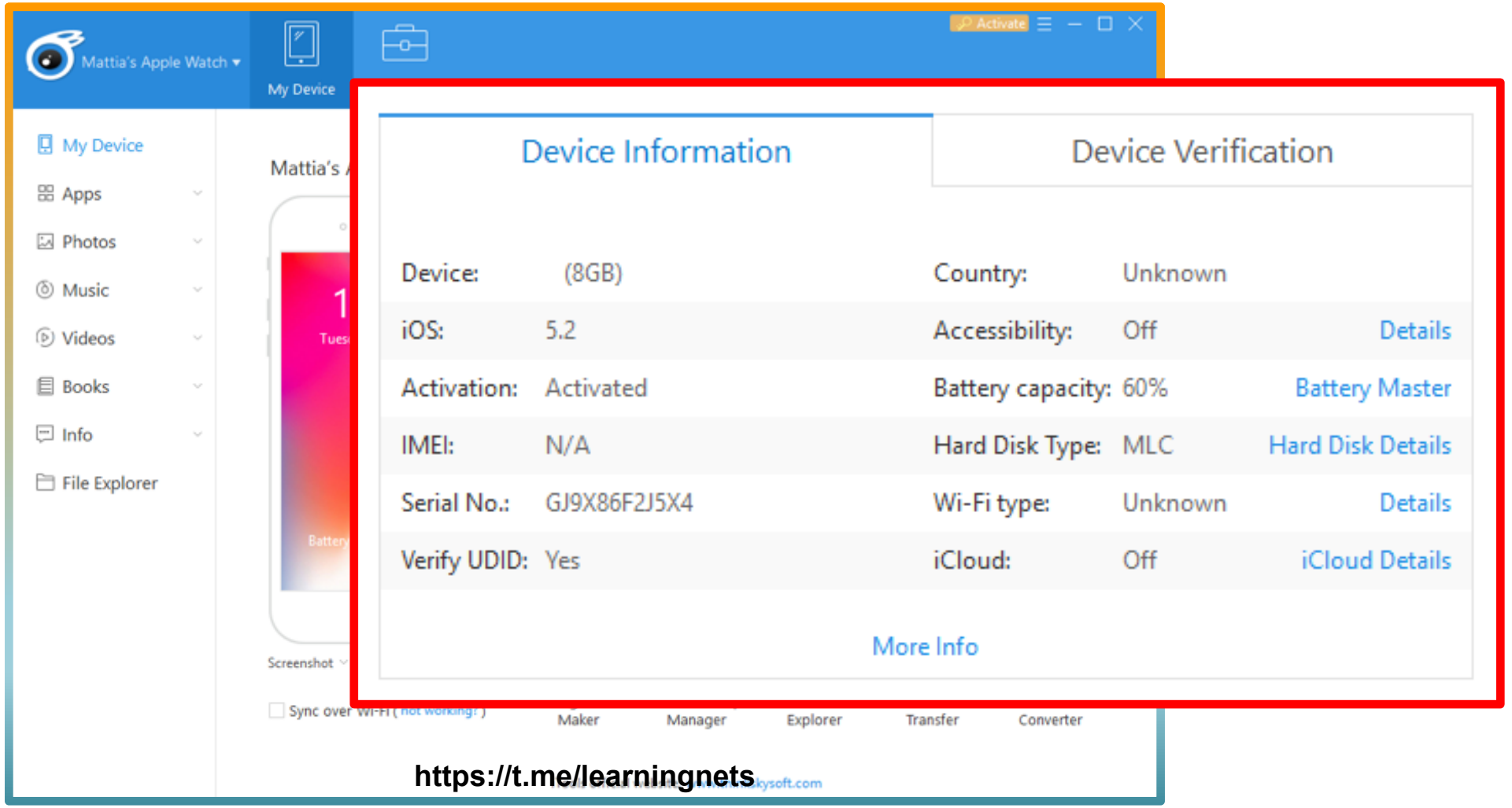
NonVolatileRAM	dict	
PartitionType	string	GUID_partition_scheme
PasswordProtected	boolean	false
ProductName	string	Watch OS
ProductType	string	Watch3,4
ProductVersion	string	5.2
ProductionSOC	boolean	true
ProtocolVersion	string	2
RegionInfo	string	QL/A
SerialNumber	string	GJ9X86F2J5X4
SoftwareBehavior	data	...
SoftwareBundleVersion	string	
SupportedDeviceFamilies	array	
TelephonyCapability	boolean	false
TimeIntervalSince1970	real	1561201076.940697
TimeZone	string	Europe/Rome
TimeZoneOffsetFromUTC	real	7200.000000
TrustedHostAttached	boolean	true
UniqueChipID	integer	1791933580181542
UniqueDeviceID	string	2a9fbea1643728ce72f820abd21cf5e854242341
UntrustedHostBUID	string	3804C550-8829-4DFD-8DCA-04F825967CB9
UseRaptorCerts	boolean	true
Uses24HourClock	boolean	true
WiFiAddress	string	b8:41:a4:14:37:df
Domain	string	General Domain

APPLE WATCH
DEVICE INFORMATION (ELCOMSOFT)

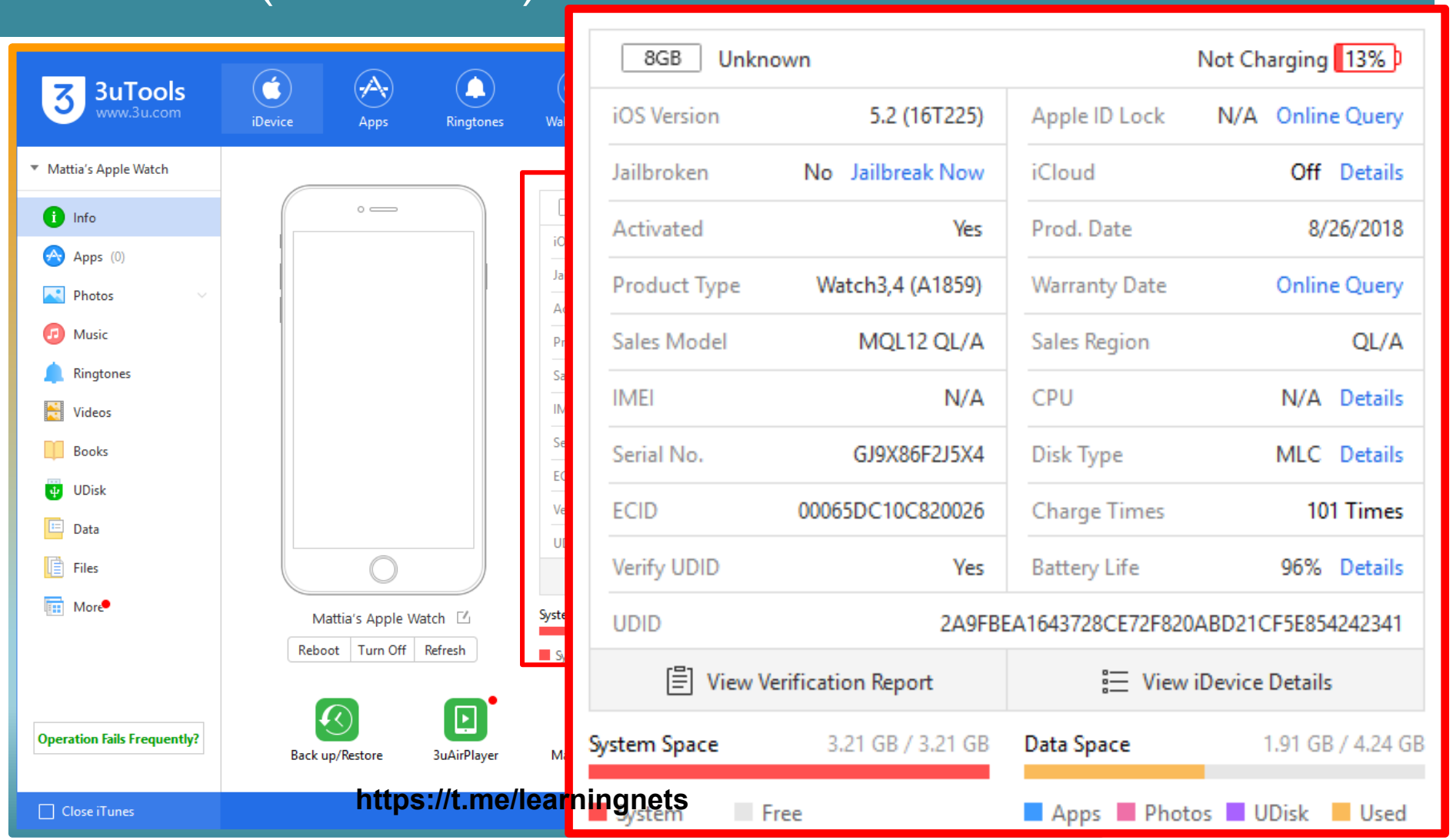


Key	Type	Value
Root	array	
	dict	
	dict	
AmountDataAvailable	integer	3117477888
AmountDataReserved	integer	209715200
AmountRestoreAvailable	integer	5658083328
CalculateDiskUsage	string	OkilyDokily
NANDInfo	data	...
TotalDataAvailable	integer	3327193088
TotalDataCapacity	integer	5643776000
TotalDiskCapacity	integer	8000000000
TotalSystemAvailable	integer	0
TotalSystemCapacity	integer	2356178944
Domain	string	com.apple.disk_usage
	dict	
Language	string	it-IT
Locale	string	it_IT
SupportedLanguages	array	
SupportedLocales	array	
Domain	string	com.apple.international
	dict	
	dict	
	dict	

APPLE WATCH
DEVICE INFORMATION (ITOOLS)



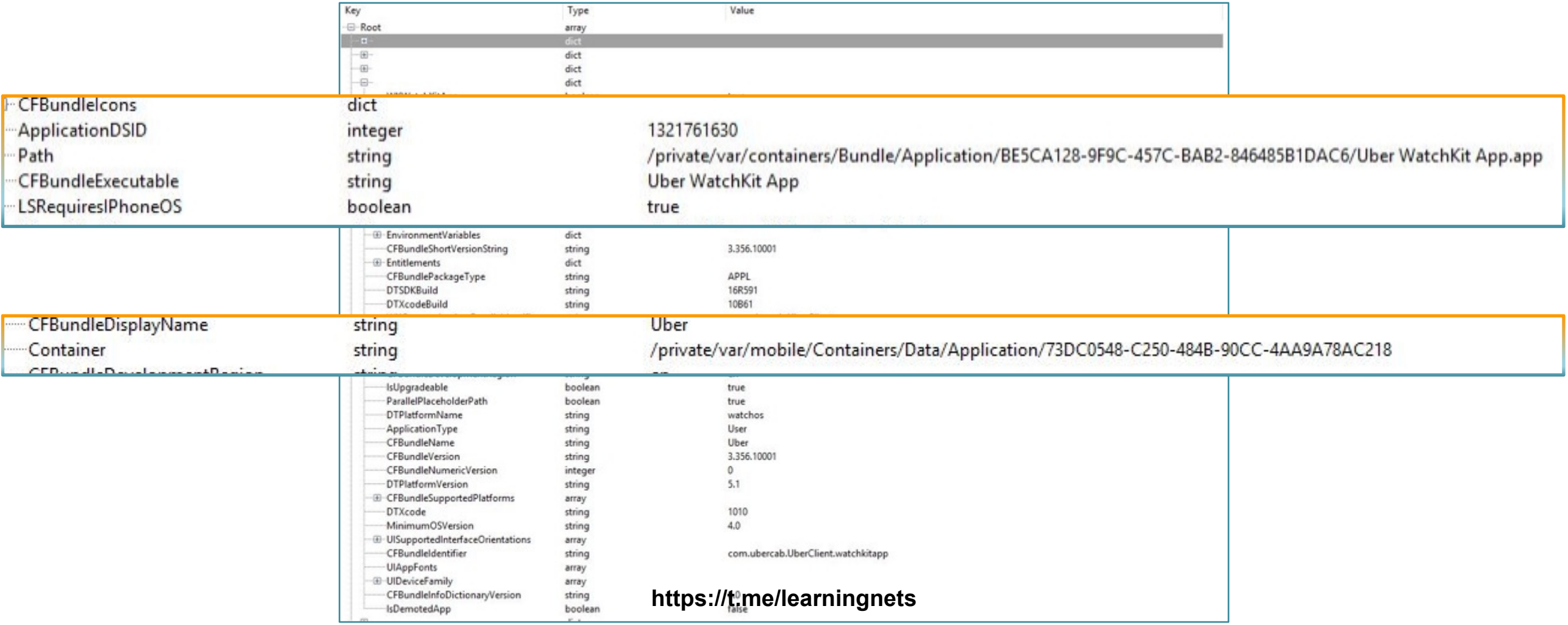
APPLE WATCH
DEVICE INFORMATION (3UTOOLS)



APPLE WATCH
INSTALLED APPLICATIONS (ELCOMSOFT)

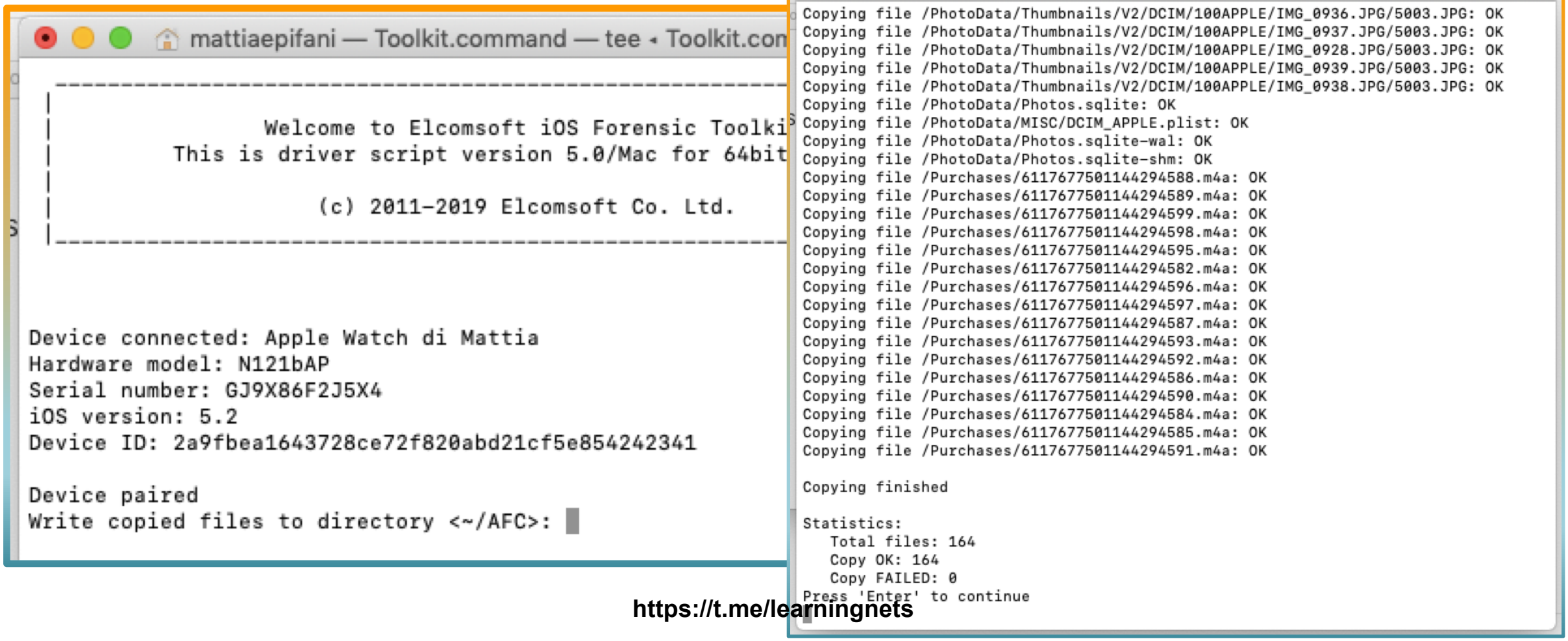
```
CFBundleIdentifier, CFBundleVersion, CFBundleDisplayName
com.melodis.soundhound.free.watchapp, "1", "SoundHound"
com.lufthansa.launcher.watchkitapp, "15084", "Lufthansa"
at.runtastic.gpssportapp.watchapp, "9.5.0.2873", "Runtastic"
com.apple.NanoRadio, "118.1", "Radio"
com.apple.NanoMusic, "880.28", "Musica"
com.apple.NanoMail, "1.0", "Mail"
com.ubercab.UberClient.watchkitapp, "3.356.10001", "Uber"
com.apple.nanonews, "406", "News"
com.viber.watchkitapp, "10.9.1.48", "Viber"
com.apple.NanoCalendar, "1.0", "Calendario"
```

APPLE WATCH INSTALLED APPLICATIONS

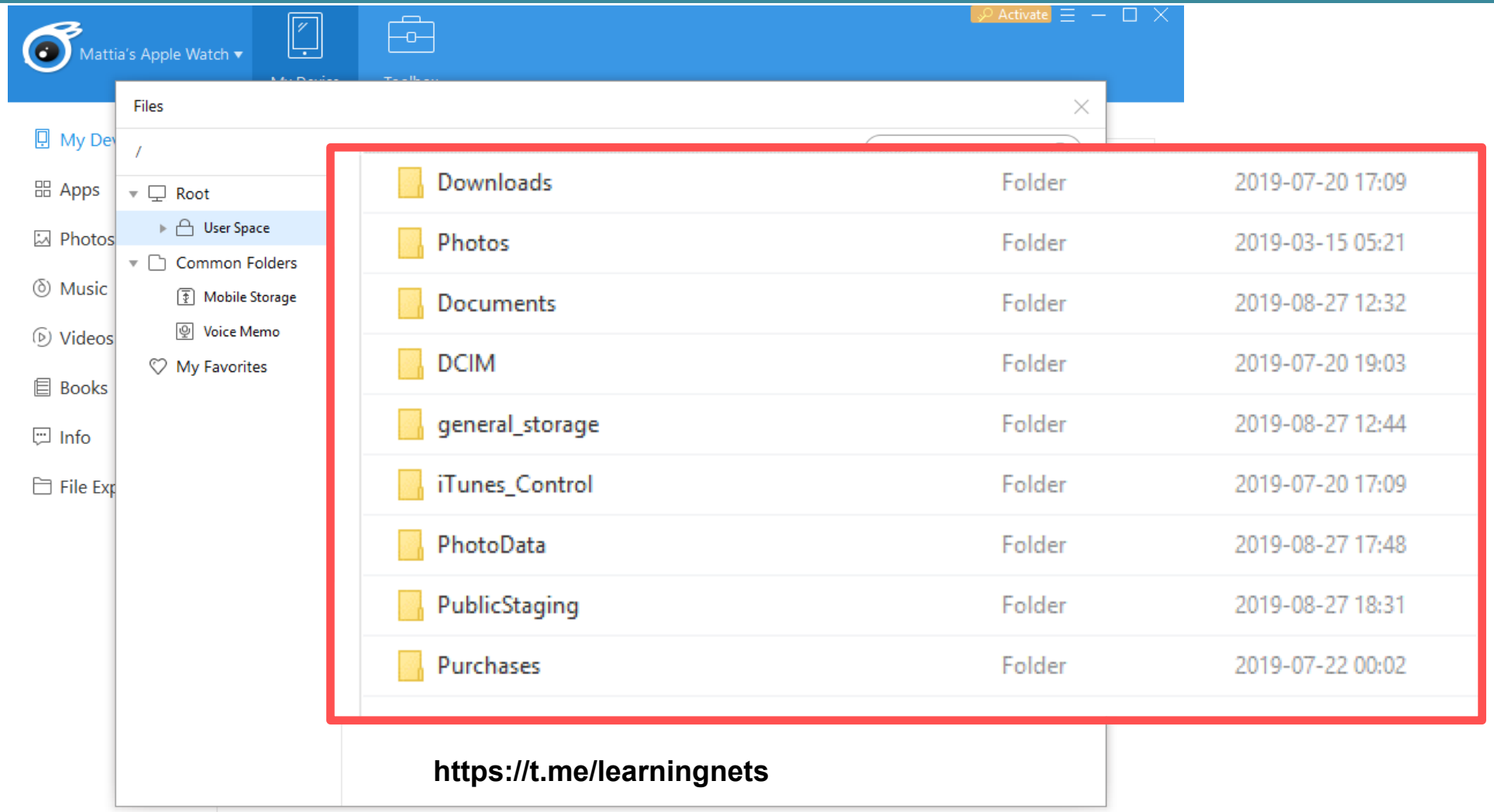


Key	Type	Value
Root	array	
	dict	
	dict	
	dict	
	dict	
CFBundleIcons	dict	
ApplicationDSID	integer	1321761630
Path	string	/private/var/containers/Bundle/Application/BE5CA128-9F9C-457C-BAB2-846485B1DAC6/Uber WatchKit App.app
CFBundleExecutable	string	Uber WatchKit App
LSRequiresIPhoneOS	boolean	true
EnvironmentVariables	dict	
CFBundleShortVersionString	string	3.356.10001
Entitlements	dict	
CFBundlePackageType	string	APPL
DTSDKBuild	string	16R591
DTXcodeBuild	string	10B61
CFBundleDisplayName	string	Uber
Container	string	/private/var/mobile/Containers/Data/Application/73DC0548-C250-484B-90CC-4AA9A78AC218
IsUpgradeable	boolean	true
ParallelPlaceholderPath	boolean	true
DTPlatformName	string	watchos
ApplicationType	string	User
CFBundleName	string	Uber
CFBundleVersion	string	3.356.10001
CFBundleNumericVersion	integer	0
DTPlatformVersion	string	5.1
CFBundleSupportedPlatforms	array	
DTXcode	string	1010
MinimumOSVersion	string	4.0
UISupportedInterfaceOrientations	array	
CFBundleIdentifier	string	com.ubercab.UberClient.watchkitapp
UIAppFonts	array	
UIDeviceFamily	array	
CFBundleInfoDictionaryVersion	string	
IsDemotedApp	boolean	false

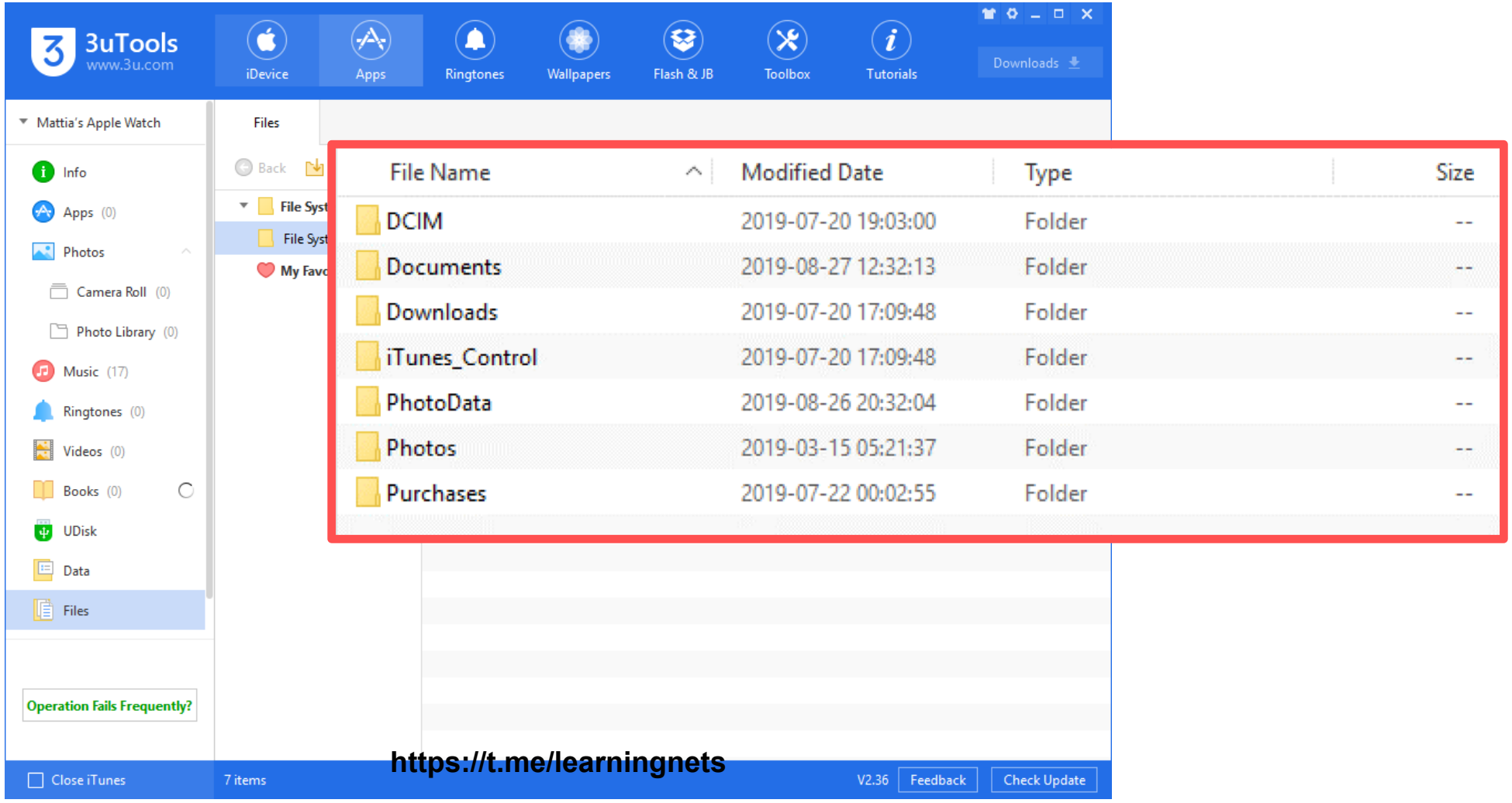
APPLE WATCH
AFC ACQUISITION (ELCOMSOFT)



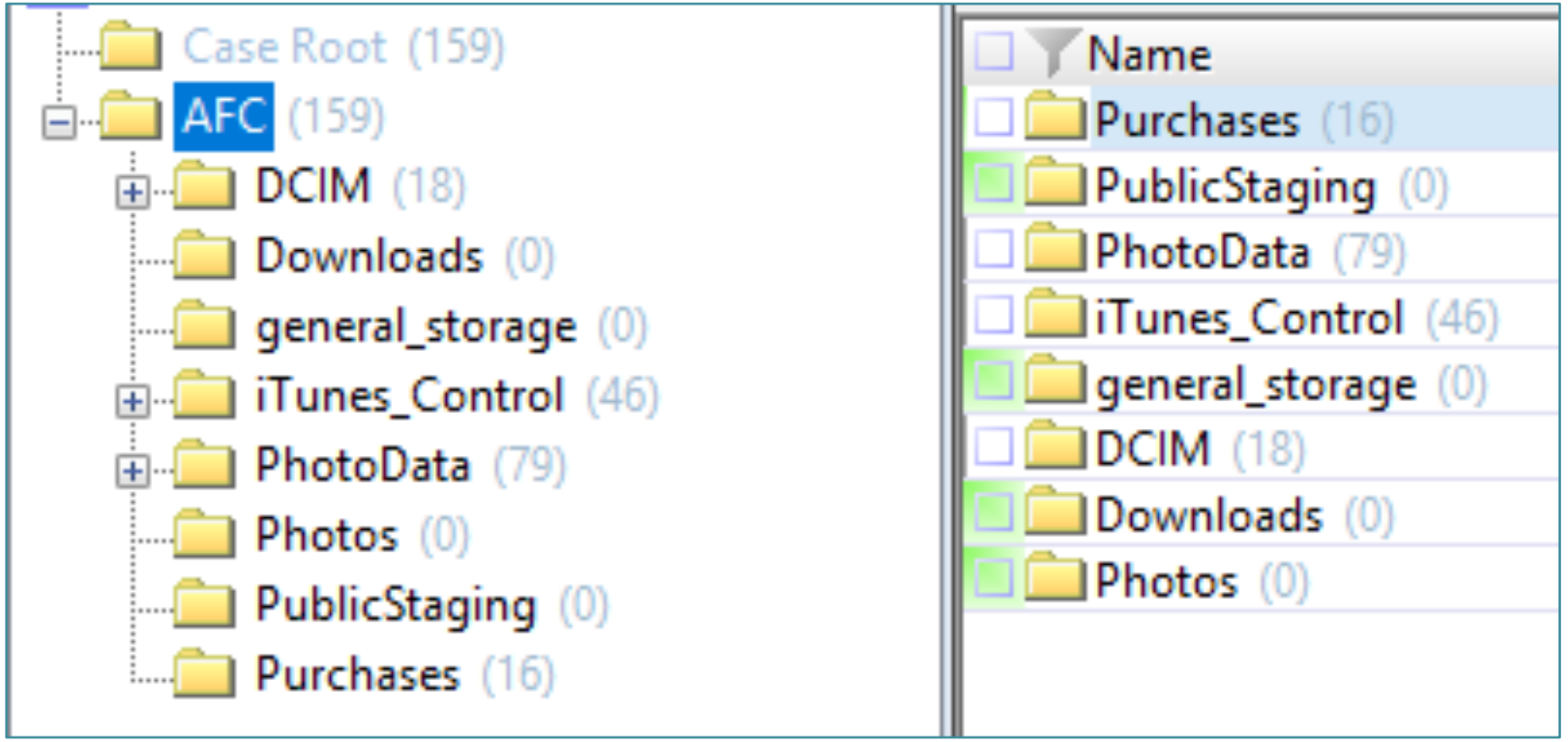
APPLE WATCH
AFC ACQUISITION (ITOOLS)



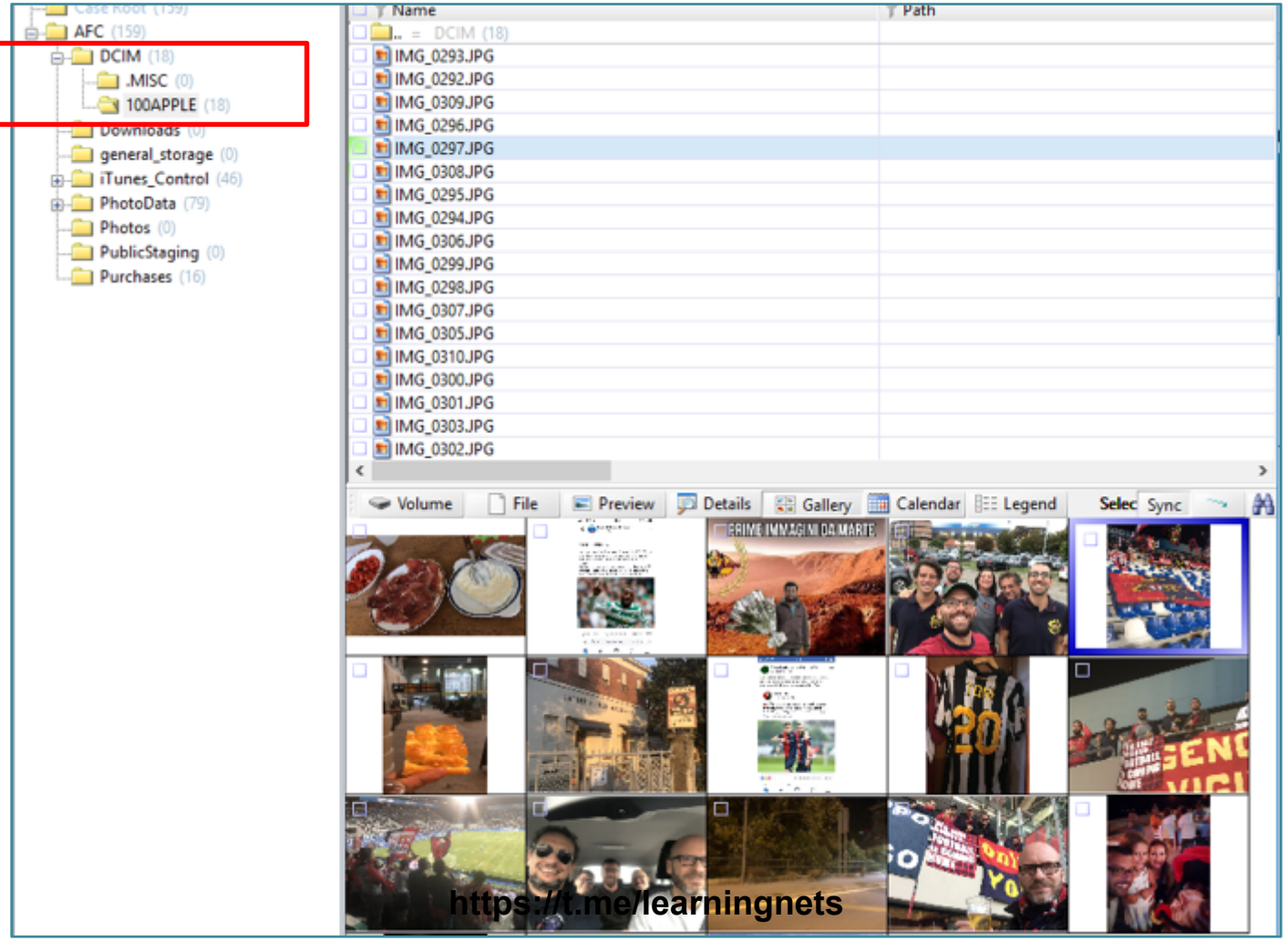
APPLE WATCH
AFC ACQUISITION (3UTOOLS)



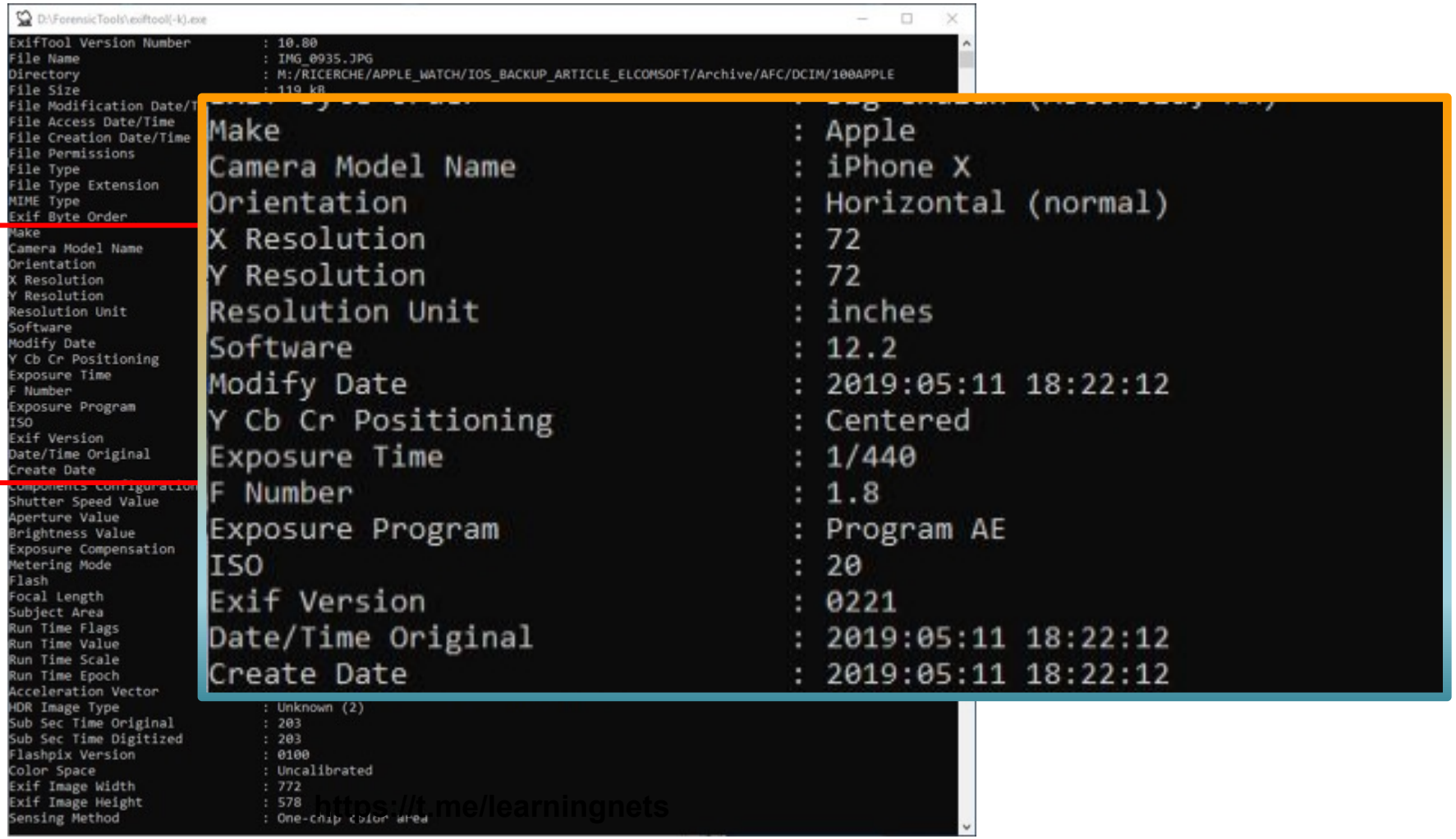
APPLE WATCH
AFC ACQUISITION



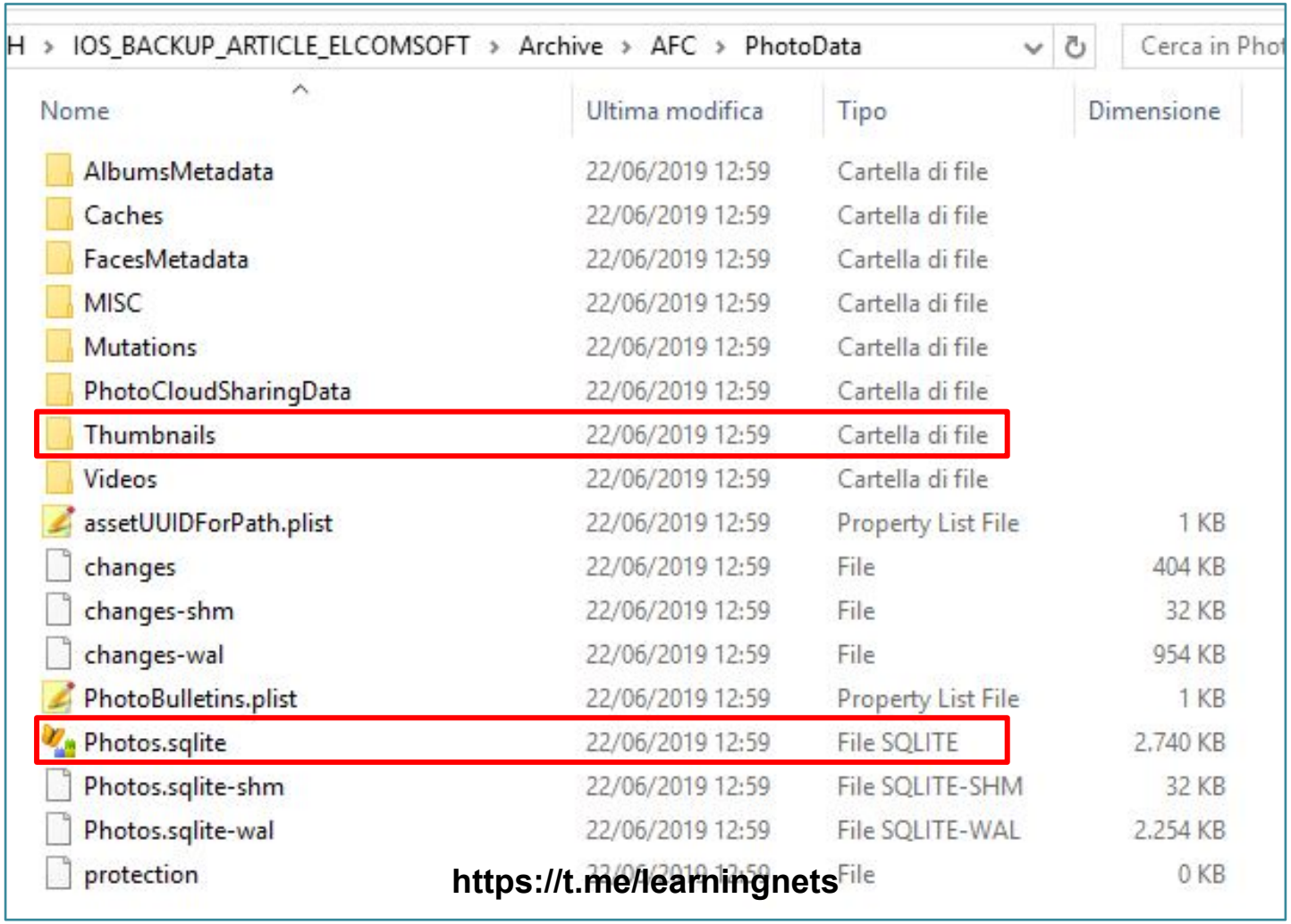
APPLE WATCH **DCIM** FOLDER



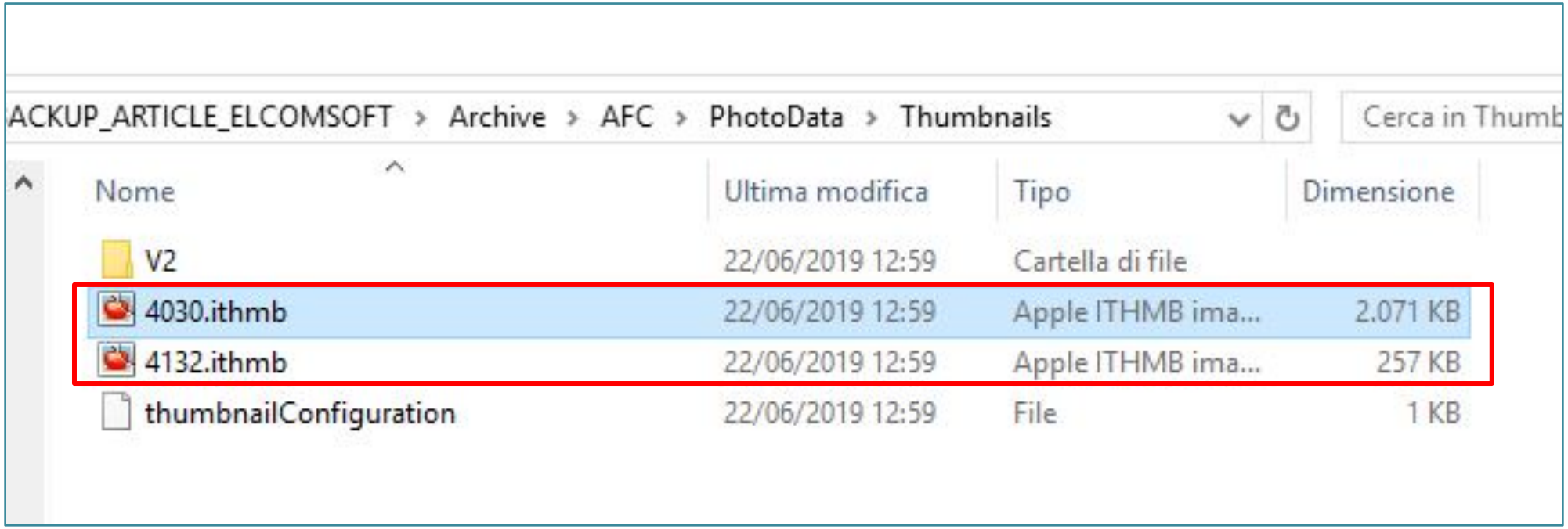
APPLE WATCH **DCIM** FOLDER



APPLE WATCH **PHOTODATA** FOLDER

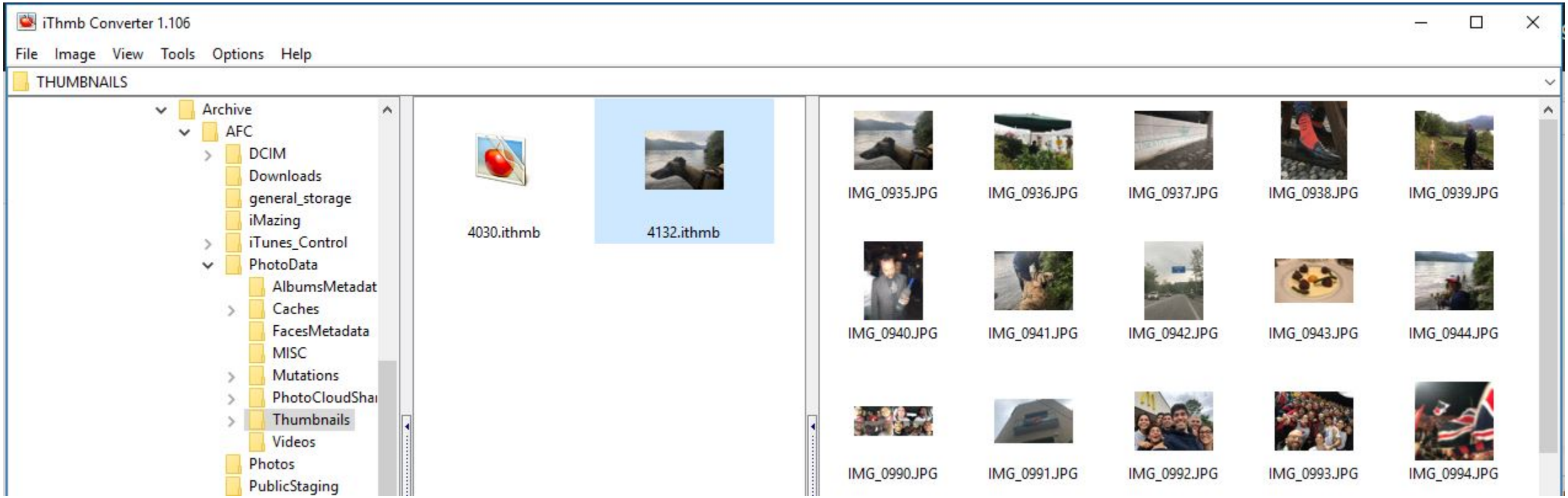


APPLE WATCH **THUMBNAILS** FOLDER

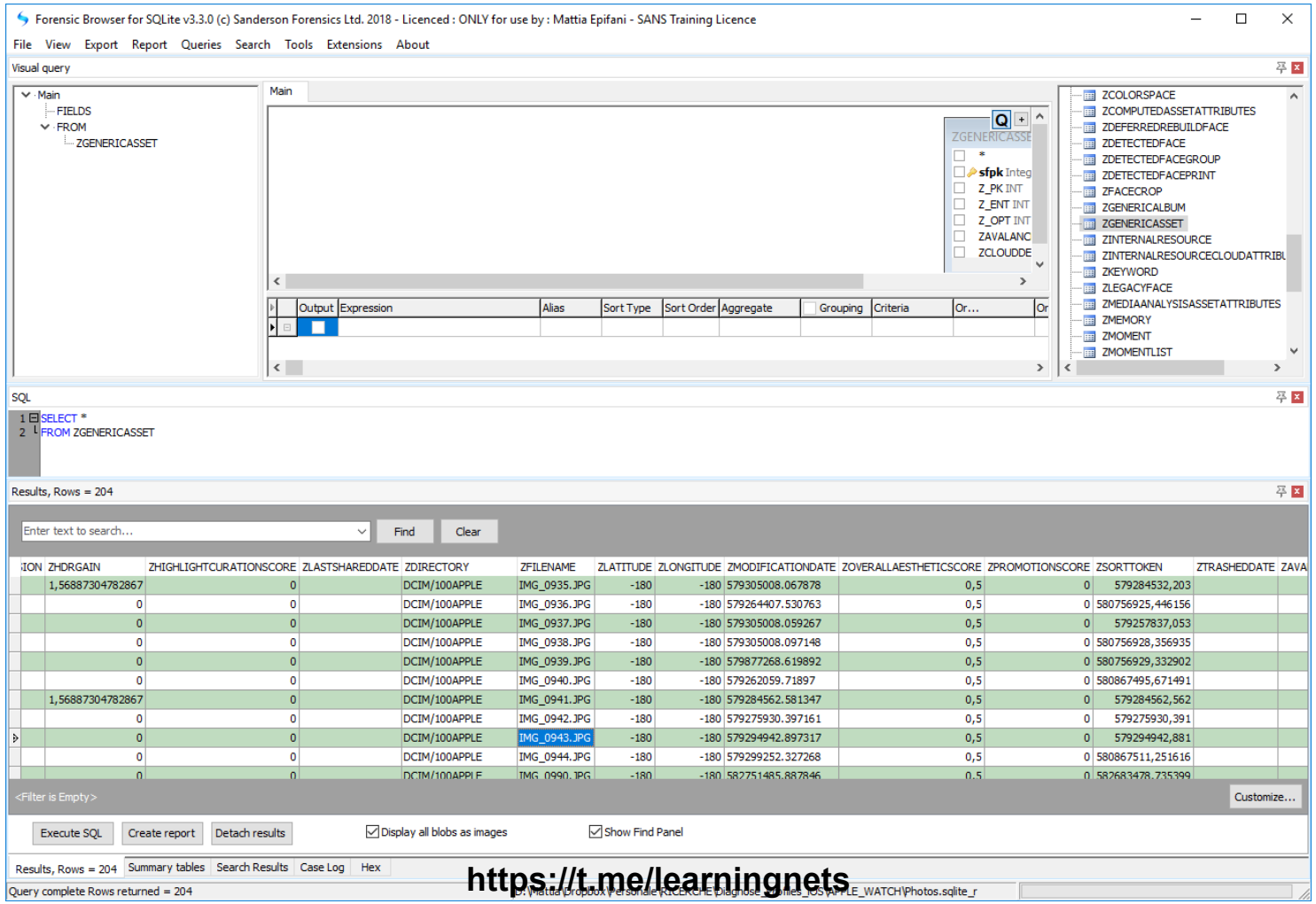


APPLE WATCH THUMBNAILS

HTTP://WWW.ITHMBCONVERTER.COM/



APPLE WATCH
PHOTOS.SQLITE



APPLE WATCH PHOTOS

SQL

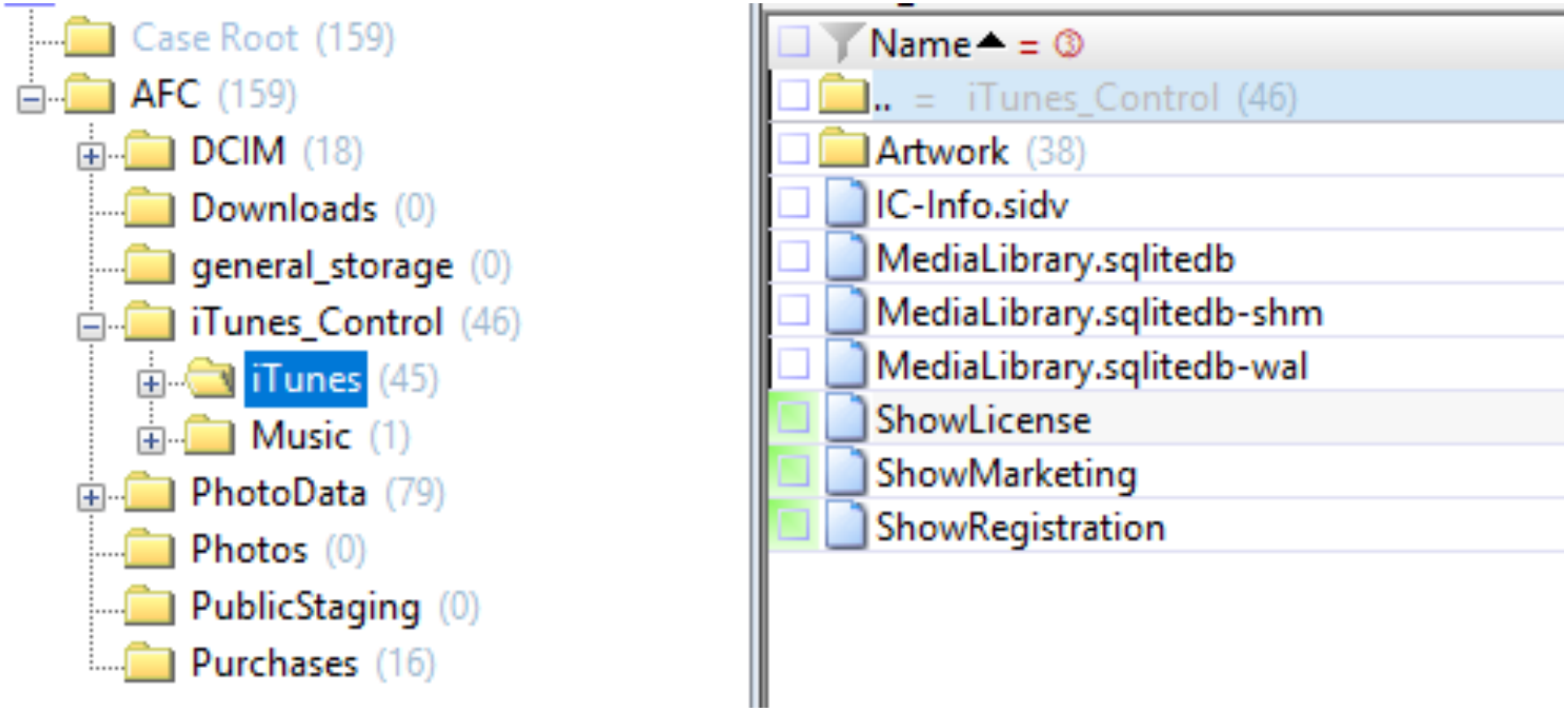
```
SELECT ZGENERICASSET.ZHEIGHT,
  ZGENERICASSET.ZWIDTH,
  ZGENERICASSET.ZLATITUDE,
  ZGENERICASSET.ZLONGITUDE,
  ZGENERICASSET.ZADDEDDATE,
  StrfTime('%Y-%m-%d %H:%M', DateTime(ZGENERICASSET.ZADDEDDATE + 978307200, 'unixepoch')) AS ZADDEDDATE_TIME,
  ZGENERICASSET.ZDATECREATED,
  StrfTime('%Y-%m-%d %H:%M', DateTime(ZGENERICASSET.ZDATECREATED + 978307200, 'unixepoch')) AS ZDATECREATED_TIME,
  ZGENERICASSET.ZDIRECTORY,
  ZGENERICASSET.ZFILENAME
FROM ZGENERICASSET
```

Results, Rows = 204

Find Clear

ZHEIGHT	ZWIDTH	ZLATITUDE	ZLONGITUDE	ZADDEDDATE	ZADDEDDATE_TIME	ZDATECREATED	ZDATECREATED_TIME	ZDIRECTORY	ZFILENAME
578	772	-180	-180	580756925.624067	2019-05-28 17:22	579284531.743759	2019-05-11 16:22	DCIM/100APPLE	IMG_0935.JPG
576	768	-180	-180	580756927.202916	2019-05-28 17:22	579264405	2019-05-11 10:46	DCIM/100APPLE	IMG_0936.JPG
659	539	-180	-180	580756929.374728	2019-05-28 17:22	579291771	2019-05-11 18:22	DCIM/100APPLE	IMG_0938.JPG
768	1024	-180	-180	580756931.03498	2019-05-28 17:22	579299334	2019-05-11 20:28	DCIM/100APPLE	IMG_0939.JPG
768	576	-180	-180	580867500.753969	2019-05-30 00:05	579262057	2019-05-11 10:07	DCIM/100APPLE	IMG_0940.JPG
578	772	-180	-180	580867504.723383	2019-05-30 00:05	579284562.001772	2019-05-11 16:22	DCIM/100APPLE	IMG_0941.JPG
772	578	-180	-180	580867509.880612	2019-05-30 00:05	579275930.021091	2019-05-11 13:58	DCIM/100APPLE	IMG_0942.JPG
432	768	-180	-180	580867511.201795	2019-05-30 00:05	579294942.939468	2019-05-11 19:15	DCIM/100APPLE	IMG_0943.JPG
576	768	-180	-180	580867520.591774	2019-05-30 00:05	579299247	2019-05-11 20:27	DCIM/100APPLE	IMG_0944.JPG
315	851	-180	-180	582683501.965043	2019-06-20 00:31	580574515	2019-05-26 14:41	DCIM/100APPLE	IMG_0990.JPG
432	768	-180	-180	582683529.792296	2019-06-20 00:32	580561165.605631	2019-05-26 10:59	DCIM/100APPLE	IMG_0991.JPG
577	768	-180	-180	582683593.098039	2019-06-20 00:33	580580073	2019-05-26 16:14	DCIM/100APPLE	IMG_0992.JPG
577	768	-180	-180	582683679.232333	2019-06-20 00:34	580596123	2019-05-26 20:42	DCIM/100APPLE	IMG_0993.JPG
768	768	-180	-180	582683765.0			2019-05-26 23:22	DCIM/100APPLE	IMG_0994.JPG

APPLE WATCH
ITUNES_CONTROL/ITUNES FOLDER



APPLE WATCH
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
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
MEDIALIBRARY.SQLITEDB

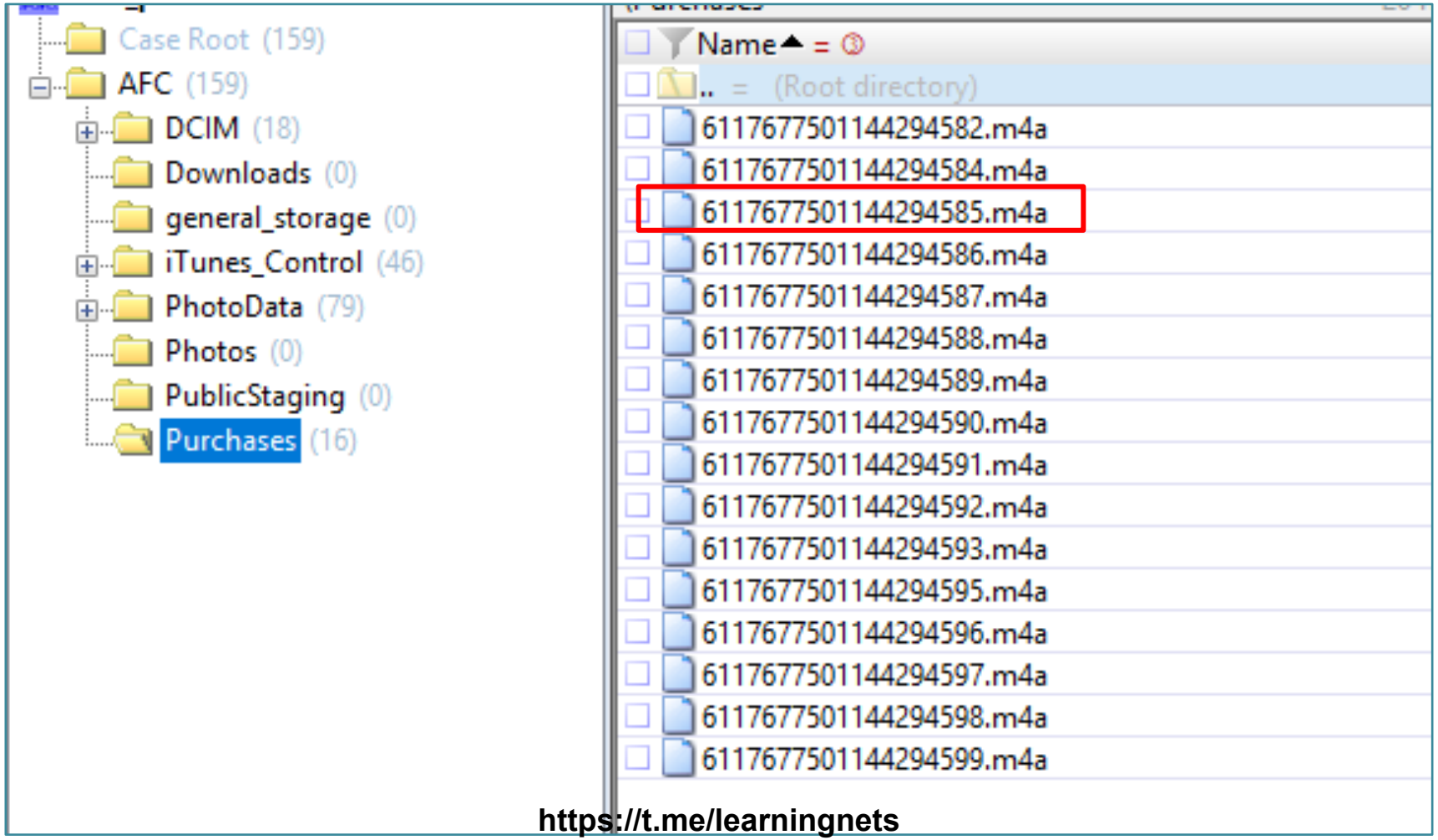
Execute SQL | Stop Query

RecNo	Title	Media Type	File format	File	Total time (ms)	File size	Year	Account ID	date_purchased	Purchase History ID
	Click here to define a filter									
18	Hai bucato la mia vita	33	m4v		60120	14451198	2012	1321761630	04/01/2012 02:28:06	230000997371841
19	IMPARARE l'INGLESE PARLANDO! + AUDIOLIBRO	0	.epub		0	1395085	2014	1321761630	11/08/2016 10:41:06	360017803710048
20	Il Benefattore	0	.epub		0	113973	2010	1321761630	05/12/2010 22:30:40	160001415351721
21	Il Kamasutra in 200 posizioni	0	.epub		0	9806818	2012	1321761630	11/08/2016 10:40:45	360017803703687
22	Il mercante di libri maledetti	0	.epub		0	1519764	2011	1321761630	30/12/2012 12:03:08	360000409803826
23	Iris (Hold Me Close)	1	m4a		319457	11149865	2014	1321761630	08/09/2014 13:17:02	4611686019343182093
24	Iris (Hold Me Close)	1	m4a		319457	11149865	2014	1321761630	08/09/2014 13:17:02	4611686019343182093
25	La Divina Commedia di Dante: Inferno	0	.epub		0	112979	2010	1321761630	14/06/2011 20:32:53	160002386875969
26	La Divina Commedia di Dante: Paradiso	0	.epub		0	115029	2010	1321761630	14/06/2011 20:33:26	160002386878477
27	La Divina Commedia di Dante: Purgatorio	0	.epub		0	113731	2010	1321761630	14/06/2011 20:34:42	160002386883534
28	Prisencolinensinainciusol (Remix)	1	m4a	6117677501144294585.m4a	320027	11034161	2012	1321761630	04/01/2012 02:28:06	230000997371840
29	Prisencolinensinainciusol (Remix)	1	m4a	6117677501144294585.m4a	320027	11034161	2012	1321761630	04/01/2012 02:28:06	230000997371840
30	Raised By Wolves	1	m4a		245599	8636426	2014	1321761630	08/09/2014 13:17:02	4611686019343182098

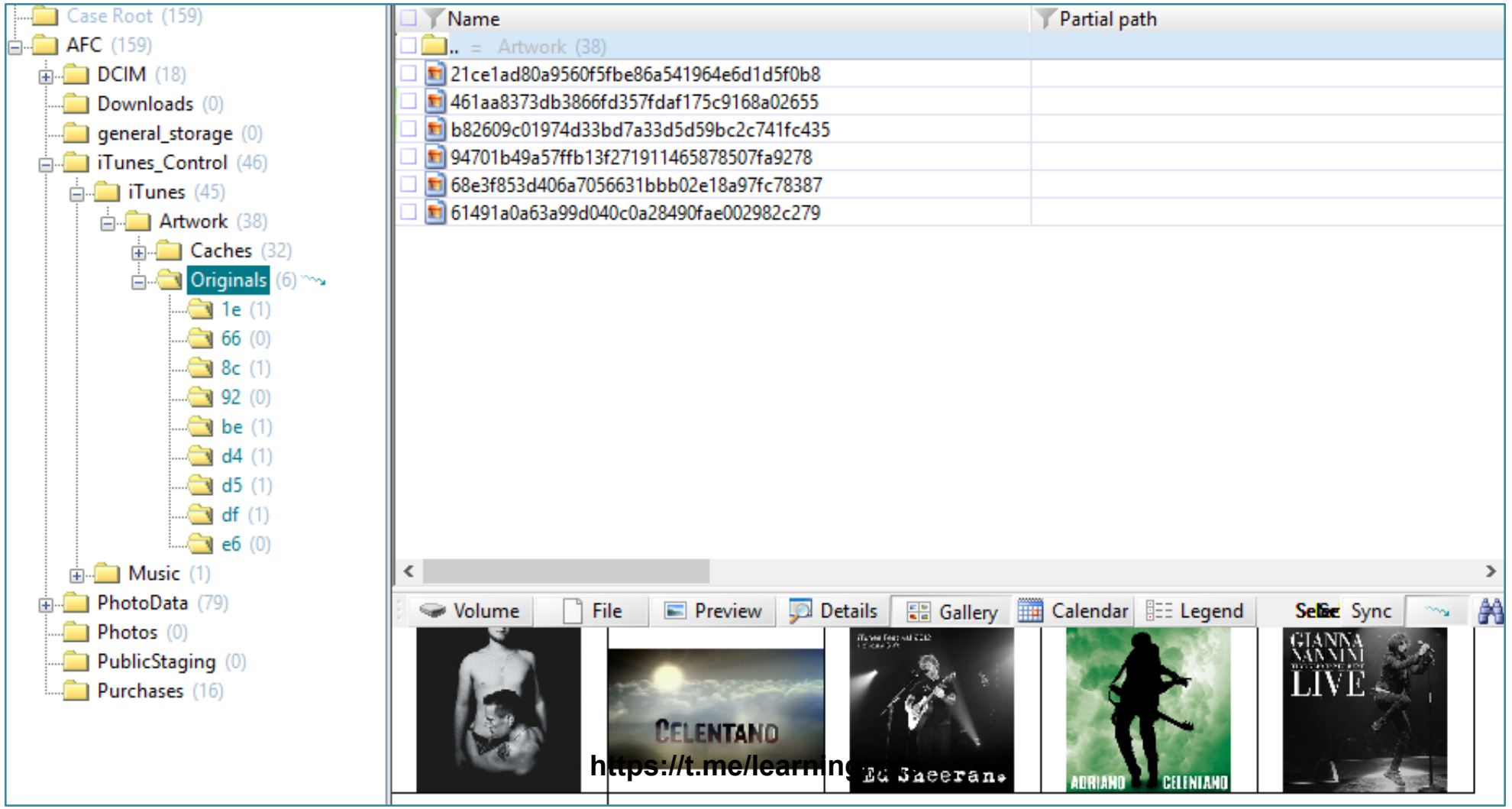
APPLE WATCH
MEDIALIBRARY.SQLITEDB

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

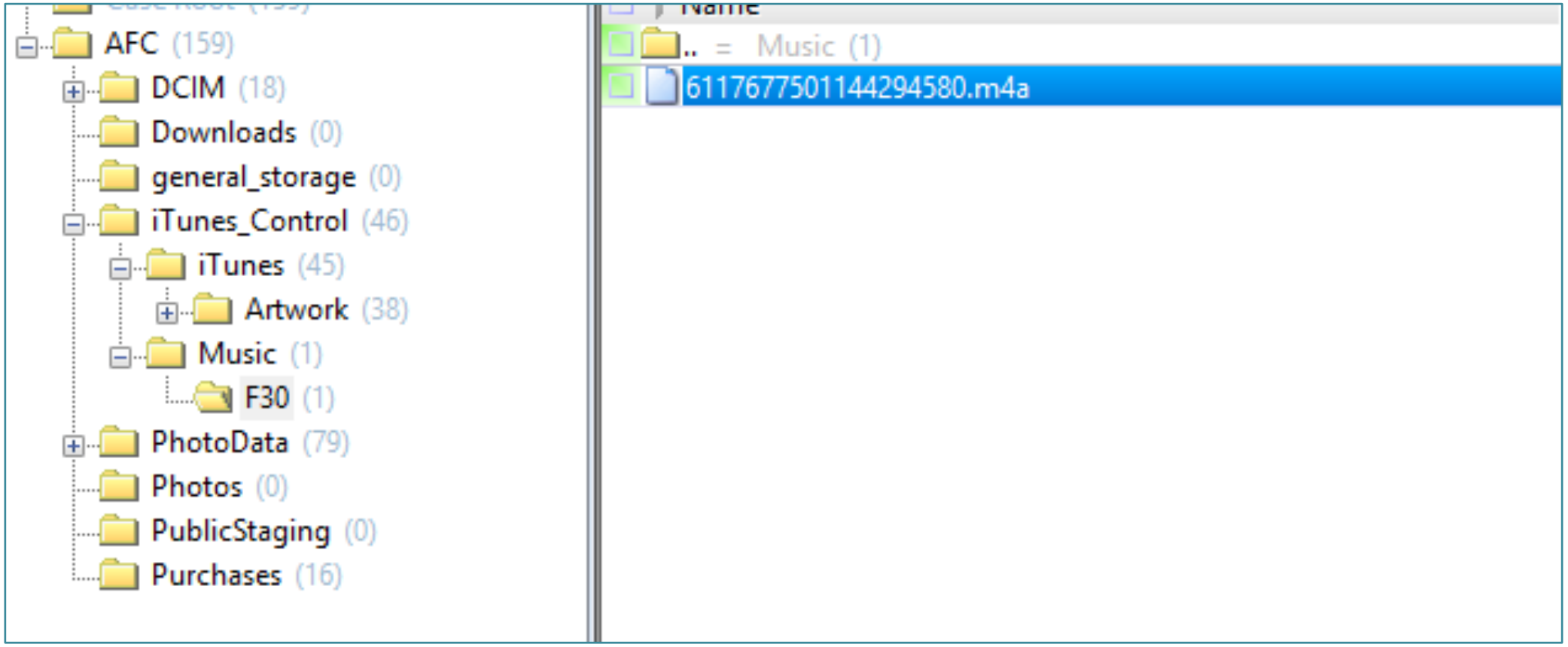
APPLE WATCH **PURCHASES** FOLDER



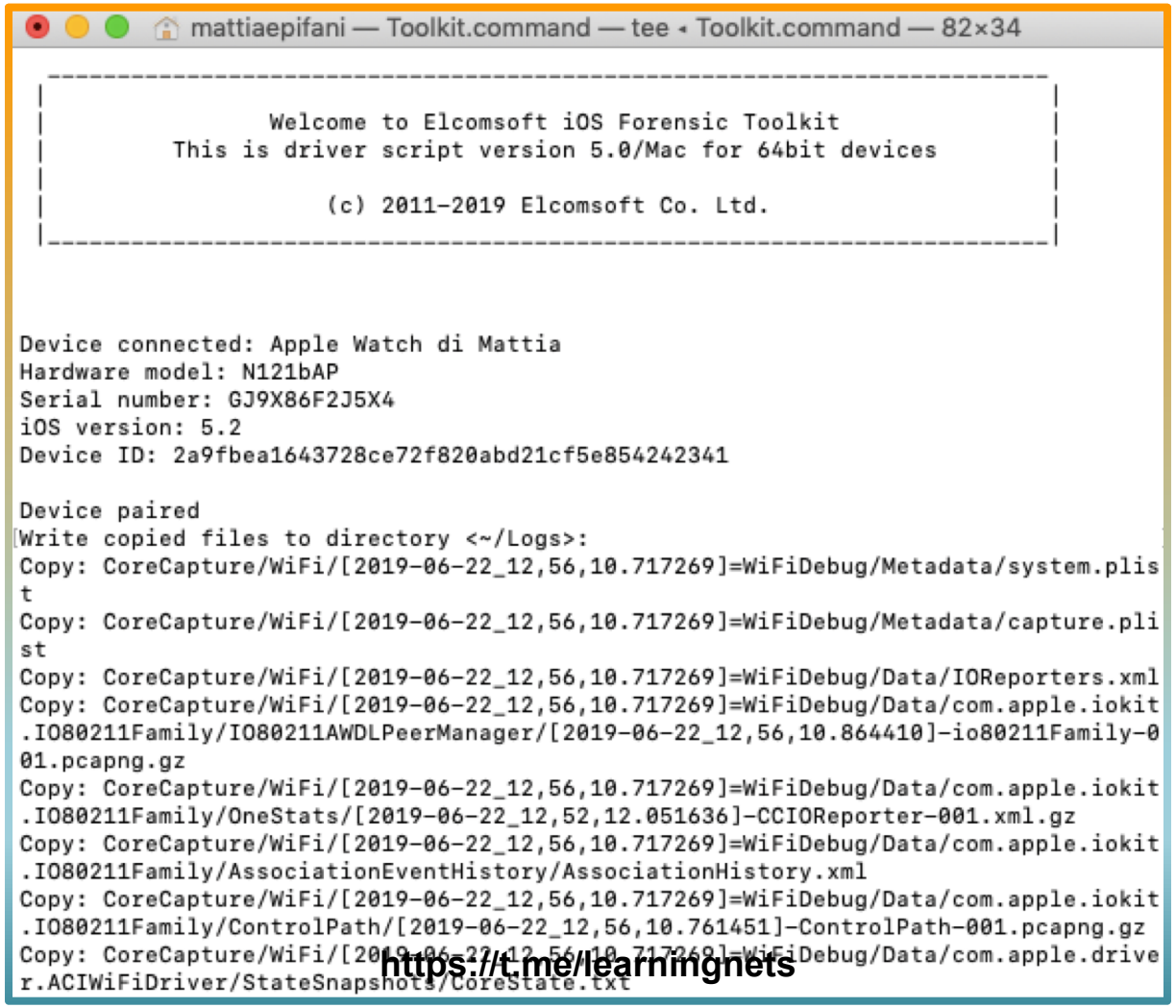
APPLE WATCH
ITUNES_CONTROL/ITUNES/ARTWORK/ORIGINALS



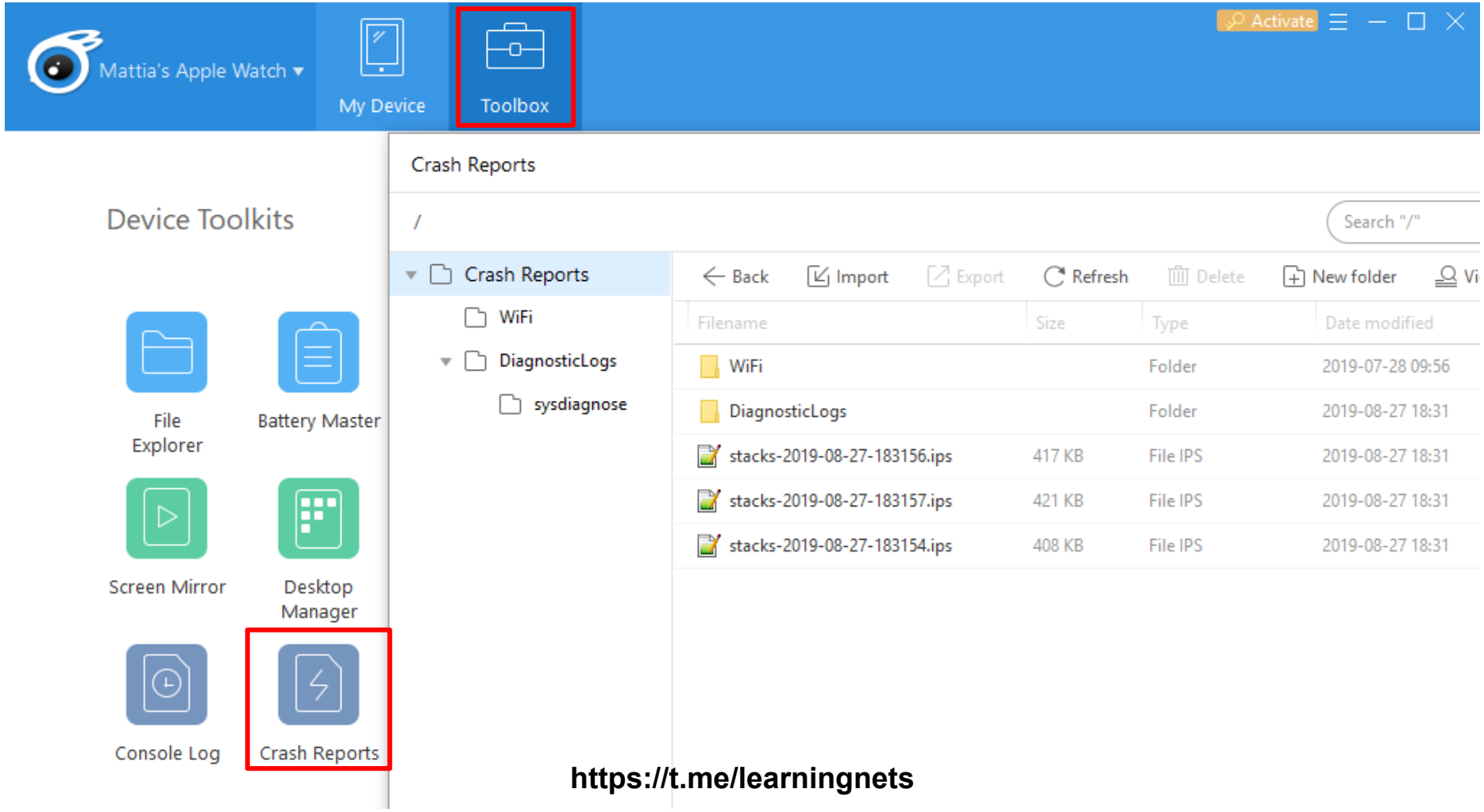
APPLE WATCH
ITUNES_CONTROL/MUSIC



APPLE WATCH
LOGS ACQUISITION (ELCOMSOFT)



APPLE WATCH LOGS ACQUISITION (ITOOLS)



APPLE WATCH SYSDIAGNOSE

- Apple provides "*a web-based tool that developers can use to report issues with Apple software and services, request enhancement to APIs and tools and track the status of their feedback*"

- To correctly use this tool and submit Apple relevant information to identify the issue, it is mandatory to "**Collect and attach any relevant logs**"

APPLE WATCH SYSDIAGNOSE

- The Apple web page "**Profiles and Logs**" contains instructions about how to extract logs from different Apple operating systems, including Mac OS X, iOS, tvOS and WatchOS
- Some logs (e.g. Crash Logs) are **generated automatically** by the operating system during its execution while others (e.g. sysdiagnose) **can be generated with specific user actions**
- Moreover, some logs **require the installation of a profile on the device** (e.g. Disk Space Diagnostics and Battery Life)

APPLE WATCH
USING APPLE "BUG REPORTING" FOR FORENSIC PURPOSES

- Mattia Epifani, Heather Mahalik and @Cheeky4n6monkey have written a document describing their initial research into these logs
- This document is freely available from

https://www.for585.com/sysdiagnose

- We also developed various scripts to parse some of the files available during sysdiagnose acquisition.
- These scripts are available from GitHub

https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts

APPLE WATCH
SYSDIAGNOSE ON WATCHOS

HTTPS://DOWNLOAD.DEVELOPER.APPLE.COM/IOS/WATCHOS_LOGS/SYSDIAGNOSE_LOGGING_INSTRUCTIONS.PDF

Sysdiagnose Logs: Apple Watch

For general watchOS issues, please gather a sysdiagnose.

Enabling Logging

1. Download the watchOS logging profile to the paired iPhone.
   If necessary, email the profile or use AirDrop
2. Tap the profile in the body of the email.
3. Choose 'Apple Watch' when prompted.
4. Tap Install (enter passcode, if prompted), agr
5. Reproduce the issue.
6. Trigger a sysdiagnose by pressing and holdin
   for two seconds and release.

Gathering Logging

1. Place the Apple Watch on the charging puck.
2. Make sure the iPhone is within range of the watch.
3. Wait for up to 15 minutes for the Apple Watch to sync the files to the iPhone.
4. Plug the iPhone into your host computer.
5. Launch iTunes.
6. Sync your iPhone with iTunes.
7. Copy all available logs as described below.

Log Locations

macOS:

```
~/Library/Logs/CrashReporter/MobileDevice/[Your_iOS_Device_Name]/DiagnosticLogs/sysdiagnose/
co-sysdiagnose_YEAR.MONTH.DAY_HH-MM-SS-xxxx.tar
```

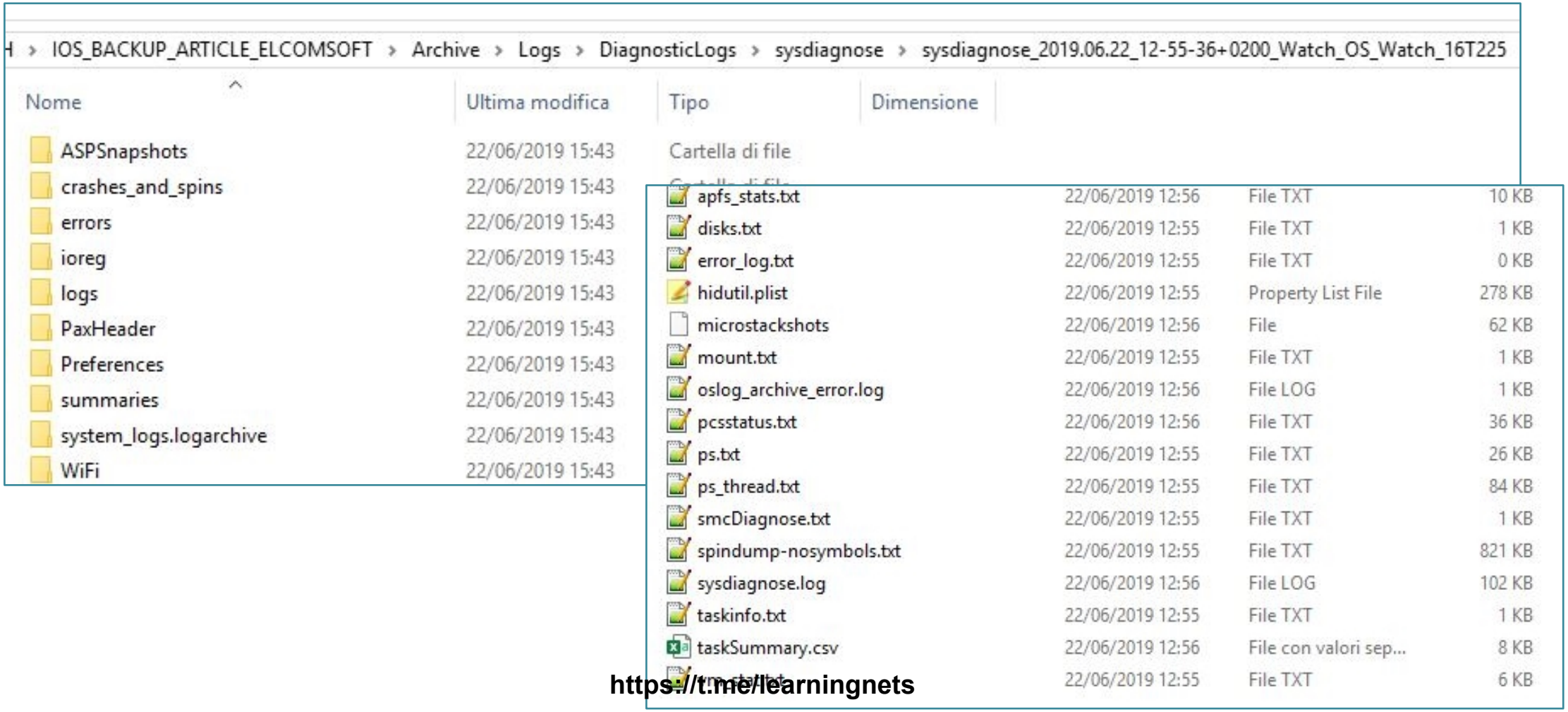
Notes: "~/Library/..." actually translates to: "/Users/[Your User Name]/Library/..."
The "/Users/[Your User Name]/Library/..." folder is hidden by default in macOS. Clicking the Finder's Go menu while holding the option key to expose the Library folder in the menu.

Windows:

```
C:\Users\[Your_User_Name]\AppData\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\
[Your_iOS_Device_Name]\DiagnosticLogs\sysdiagnose\co-sysdiagnose_YEAR.MONTH.DAY_HH-MM-SS-
xxxx.tar
```

Note: The Windows AppData folder is normally hidden by default. For instructions on how to expose hidden folders on the PC, please visit Microsoft's help center for your specific operating system version.

APPLE WATCH SYSDIAGNOSE



APPLE WATCH
MOBILE ACTIVATION LOGS

sysdiagnose — -bash — 153×55

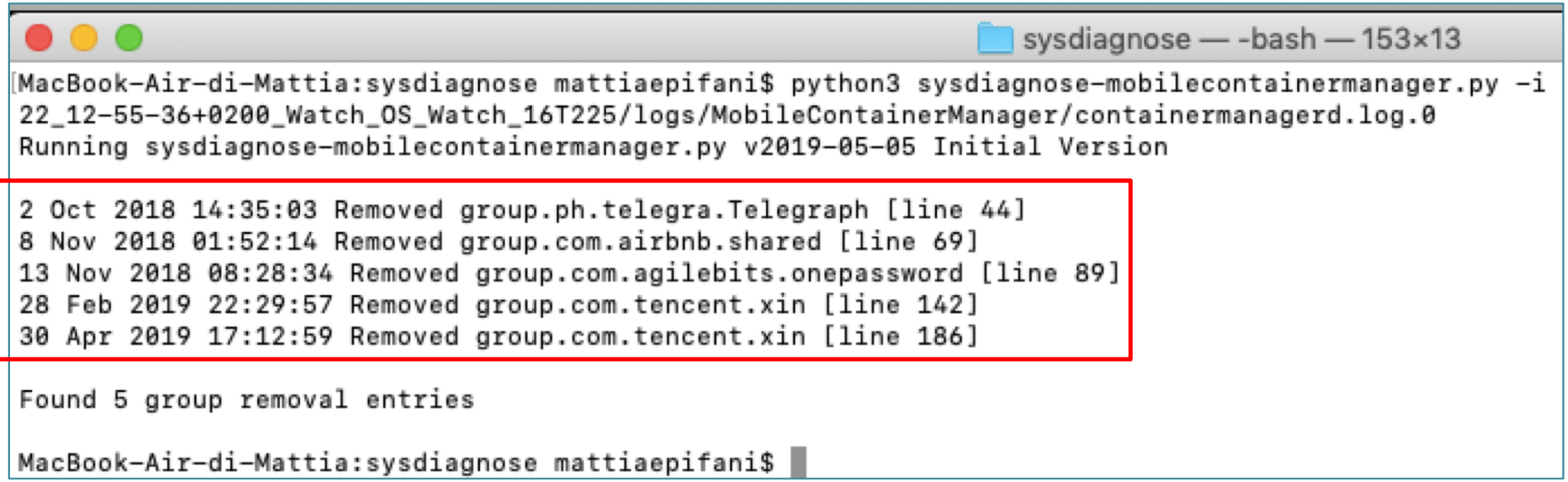
```
MacBook-Air-di-Mattia:sysdiagnose mattiaepifani$ python3 sysdiagnose-mobileactivation.py -i ../../../Desktop/Sysdiagnose\ test/sysdiagnose_2019.06.22_12-
```

sysdiagnose — -bash — 153×29

```
18 Apr 2019 12:46:35 Mobile Activation Startup  [line 170]
18 Apr 2019 12:46:35 Mobile Activation Build Version = 16S535
18 Apr 2019 12:46:35 Mobile Activation Hardware Model = N121bAP
18 Apr 2019 12:46:35 Mobile Activation Product Type = Watch3,4
18 Apr 2019 12:46:35 Mobile Activation Device Class = Watch

19 Apr 2019 11:17:36 Mobile Activation Startup  [line 186]
19 Apr 2019 11:17:36 Mobile Activation Build Version = 16T225
19 Apr 2019 11:17:36 Mobile Activation Hardware Model = N121bAP
19 Apr 2019 11:17:36 Mobile Activation Product Type = Watch3,4
19 Apr 2019 11:17:36 Mobile Activation Device Class = Watch

19 Apr 2019 11:17:36 Upgraded from 16S535 to 16T225 [line 200]

25 Apr 2019 13:14:36 Mobile Activation Startup  [line 203]
25 Apr 2019 13:14:36 Mobile Activation Build Version = 16T225
25 Apr 2019 13:14:36 Mobile Activation Hardware Model = N121bAP
25 Apr 2019 13:14:36 Mobile Activation Product Type = Watch3,4
25 Apr 2019 13:14:36 Mobile Activation Device Class = Watch

25 Apr 2019 13:17:08 Mobile Activation Startup  [line 218]
25 Apr 2019 13:17:08 Mobile Activation Build Version = 16T225
25 Apr 2019 13:17:08 Mobile Activation Hardware Model = N121bAP
25 Apr 2019 13:17:08 Mobile Activation Product Type = Watch3,4
25 Apr 2019 13:17:08 Mobile Activation Device Class = Watch

3 May 2019 21:52:33 Mobile Activation Startup  [line 233]
3 May 2019 21:52:33 Mobile Activation Build Version = 16T225
3 May 2019 21:52:33 Mobile Activation Hardware Model = N121bAP
```

```
23 Mar 2019 01:14:13 Mobile Activation Product Type = Watch3,4
23 Mar 2019 01:14:13 Mobile Activation Device Class = Watch
```

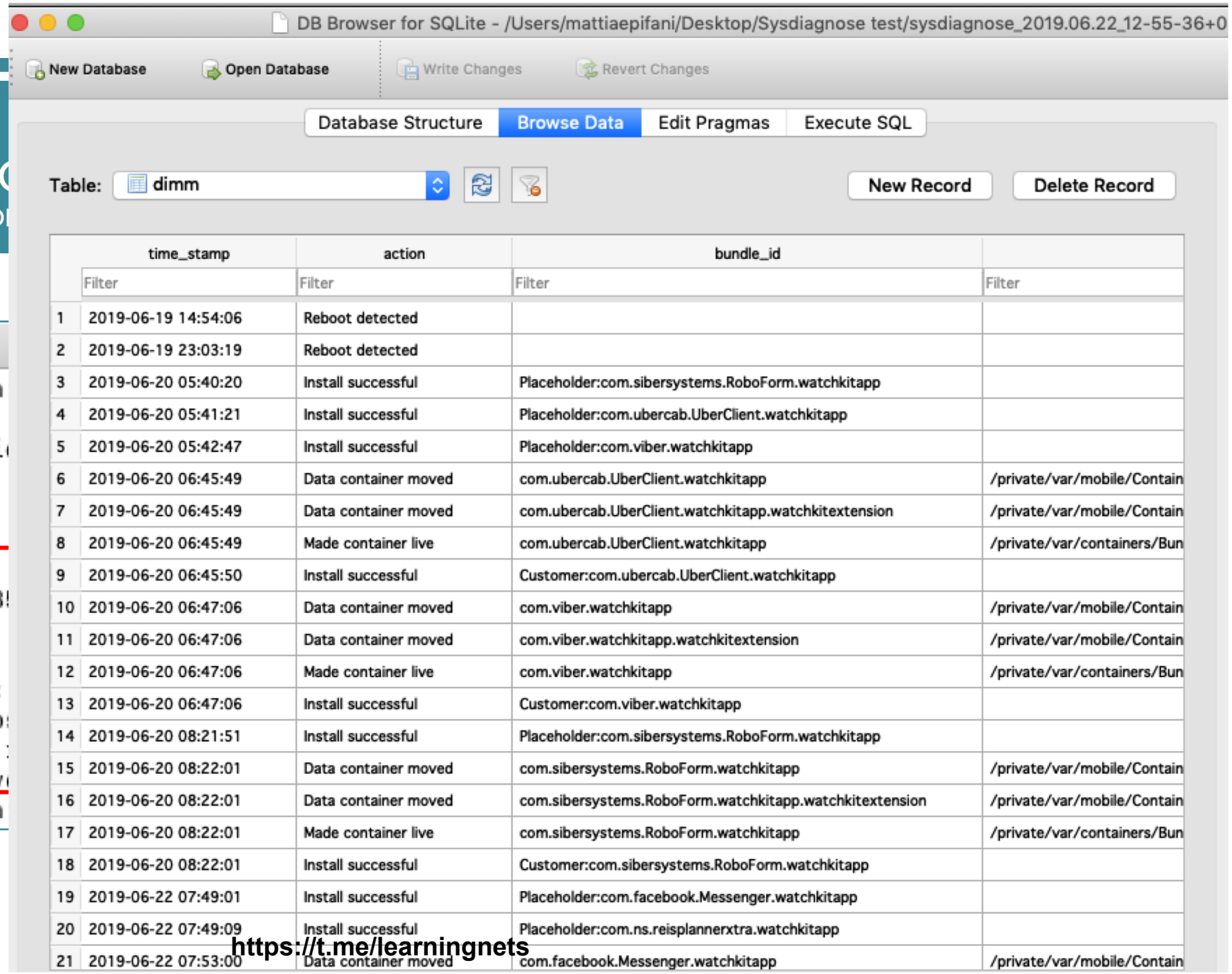
APPLE WATCH
MOBILE CONTAINER MANAGER LOGS



APPLE WATCH MOBILE INSTALLATI

HTTPS://ABRIGNONI.BLOGSPOT.CO

```
[MacBook-Air-di-Mattia

iOS Mobile Installati
By: @AlexisBrignoni
Web: abrignoni.com

Logs processed:  2
Lines processed:  253

Total apps:  29
Total installed apps:
Total uninstalled app
Total historical app
Total system state ev
MacBook-Air-di-Mattia
```



	time_stamp	action	bundle_id	
	Filter	Filter	Filter	Filter
1	2019-06-19 14:54:06	Reboot detected		
2	2019-06-19 23:03:19	Reboot detected		
3	2019-06-20 05:40:20	Install successful	Placeholder:com.sibersystems.RoboForm.watchkitapp	
4	2019-06-20 05:41:21	Install successful	Placeholder:com.ubercab.UberClient.watchkitapp	
5	2019-06-20 05:42:47	Install successful	Placeholder:com.viber.watchkitapp	
6	2019-06-20 06:45:49	Data container moved	com.ubercab.UberClient.watchkitapp	/private/var/mobile/Contain
7	2019-06-20 06:45:49	Data container moved	com.ubercab.UberClient.watchkitapp.watchkitextension	/private/var/mobile/Contain
8	2019-06-20 06:45:49	Made container live	com.ubercab.UberClient.watchkitapp	/private/var/containers/Bun
9	2019-06-20 06:45:50	Install successful	Customer:com.ubercab.UberClient.watchkitapp	
10	2019-06-20 06:47:06	Data container moved	com.viber.watchkitapp	/private/var/mobile/Contain
11	2019-06-20 06:47:06	Data container moved	com.viber.watchkitapp.watchkitextension	/private/var/mobile/Contain
12	2019-06-20 06:47:06	Made container live	com.viber.watchkitapp	/private/var/containers/Bun
13	2019-06-20 06:47:06	Install successful	Customer:com.viber.watchkitapp	
14	2019-06-20 08:21:51	Install successful	Placeholder:com.sibersystems.RoboForm.watchkitapp	
15	2019-06-20 08:22:01	Data container moved	com.sibersystems.RoboForm.watchkitapp	/private/var/mobile/Contain
16	2019-06-20 08:22:01	Data container moved	com.sibersystems.RoboForm.watchkitapp.watchkitextension	/private/var/mobile/Contain
17	2019-06-20 08:22:01	Made container live	com.sibersystems.RoboForm.watchkitapp	/private/var/containers/Bun
18	2019-06-20 08:22:01	Install successful	Customer:com.sibersystems.RoboForm.watchkitapp	
19	2019-06-22 07:49:01	Install successful	Placeholder:com.facebook.Messenger.watchkitapp	
20	2019-06-22 07:49:09	Install successful	Placeholder:com.ns.reisplannerxtra.watchkitapp	
21	2019-06-22 07:53:00	Data container moved	com.facebook.Messenger.watchkitapp	/private/var/mobile/Contain

APPLE WATCH POWER LOGS

HTTPS://GITHUB.COM/MAC4N6/APOLLO

APOLLO — -bash — 149×42

```
MacBook-Air-di-Mattia:APOLLO mattiaepifani$ python apollo.py -o csv -p ios -v yolo modules /Users/mattiaepifani/Dropbox/Personale/Diagnose_Profiles_iOS/APPLE_WATCH/
Parsing Modules...
Parsing:  129  modules.
Searching for database files...

modules/knowledge_audio_media_nowplaying.txt : 0 databases.

modules/knowledge_app_calendar_activity.txt : 0 databases.

modules/locationd_cacheencryptedAB_appharvest.txt : 0 databases.

modules/netusage_zliverouteperf.txt : 0 databases.

modules/knowledge_app_install.txt : 0 databases.

modules/routined_local_vehicle_parked.txt : 0 databases.

modules/powerlog_springboard_aggregate_notifications.txt : 1 databases.
        Executing module on: /Users/mattiaepifani/Dropbox/Personale/Diagnose_Profiles_iOS/APPLE_WATCH/CurrentPowerlog.PLSQL
        ***ERROR***: Could not parse database [/Users/mattiaepifani/Dropbox/Personale/Diagnose_Profiles_iOS/APPLE_WATCH/CurrentPowerlog.PLSQL]. Often
 this is due to file permissions, or changes in the database schema. This also happens with same-named databases that contain different data (ie: cac
he_encryptedB.db).

modules/locationd_cacheencryptedAB_poiharvestlocation.txt : 0 databases.

modules/powerlog_device_telephony_registration.txt : 1 databases.
        Executing module on: /Users/mattiaepifani/Dropbox/Personale/Diagnose_Profiles_iOS/APPLE_WATCH/CurrentPowerlog.PLSQL
        ***ERROR***: Could not parse database [/Users/mattiaepifani/Dropbox/Personale/Diagnose_Profiles_iOS/APPLE_WATCH/CurrentPowerlog.PLSQL]. Often
 this is due to file permissions, or changes in the database schema. This also happens with same-named databases that contain different data (ie: cac
he_encryptedB.db).

modules/locationd_cacheencryptedAB_locationharvest.txt : 0 databases.

modules/powerlog_device_volume.txt : 1 databases.
        Executing module on: /Users/mattiaepifani/Dropbox/Personale/Diagnose_Profiles_iOS/APPLE_WATCH/CurrentPowerlog.PLSQL
                Number of Records: 25

modules/knowledge_device_is_backlit.txt : 0 databases.

modules/powerlog_button_state.txt : 1 databases.
        Executing module on: /Users/mattiaepifani/Dropbox/Personale/Diagnose_Profiles_iOS/APPLE_WATCH/CurrentPowerlog.PLSQL
```

APPLE WATCH POWER LOGS

HTTPS://GITHUB.COM/MAC4N6/APOLLO

Timestamp	Activity	Output
21/06/2019 14:27	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 14:27:51] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO
21/06/2019 14:27	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:27:57] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI
21/06/2019 14:28	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:28:00] [BUNDLE_ID: com.apple.NanoMail] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT
21/06/2019 14:28	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:28:10] [BUNDLE_ID: com.apple.carousel.home-screen] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SC
21/06/2019 14:32	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:32:58] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI
21/06/2019 14:34	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:34:54] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI
21/06/2019 14:47	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:47:08] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_
21/06/2019 14:57	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:57:30] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_
21/06/2019 14:59	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 14:59:55] [ACTIVEROUTE: INVALID] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO
21/06/2019 14:59	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:59:58] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_ST
21/06/2019 15:00	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:00:17] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO
21/06/2019 15:00	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:00:21] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_ST
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:19] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:37] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:40] [BUNDLE_ID: com.apple.carousel.home-screen] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREE
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:42] [BUNDLE_ID: com.apple.NanoPhone] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATE_
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_ST
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_ST
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [ACTIVEROUTE: INVALID] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:47] [ACTIVEROUTE: Speaker] [ACTIVE: YES] [ACTIVE PID: 0] [OUTPUT CATEGORY: PhoneCall] [HEADSET HAS INPUT: 0] [HEADPHONE
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:47] [VOLUME PERCENTAGE: 95.4648911953] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 1970-10-07 07:16:22] [OFFSET_TIMEST
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:50] [BUNDLE_ID: com.apple.NanoPhone] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATE_
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:53] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:53] [VOLUME PERCENTAGE: 69.9999988079] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 1970-10-07 07:16:28] [OFFSET_TIMEST

APPLE WATCH POWER LOGS

HTTPS://GITHUB.COM/MAC4N6/APOLLO

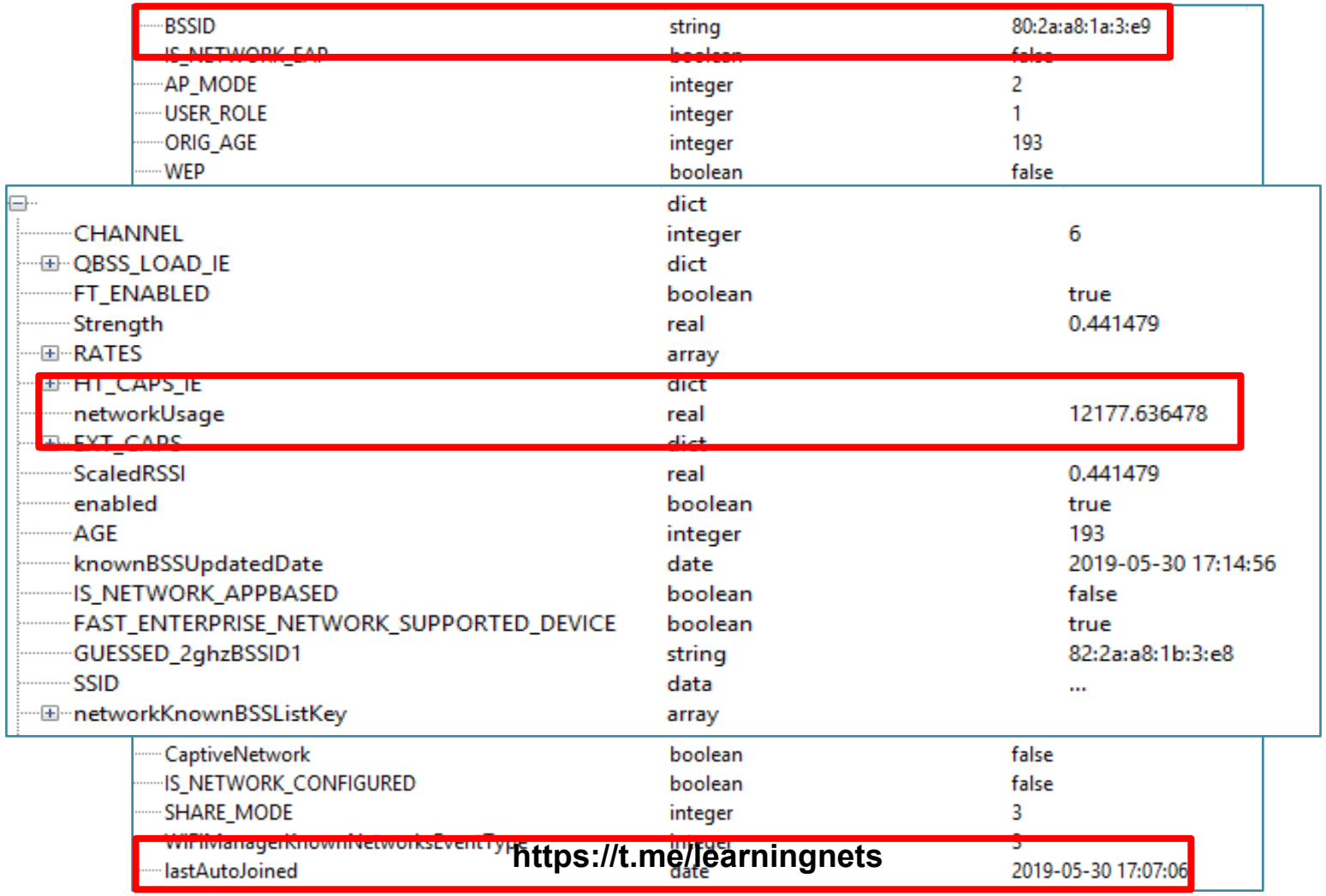
Timestamp	Activity	Output
21/06/2019 14:27	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 14:27:51] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO
21/06/2019 14:27	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:27:57] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI
21/06/2019 14:28	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:28:00] [BUNDLE_ID: com.apple.NanoMail] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATE_TI
21/06/2019 14:28	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:28:10] [BUNDLE_ID: com.apple.carousel.home-screen] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREE
21/06/2019 14:30	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:30:45] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI
21/06/2019 14:32	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:32:58] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI
21/06/2019 14:47	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:47:08] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIG
21/06/2019 14:57	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:57:30] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIG
21/06/2019 14:59	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 14:59:55] [ACTIVEROUTE: INVALID] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADS
21/06/2019 14:59	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:59:58] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT
21/06/2019 15:00	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:00:17] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADS
21/06/2019 15:00	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:00:21] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:19] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIG
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:37] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIG
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:42] [BUNDLE_ID: com.apple.NanoPhone] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATE_
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_ST
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_ST
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [ACTIVEROUTE: INVALID] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:47] [ACTIVEROUTE: Speaker] [ACTIVE: YES] [ACTIVE PID: 0] [OUTPUT CATEGORY: PhoneCall] [HEADSET HAS INPUT: 0] [HEADPHONE
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:47] [VOLUME PERCENTAGE: 95.4648911953] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 1970-10-07 07:16:22] [OFFSET_TIMEST
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:50] [BUNDLE_ID: com.apple.NanoPhone] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATE_
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:53] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:53] [VOLUME PERCENTAGE: 69.99999880791] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 1970-10-07 07:16:28] [OFFSET_TIMEST

APPLE WATCH POWER LOGS

HTTPS://GITHUB.COM/MAC4N6/APOLLO

Timestamp	Activity	Output	D
21/06/2019 14:27	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 14:27:51] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO	/U
21/06/2019 14:27	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:27:57] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI	/U
21/06/2019 14:28	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:28:00] [BUNDLE_ID: com.apple.NanoMail] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATE_TI	/U
21/06/2019 14:28	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:28:10] [BUNDLE_ID: com.apple.carousel.home-screen] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREE	/U
21/06/2019 14:30	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:30:45] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI	/U
21/06/2019 14:32	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:32:58] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI	/U
21/06/2019 14:34	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:34:54] [BUNDLE_ID: com.apple.carousel.clock] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_STATI	/U
21/06/2019 14:47	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:47:08] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_	/U
21/06/2019 14:57	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:57:30] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_	/U
21/06/2019 14:59	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 14:59:55] [ACTIVEROUTE: INVALID] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO	/U
21/06/2019 14:59	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 14:59:58] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_ST	/U
21/06/2019 15:00	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:00:17] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHO	/U
21/06/2019 15:00	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:00:21] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_ST	/U
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:19] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_	/U
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:37] [BUNDLE_ID: com.spotify.client.watchkitapp] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGHT: 1.0] [ORIGINAL_SCREEN_	/U
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:42] [BUNDLE_ID: com.apple.NanoPhone] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGH	
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREEN	
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [BUNDLE_ID: com.apple.carousel.alert] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 3000.0] [SCREEN	
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:46] [ACTIVEROUTE: INVALID] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video]	
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:47] [ACTIVEROUTE: Speaker] [ACTIVE: YES] [ACTIVE PID: 0] [OUTPUT CATEGORY: PhoneCall] [HE	
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:47] [VOLUME PERCENTAGE: 95.4648911953] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 19	
21/06/2019 15:02	Application Usage	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:50] [BUNDLE_ID: com.apple.NanoPhone] [APPROLE: 0] [DISPLAY: 0] [LEVEL: 0.0] [SCREENWEIGH	
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:53] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video]	
21/06/2019 15:02	Device State	[ADJUSTED_TIMESTAMP: 2019-06-21 15:02:53] [VOLUME PERCENTAGE: 69.9999988079] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 19	

APPLE WATCH WIFI LOGS



APPLE WATCH WIFI LOGS

Stats | Tools

BSSID/MAC: 80:2a:a8:1a:03:e9

SSID / Network Name (exact match):

SSID / Network Name (wildcards[1]: %

Must Be a FreeNet | Must Be a C

Query | Reimposta

[0] 0-7 Product of number of observers and observations.

[1] '%' means zero-or-more characters, '_' means a single character.

BSSID/MAC: 80:2a:a8:1a:03:e9

SSID / Network Name (exact match): foobar

SSID / Network Name (wildcards[1]: % and _): foobar%

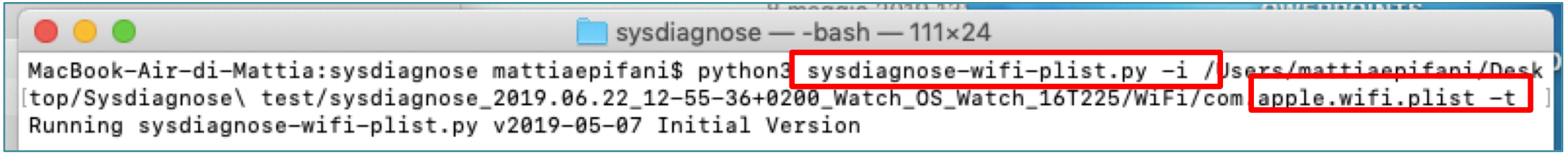
Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS
map	80:2A:A8:1A:03:E9	ITTIG-CNR		infra	2016-09-23T00:[illegible]	2018-01-[illegible]	WPA	43.79183578	11.22836018	6	0	2

APPLE WATCH WIFI LOGS

80211W_ENABLED	boolean	true
WiFiNetworkIsAutoJoined	boolean	true
SCAN_RESULT_FROM_PROBE_RSP	boolean	false
CARPLAY_NETWORK	boolean	false
PHY_MODE	integer	16
IS_NETWORK_CAPTIVE	boolean	false
lastJoined	date	2019-03-09 19:44:26
SSID_STR	string	Andante_Restaurante
CHANNEL_WIDTH	integer	20
UserDirected	boolean	false
BEACON_INT	integer	100
RSSI	integer	-78
IS_NETWORK_EXPIRABLE	boolean	false
IE	data	...
CaptiveNetwork	boolean	false
IS_NETWORK_CONFIGURED	boolean	false
SHARE_MODE	integer	3
WiFiManagerKnownNetworksEventType	integer	3
lastAutoJoined	date	2019-03-09 20:00:45
lastUpdated	date	2019-03-09 03:43:18
CAPABILITIES	integer	1073
RSN_IE	dict	

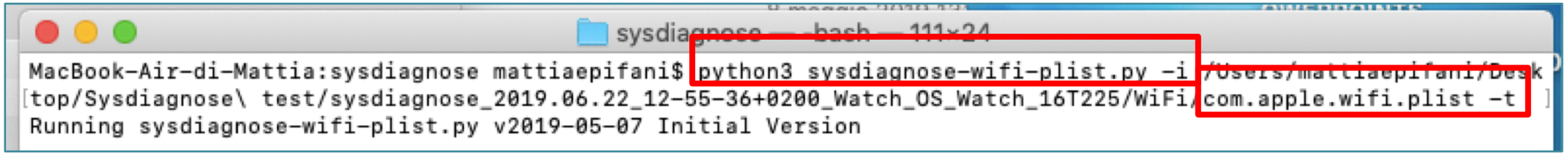
APPLE WATCH WIFI LOGS

```
sysdiagnose-wifi-plist.py -i
```



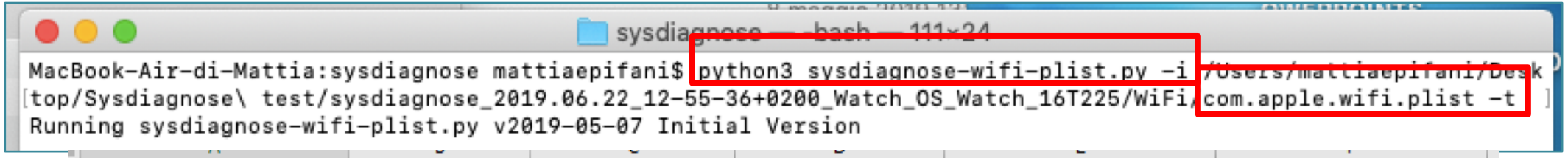

```
com.apple.wifi.plist -t
```

APPLE WATCH WIFI LOGS



SSID	BSSID	NETUSAGE	COUNTRYCODE	LASTJOINED	LASTAUTOJOINED
rnsys	cc:2d:e0:93:14:25	491974.9299207926		2019-06-22 09:56:20.134874	2019-06-22 10:50:06.292416
Vodafone-30452471	90:35:6e:cb:69:68	1917152.7370038033	IT	2019-06-21 20:50:09.500747	2019-04-18 19:30:04.522801
NETGEAR13	8:bd:43:68:1f:48	105486.80752205849		2019-06-21 15:11:04.720972	2019-06-21 15:11:05.372420
EPIFANI_NEW	cc:40:d0:c7:1e:70	4139.615980029106		2019-06-18 13:04:49.779367	2019-06-18 12:32:08.724745
EleSpongie	3e:5c:f2:7f:7a:20	2338.421647310257	IT	2019-06-06 19:43:51.609769	2019-06-06 20:18:29.479695
Ospiti	9c:1c:12:4c:69:24	2567.6274020671844		2019-06-04 14:08:29.851830	2019-06-04 13:19:45.907810
Strike	a4:b1:e9:99:ce:29	2871.0092381238937		2019-05-24 19:52:46.923116	2019-05-24 18:50:57.488311
Starhotels	54:3d:37:39:43:cc	799.9198870658875	IT	2019-05-18 01:34:31.043223	2018-11-13 01:15:56.358491
unaltrapasta	d4:60:e3:d7:ad:cb	73.28322696685791	IT	2019-05-14 18:55:16.285575	2019-05-14 18:55:02.862883
EOLO - FRITZ!Box 4020 EN	38:10:d5:b3:e:55	22394.69042801857	DE	2019-05-12 09:06:23.662969	2019-05-12 09:01:03.199525
leondoro-ospiti	ac:84:c6:55:46:28	4850.699810028076		2019-05-11 19:03:20.041714	2019-05-11 19:03:21.191929
Lacucinadeirolli	b0:ea:bc:77:e8:26			2019-04-30 10:46:06.198349	
scandic_easy	94:f6:65:3e:6a:cc	11.447627067565918	NO	2019-04-26 14:22:03.710064	2019-04-23 22:06:40.724572
NHV25 Gjest	28:6f:7f:82:2:a0	21904.303030967712	NO	2019-04-26 12:41:05.498512	2019-04-26 13:41:12.637502
Paleis Hotel	d4:68:4d:4f:58:fc	6.301298975544519	NL	2019-03-28 04:12:37.300878	2018-11-19 16:38:02.600754

APPLE WATCH WIFI LOGS



SSID	BSSID	NETUSAGE	COUNTRYCODE	LASTJOINED	LASTAUTOJOINED
hhonors	c0:7b:bc:38:2f:51	8.49052608013153		2019-03-14 00:12:20.820977	2019-03-11 15:09:42.671418
Hilton_Meetings	58:97:bd:5c:b5:ec	14.572947978973389	US	2019-03-13 23:58:25.644837	2019-03-11 19:28:51.001382
attwifi	c0:7b:bc:38:2f:50	14.254495024681091		2019-03-12 04:54:58.752070	2019-03-11 21:54:47.070492
GAP FREE	c:8d:db:b2:f4:a6	1804.6912928819656	MX	2019-03-10 20:03:54.780260	2019-03-10 20:25:17.038113
it 29	7c:76:68:ac:32:f8	3090.763992667198		2019-03-10 16:24:48.690164	2019-03-10 14:52:48.583971
made	5c:77:76:9e:ad:77	108.41480600833893	MX	2019-03-09 22:07:57.616273	2019-03-09 22:18:58.010924
LINK_F0DA	d4:6e:e:2c:f0:da	44964.695753932		2019-03-09 19:06:20.494336	2019-03-09 19:06:22.032070
dante_Restaurante	78:8a:20:12:87:82	3556.1446338891983	MX	2019-03-09 18:44:26.275691	2019-03-09 19:00:45.195768
PVRestaurante	24:a4:3c:92:86:b4	107.86840093135834		2019-03-09 02:24:53.632197	2019-03-09 02:24:23.629496
INFINITUM2972	d0:5:2a:14:1e:70	2250.9017400741577	MX	2019-03-09 00:31:19.015224	2019-03-09 00:31:19.935449
Surf Town	4:18:d6:25:26:5e			2019-03-08 04:22:29.695634	
#SFO FREE WIFI	f4:cf:e2:da:48:bc	6.610926985740662	US	2019-03-06 17:28:56.883284	2019-03-06 16:46:27.440489
The Laurel Inn	2c:c5:d3:33:fc:fc	10.98872995376587	US	2019-03-06 15:04:42.830168	2019-03-04 02:52:16.847448
Marriott_GUEST	d4:68:4d:30:58:ec	5.4302390813827515	DE	2019-03-06 00:35:47.130973	2018-12-10 17:59:19.654429
Carmel Lodge	c:f4:d5:34:39:dc	207.6443749666214	US	2019-03-03 18:58:12.058406	2019-03-03 18:34:17.195517
xfinitywifi	54:b2:3:21:db:88	14.251927018165588	US	2019-03-03 07:17:17.206558	2019-02-28 19:45:42.240836
Bluebird	4:18:d6:78:9f:c0	13401.491521000862		2019-03-02 17:11:20.105642	2019-03-02 16:49:14.051049
@SBWineTherapy Free Wi-	8:62:66:40:96:a	14.141973972320557		2019-03-02 01:13:18.510539	2019-03-02 00:50:59.700302

APPLE WATCH FORENSICS – MANUAL ACQUISITION

MATTIA EPIFANI – FRANCESCO PICASSO

SANS DFIR EU SUMMIT

PRAGUE, 29 SEPTEMBER 2019

APPLE WATCH MANUAL ACQUISITION

NATIVE APPLICATIONS

- Contacts
- Call logs
- SMS/iMessage
- Mail
- Calendar
- Wallet
- Health / Heart rate
- Photos (if enabled)
- iTunes

THIRD PARTY APPLICATIONS

- Facebook Messenger
- Telegram
- Spotify
- Shazam
- Lufthansa
- British Airways
- Alitalia
- Uber

APPLE WATCH MANUAL ACQUISITION

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

APPLE WATCH FORENSICS – SYNCED IPHONE

MATTIA EPIFANI – FRANCESCO PICASSO

SANS DFIR EU SUMMIT

PRAGUE, 29 SEPTEMBER 2019

APPLE WATCH BACKUP

HTTPS://SUPPORT.APPLE.COM/EN-US/HT204518

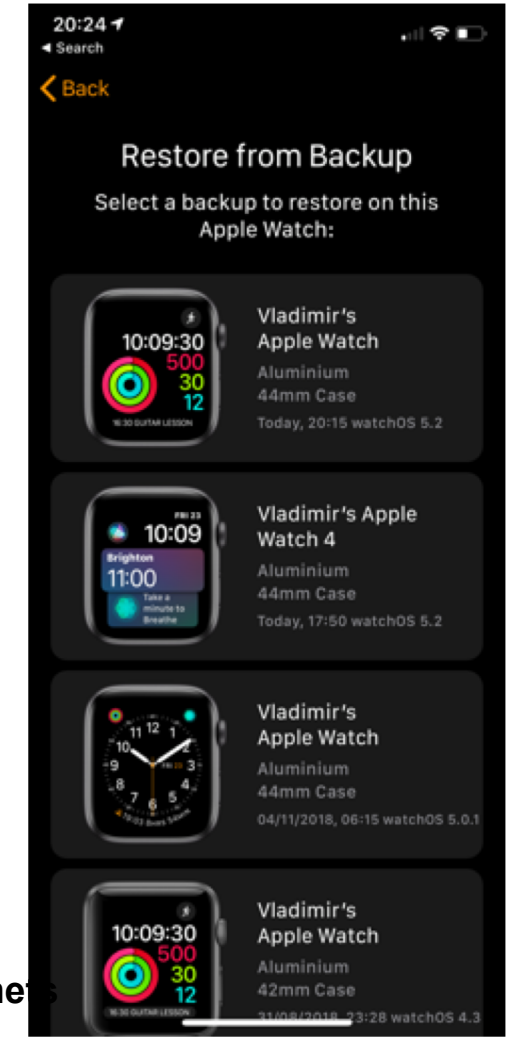
- Apple Watch **backup data automatically to your companion iPhone**, so you can restore your Apple Watch from a backup
- When you backup your iPhone to iCloud or iTunes, **your iPhone backup will also include your Apple Watch data**

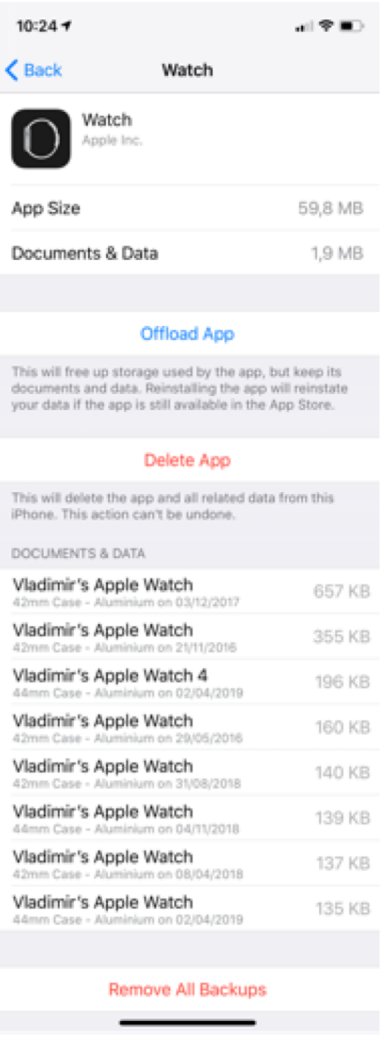
APPLE WATCH BACKUP AND UNPAIR

- 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

APPLE WATCH BACKUP RESTORE

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





APPLE WATCH
BACKUP - WHAT'S INSIDE?

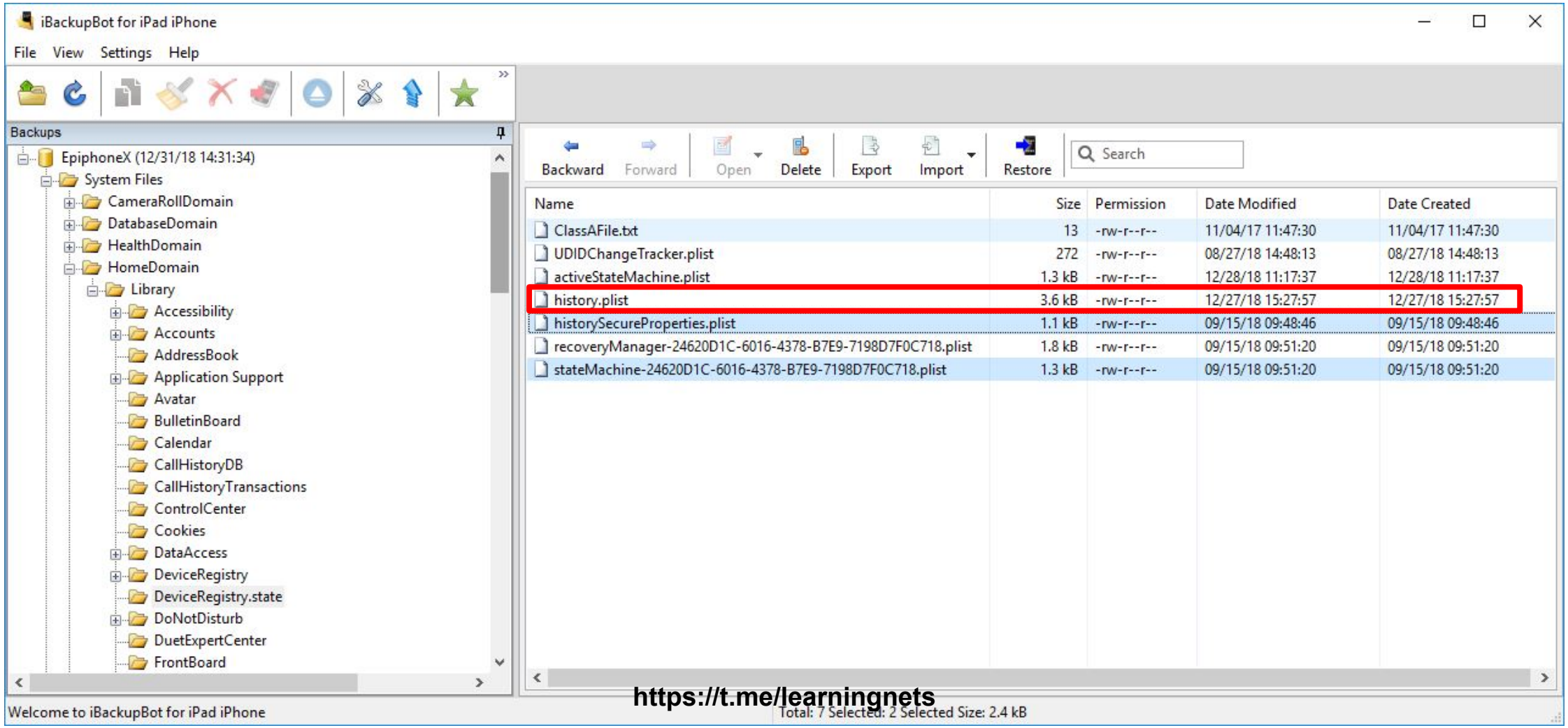
- Built-in apps (App data and settings)
- Third-party apps (Only settings)
- Health and Fitness data
  - **To back up Health and Fitness data, you need to use iCloud or an encrypted iTunes backup**

- App layout on Home screen
- Clock face and dock settings
- Notification settings
- Music playlists and albums
- Synced photo album
- Time Zone

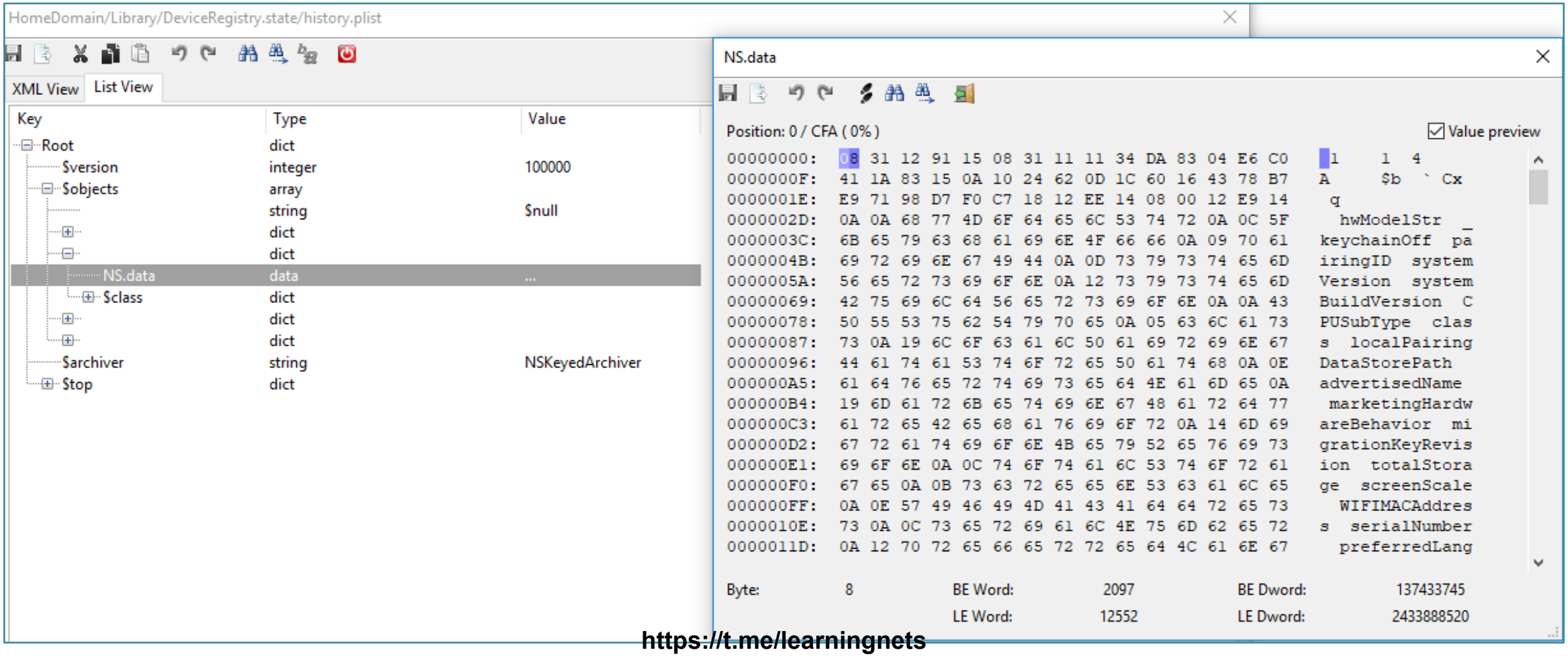
APPLE WATCH
BACKUP - WHAT'S **NOT** INCLUDED?

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

APPLE WATCH **DEVICEREGISTRY.STATE** FOLDER



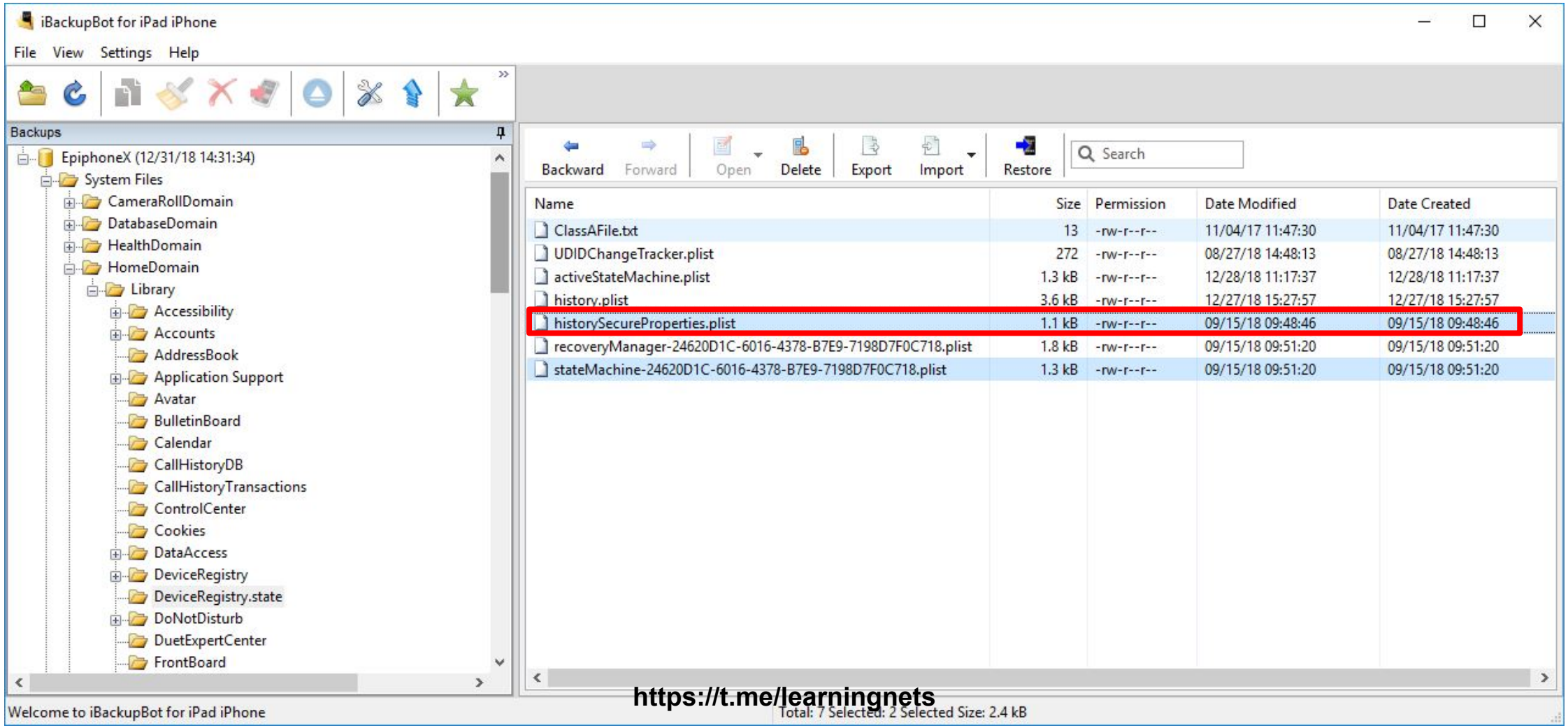
APPLE WATCH
HISTORY.PLIST



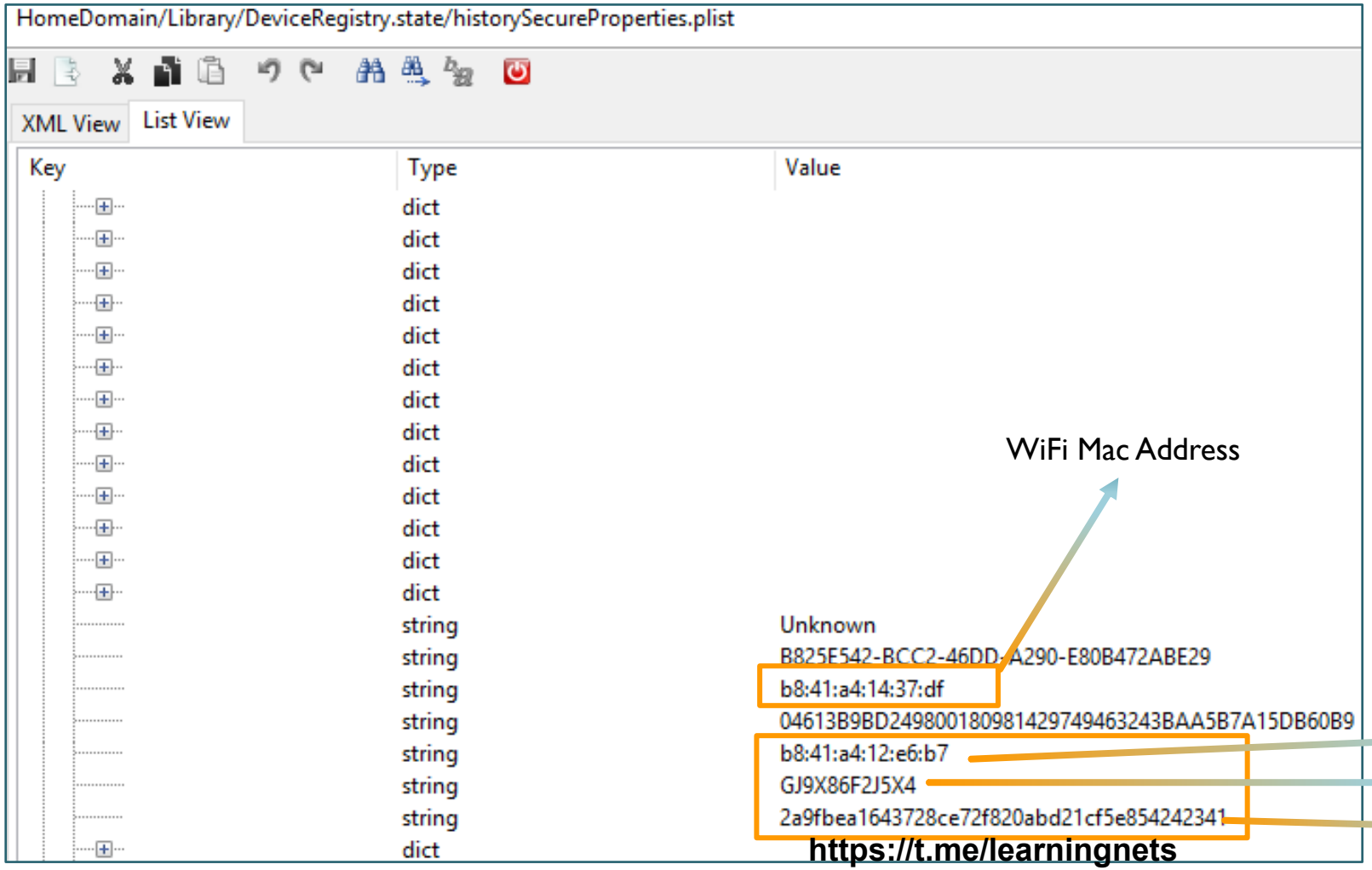
APPLE WATCH
HISTORY.PLIST

Field name	Field value
hwModelStr	N121bAP
systemVersion	5.1.1
systemBuildVersion	16R600
localPairingDataStorePath	/var/mobile/Library/DeviceRegistry/24620D1C-6016-4378-B7E9-7198D7F0C71
advertisedName	69647CEB
Name	Apple Watch di Mattia
modelNumber	A1859
deviceNameString	Watch3,4

APPLE WATCH **DEVICEREGISTRY.STATE** FOLDER



APPLE WATCH
HISTORYSECUREPROPERTIES.PLIST



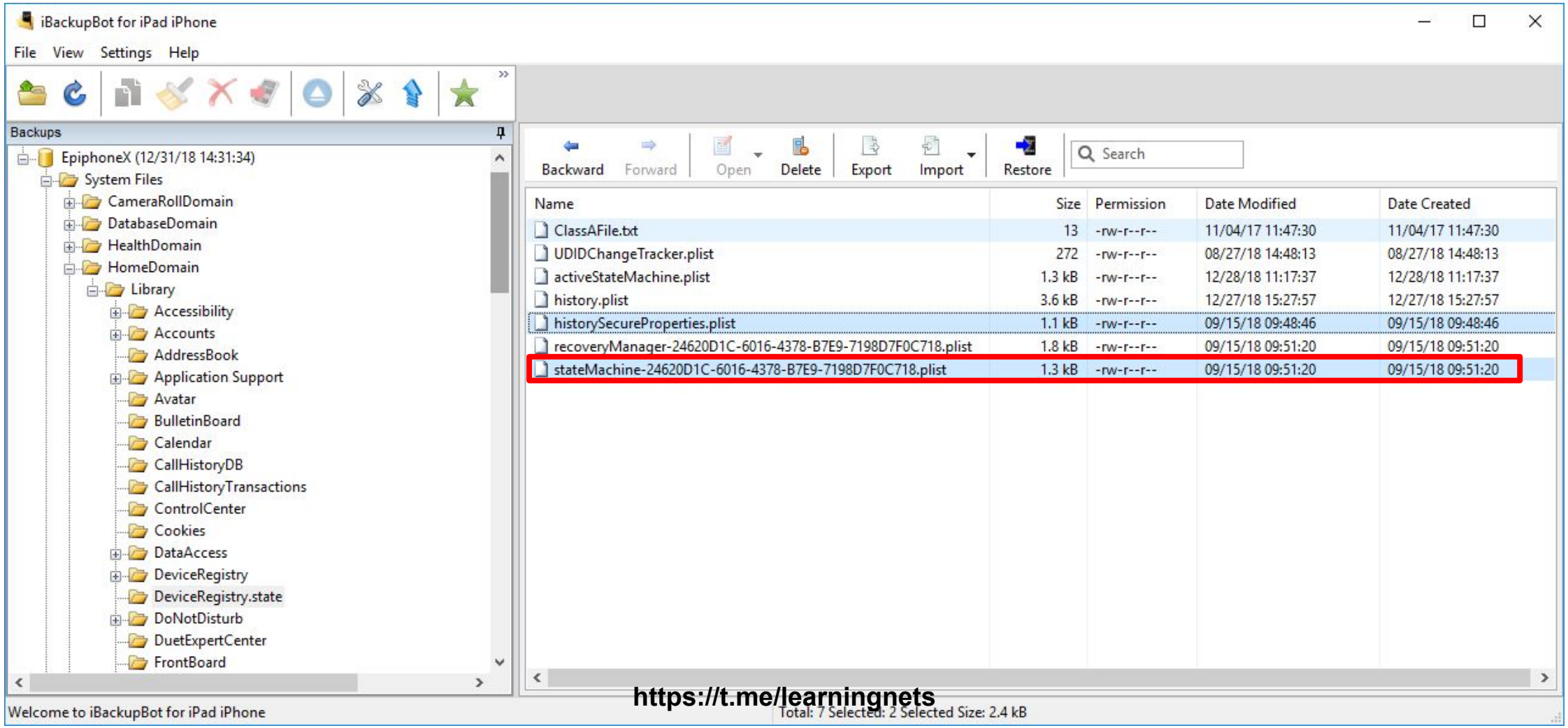
WiFi Mac Address

BT Mac Address

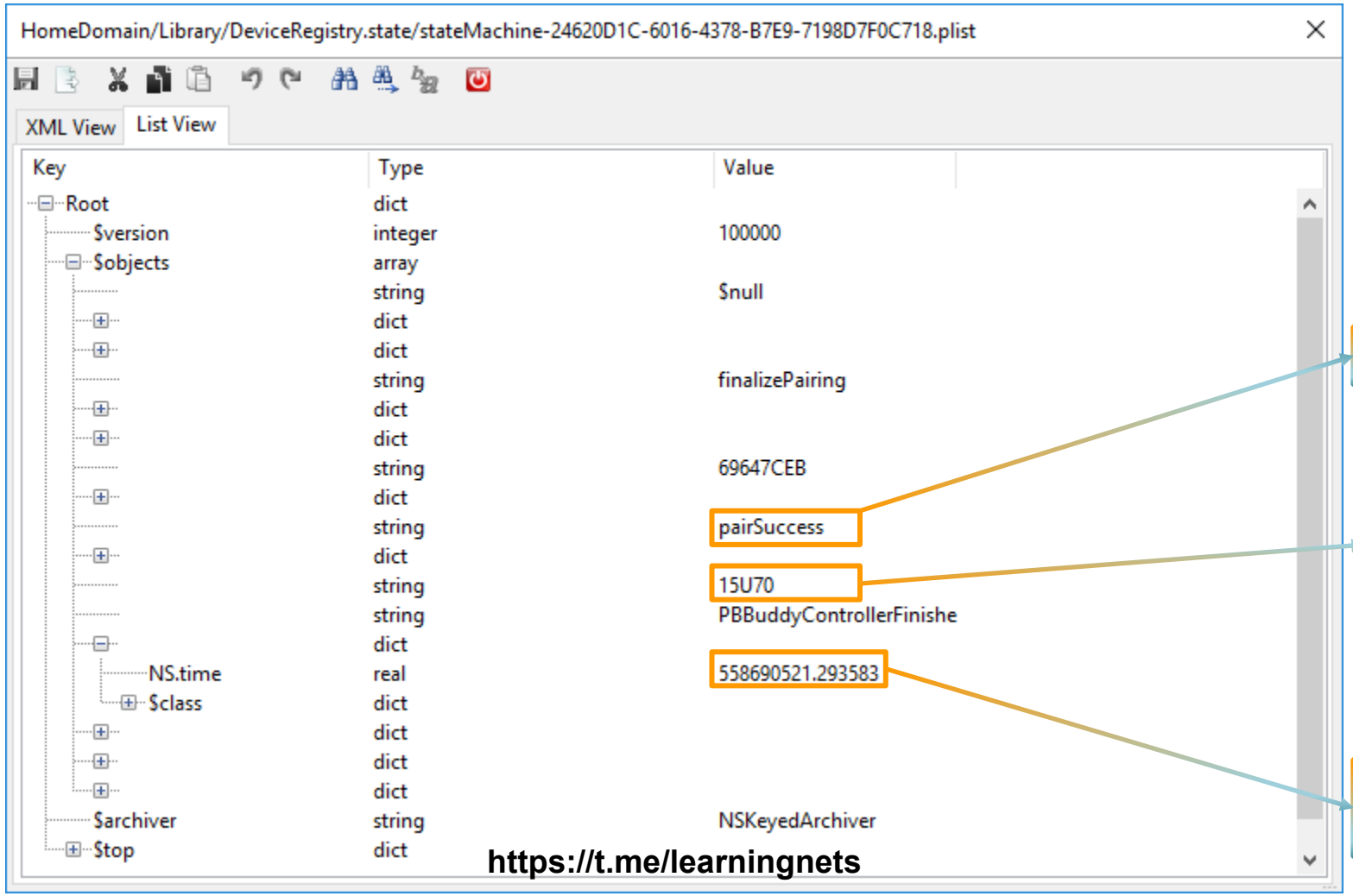
Serial Number

UDID

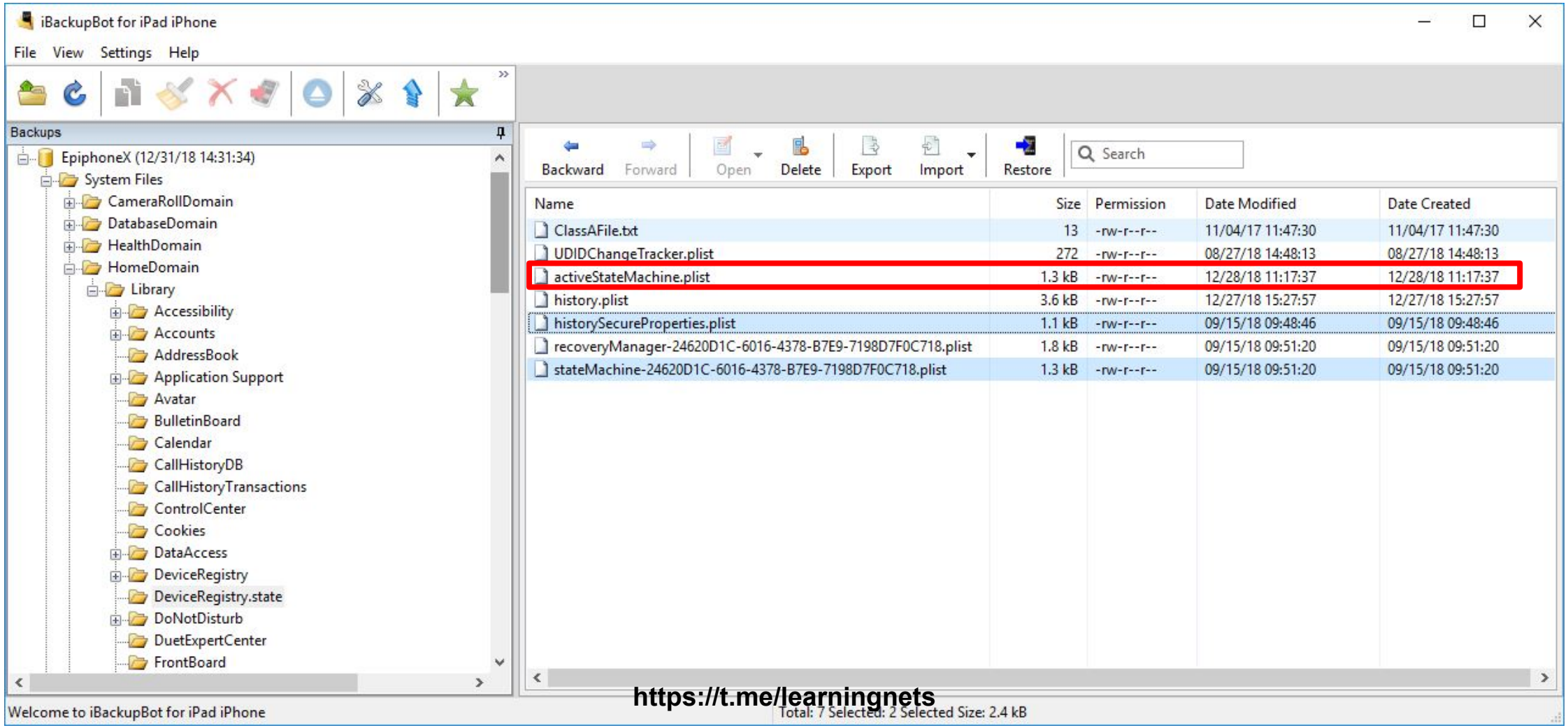
APPLE WATCH **DEVICEREGISTRY.STATE** FOLDER



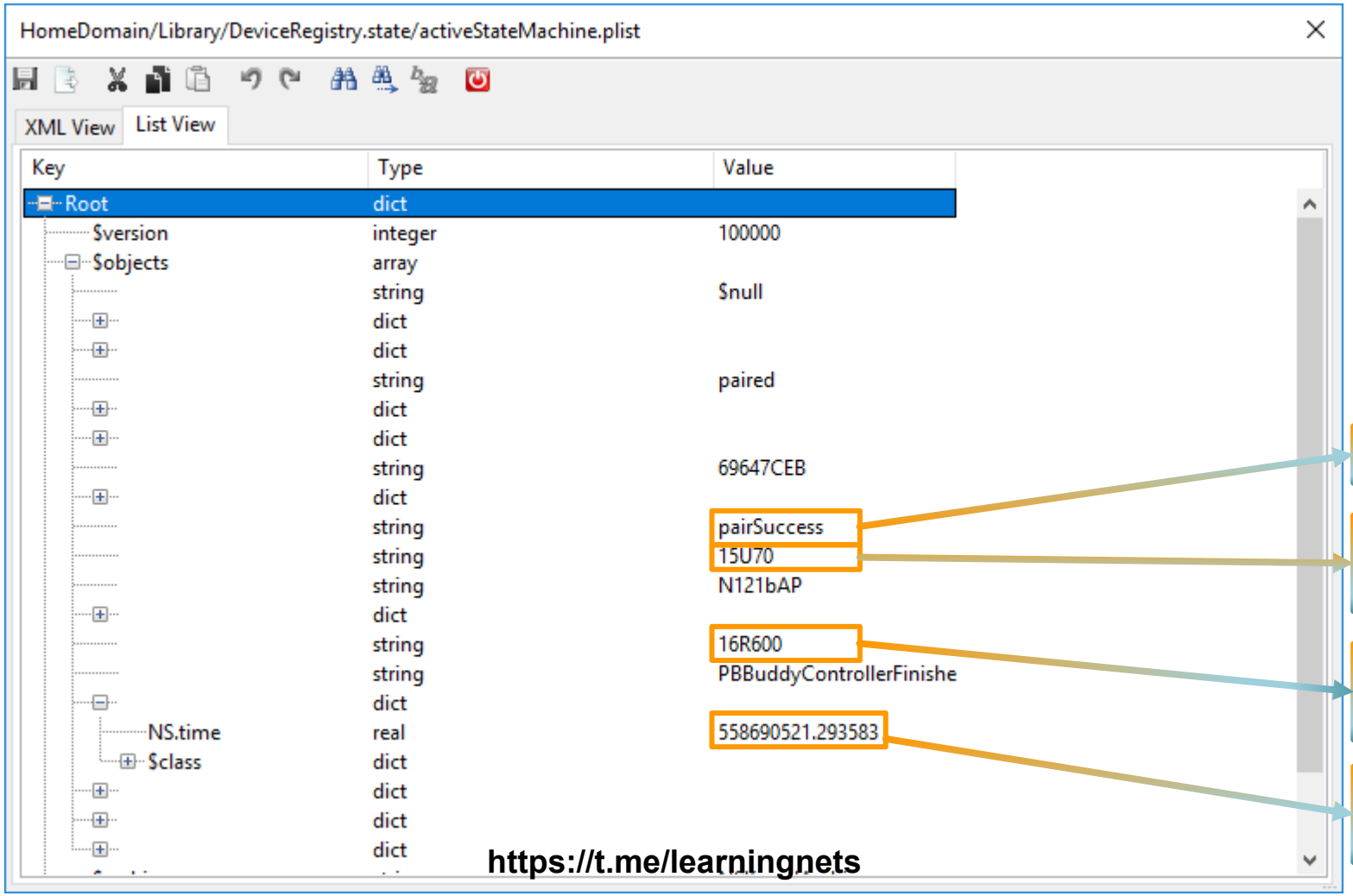
APPLE WATCH
STATEMACHINE-<GUID>.PLIST



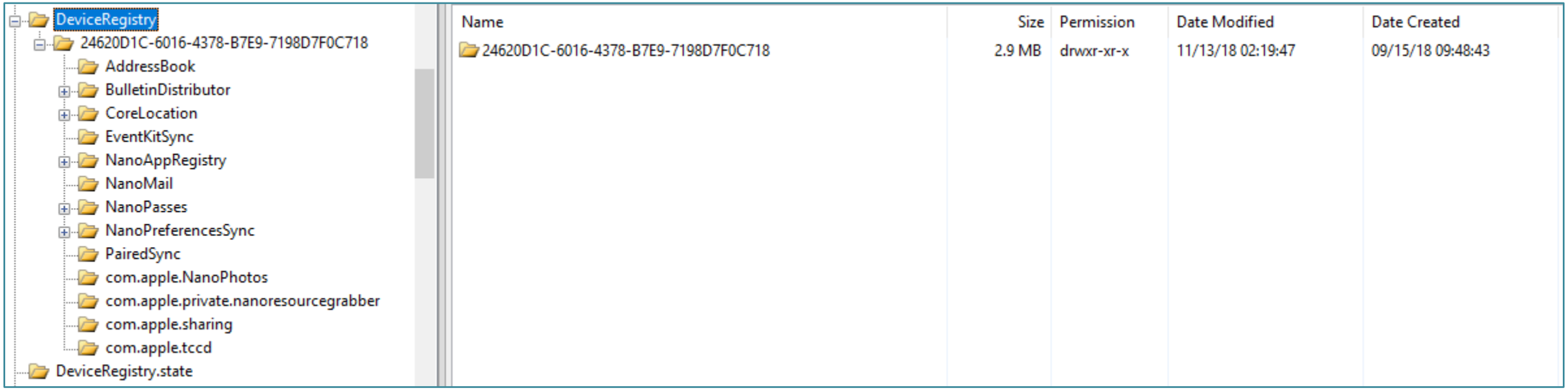
APPLE WATCH
DEVICEREGISTRY.STATE FOLDER



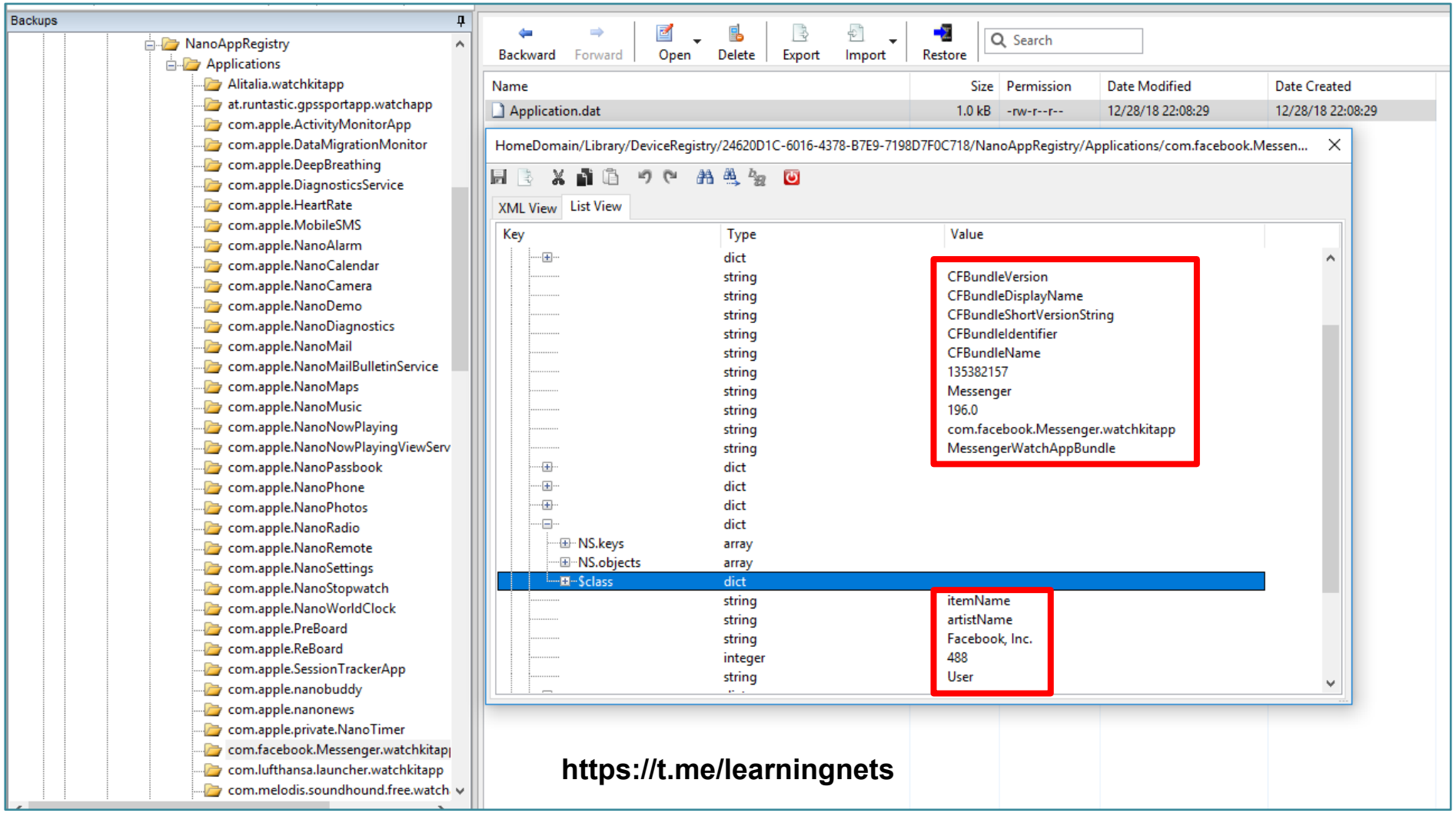
APPLE WATCH
ACTIVESTATEMACHINE.PLIST



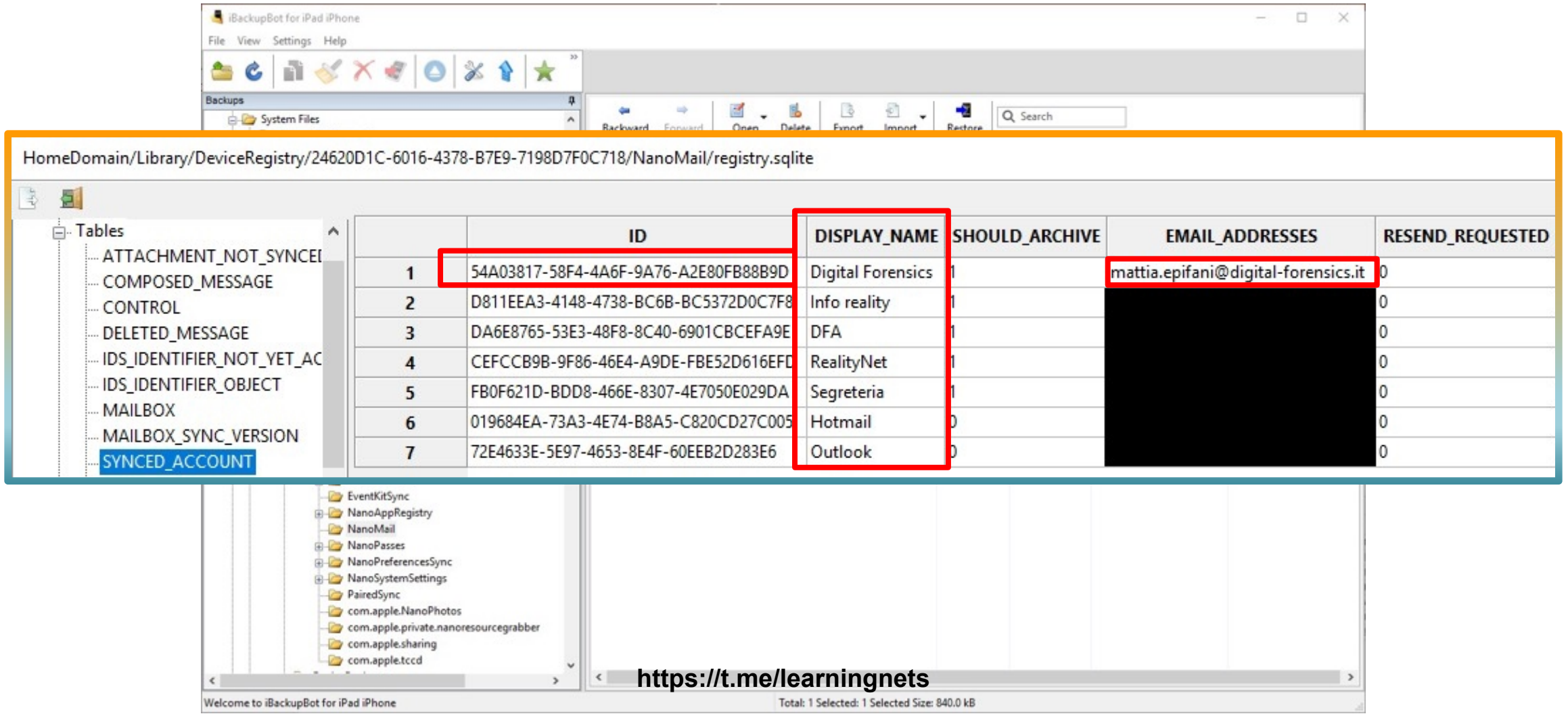
APPLE WATCH **DEVICEREGISTRY** FOLDER



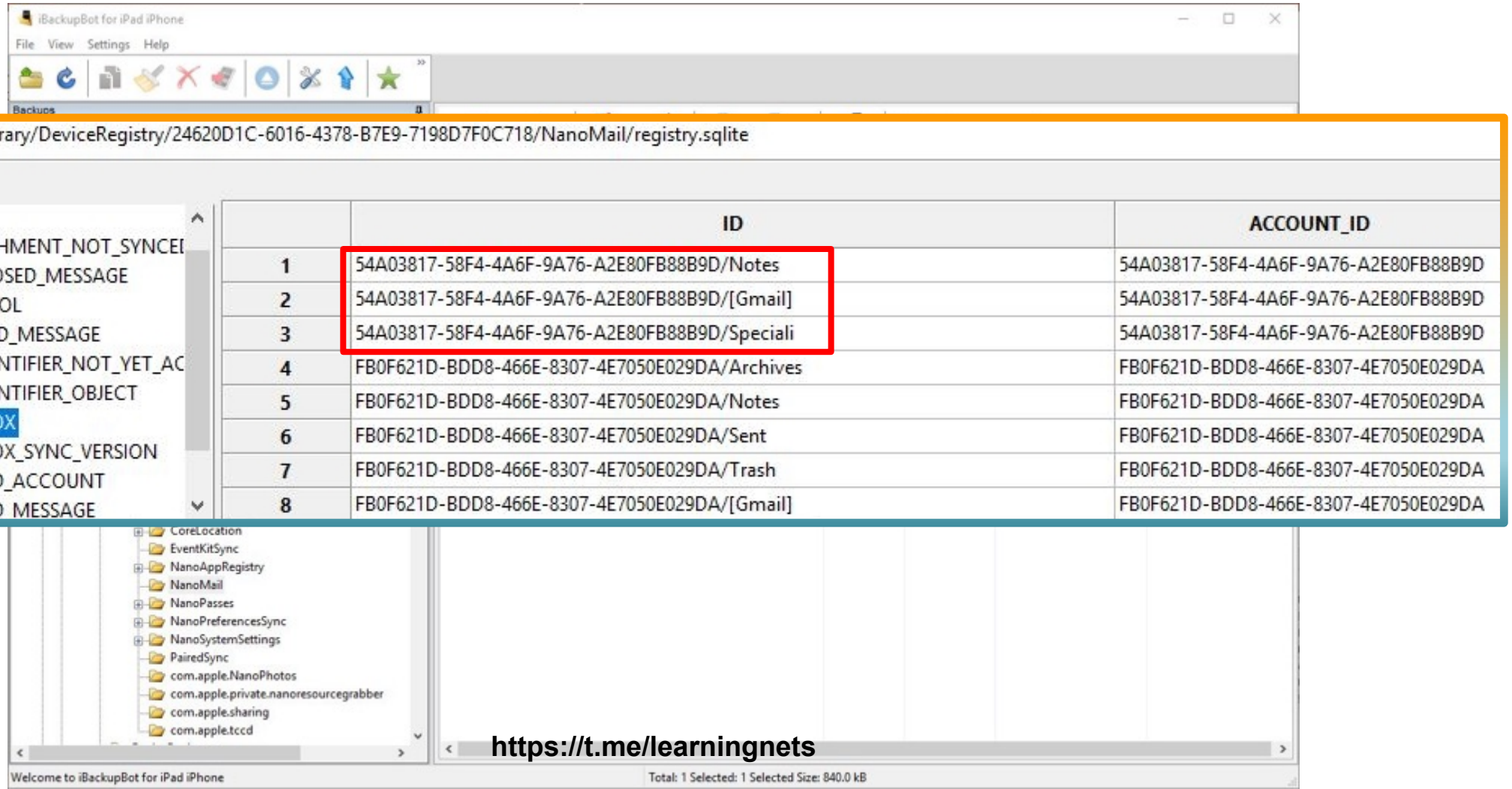
APPLE WATCH **NANOAPPREGISTRY** FOLDER



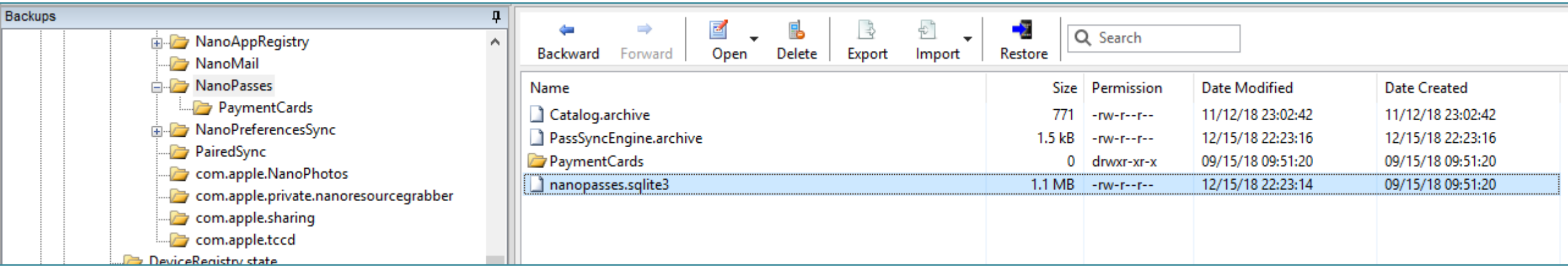
APPLE WATCH
NANOMAIL\REGISTRY.SQLITE



APPLE WATCH
NANOMAIL\REGISTRY.SQLITE

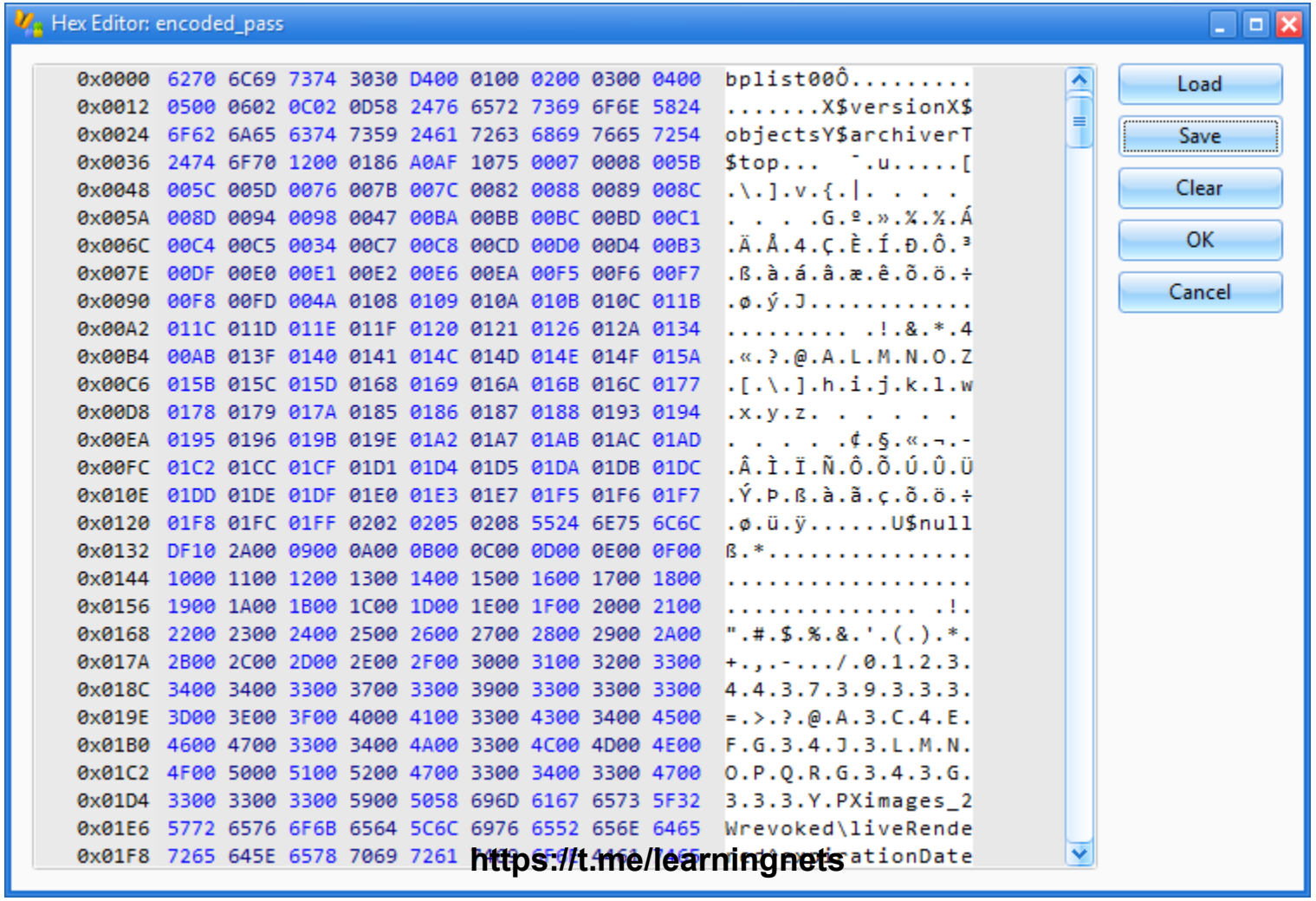


APPLE WATCH
NANOPASSES\NANOPASSES.SQLITE3

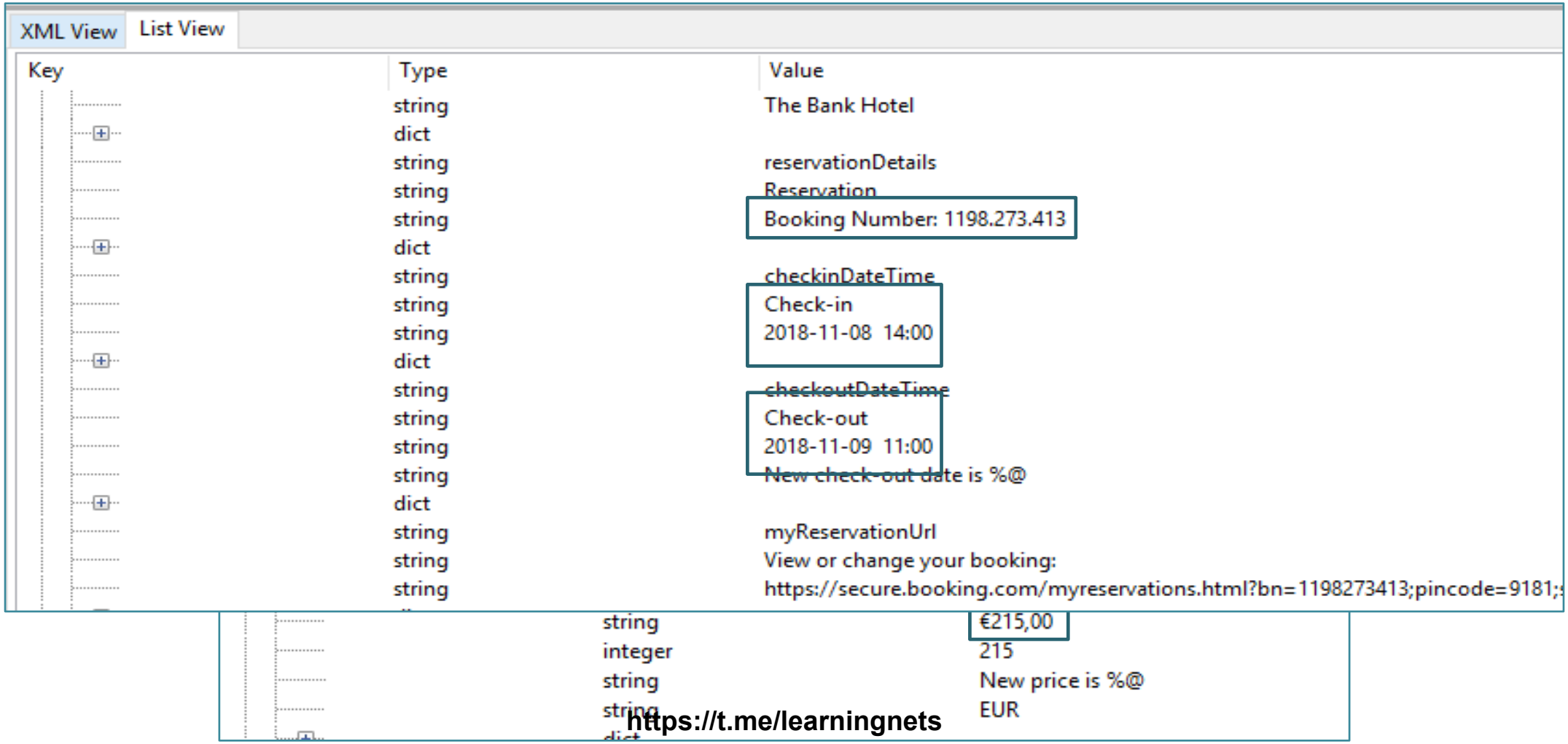


unique_id	type_id	organization_name	ingested_date	localized_description
				Click here to define a filter
Oc+NJo83fq3-17eDWmzVSyHPfzU=	pass.com.booking.reservation	Booking.com	563059511	Situato nel quartiere Jordaan di Amsterdam, il moderno Bank Hotel si trova nell'antico edificio di una ex banca sulla 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	Be[illegible]	[illegible]	[illegible]. Get. Rewarded.

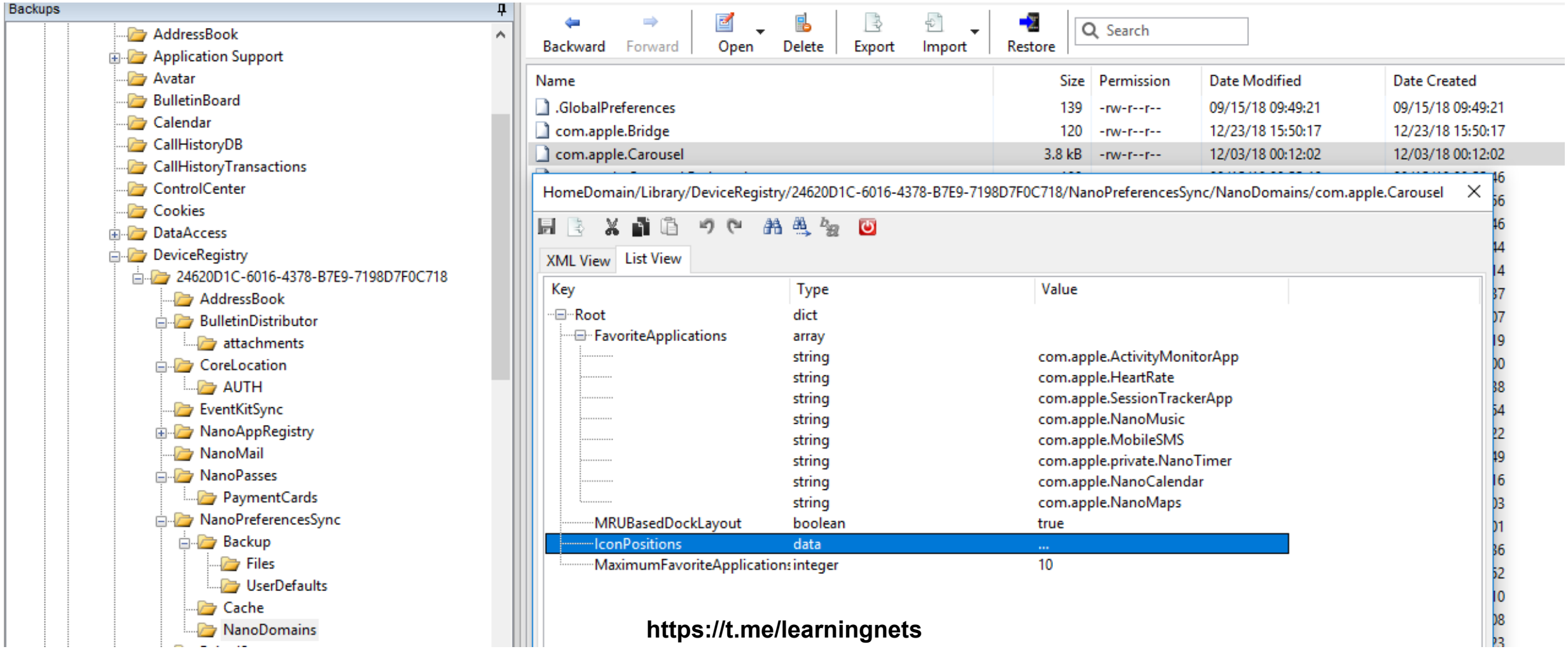
APPLE WATCH
NANOPASSES\NANOPASSES.SQLITE3



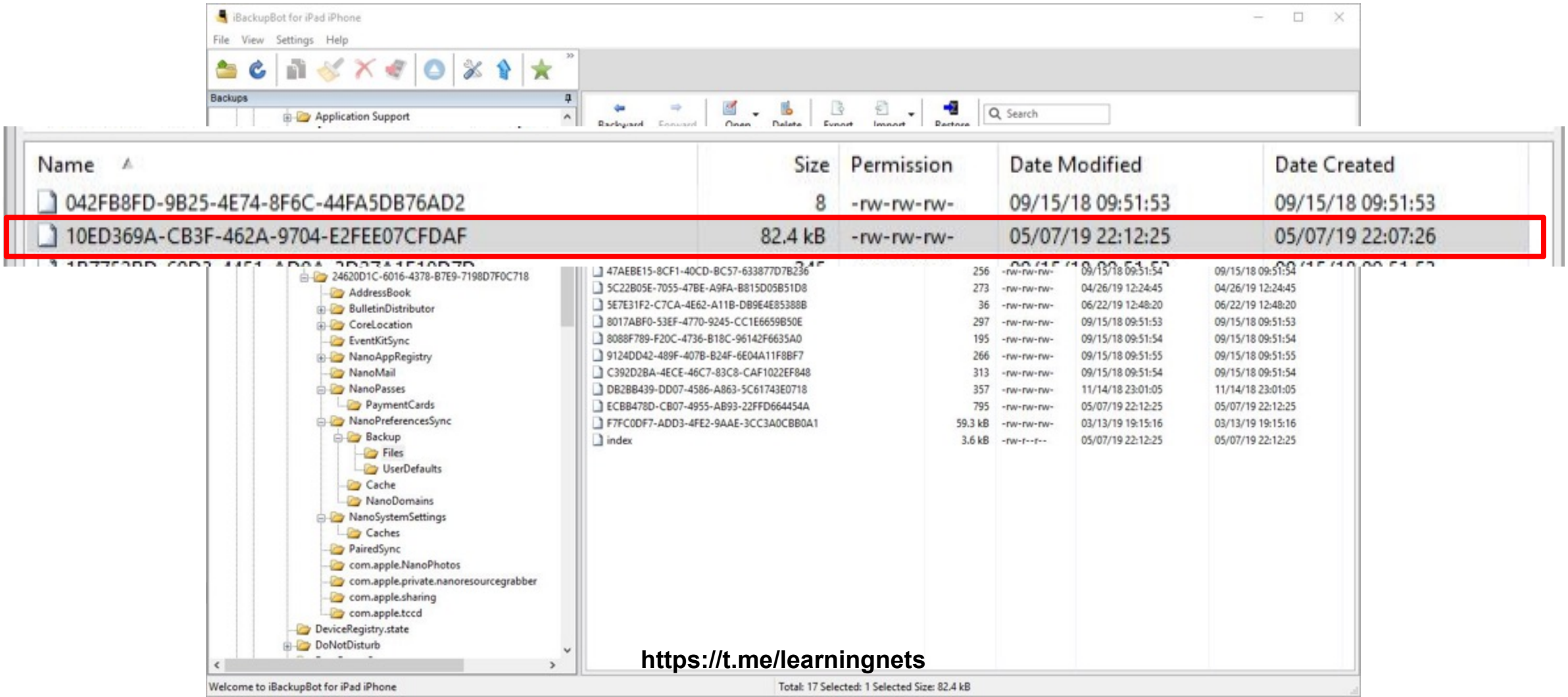
APPLE WATCH
NANOPASSES\NANOPASSES.SQLITE3



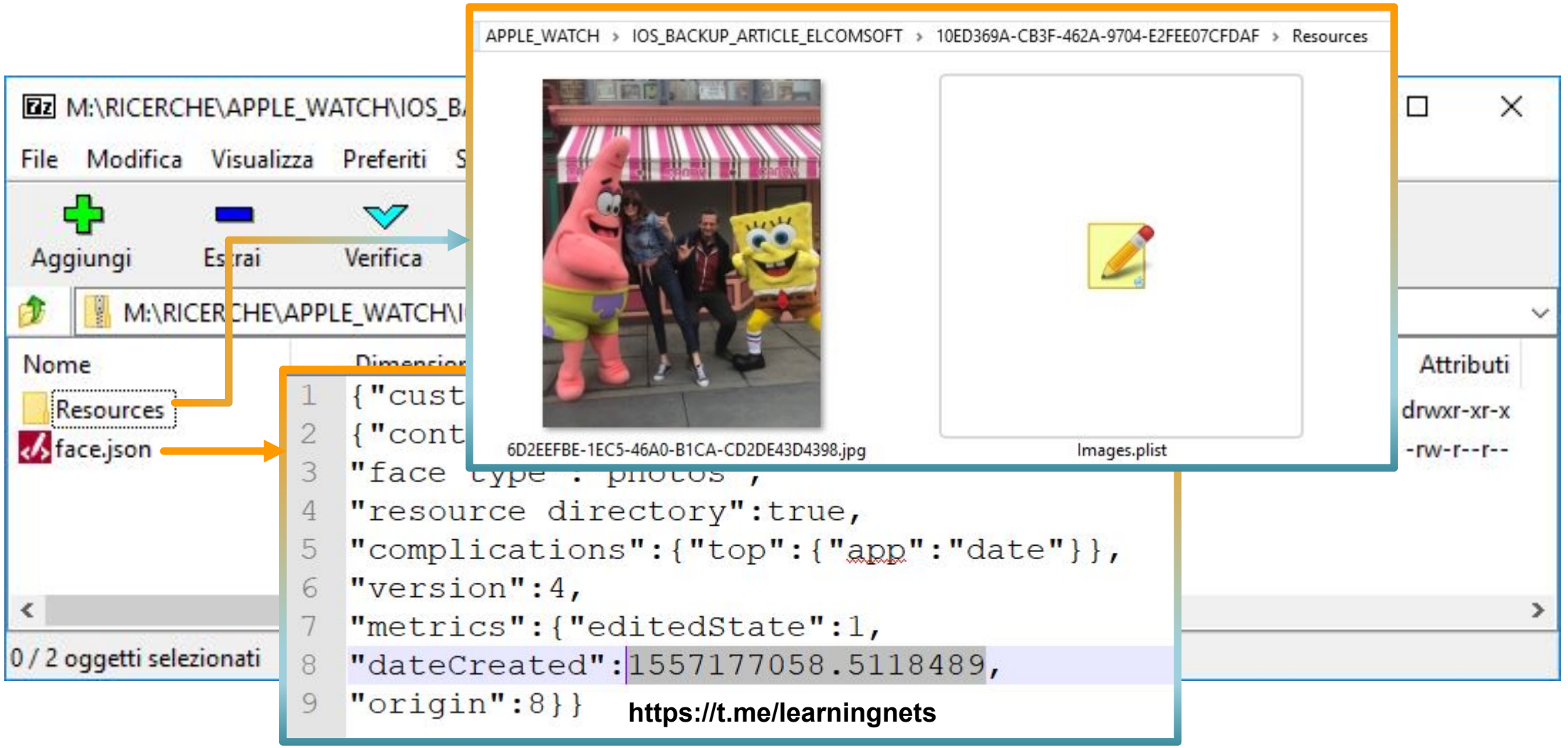
APPLE WATCH
NANOPREFERENCESSYNC/NANODOMAINS/COM.APPLE.CAROUSEL



APPLE WATCH
NANOPREFERENCESSYNC\BACKUP\FILES FOLDER



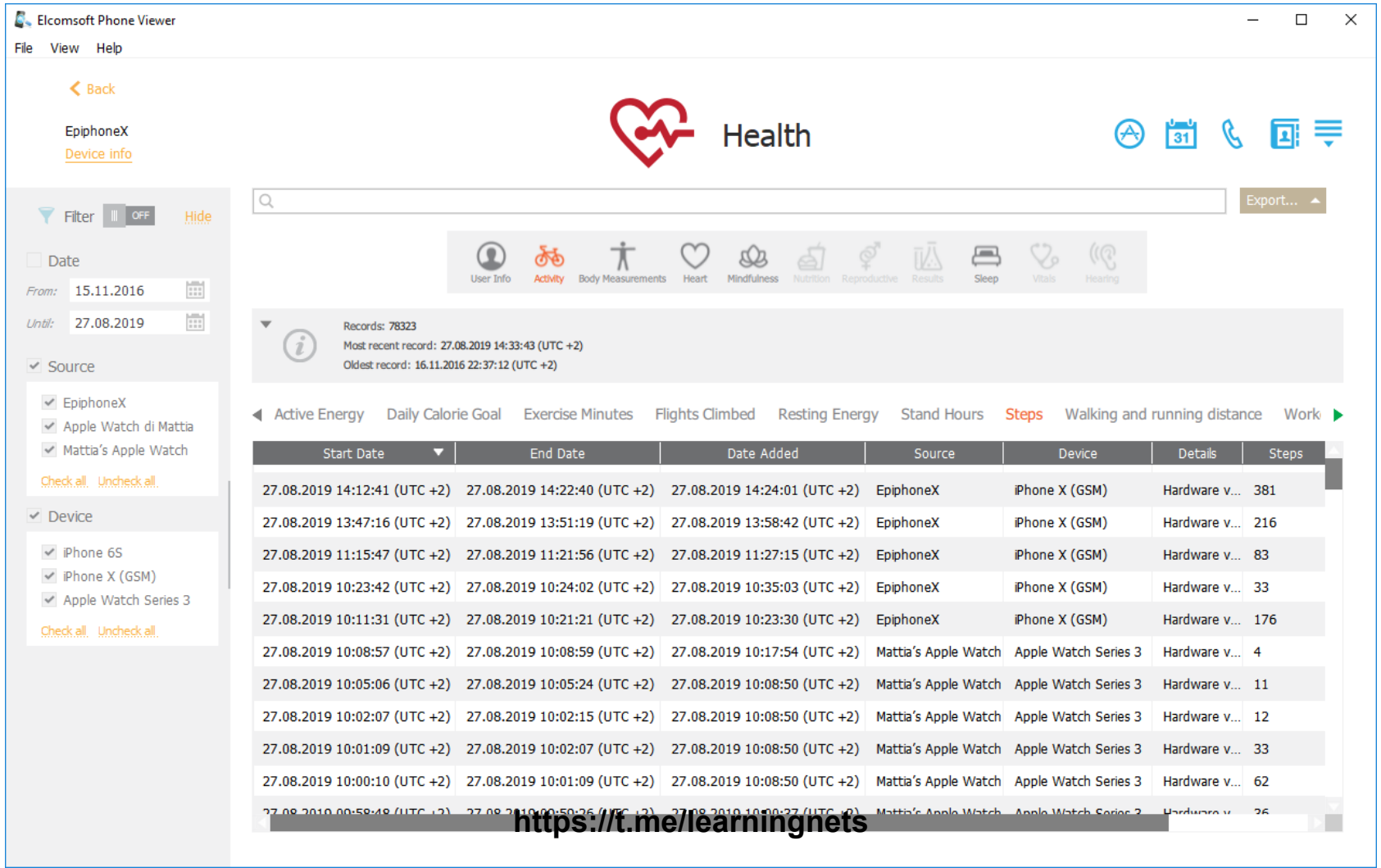
APPLE WATCH
NANOPREFERENCESSYNC\BACKUP\FILES FOLDER



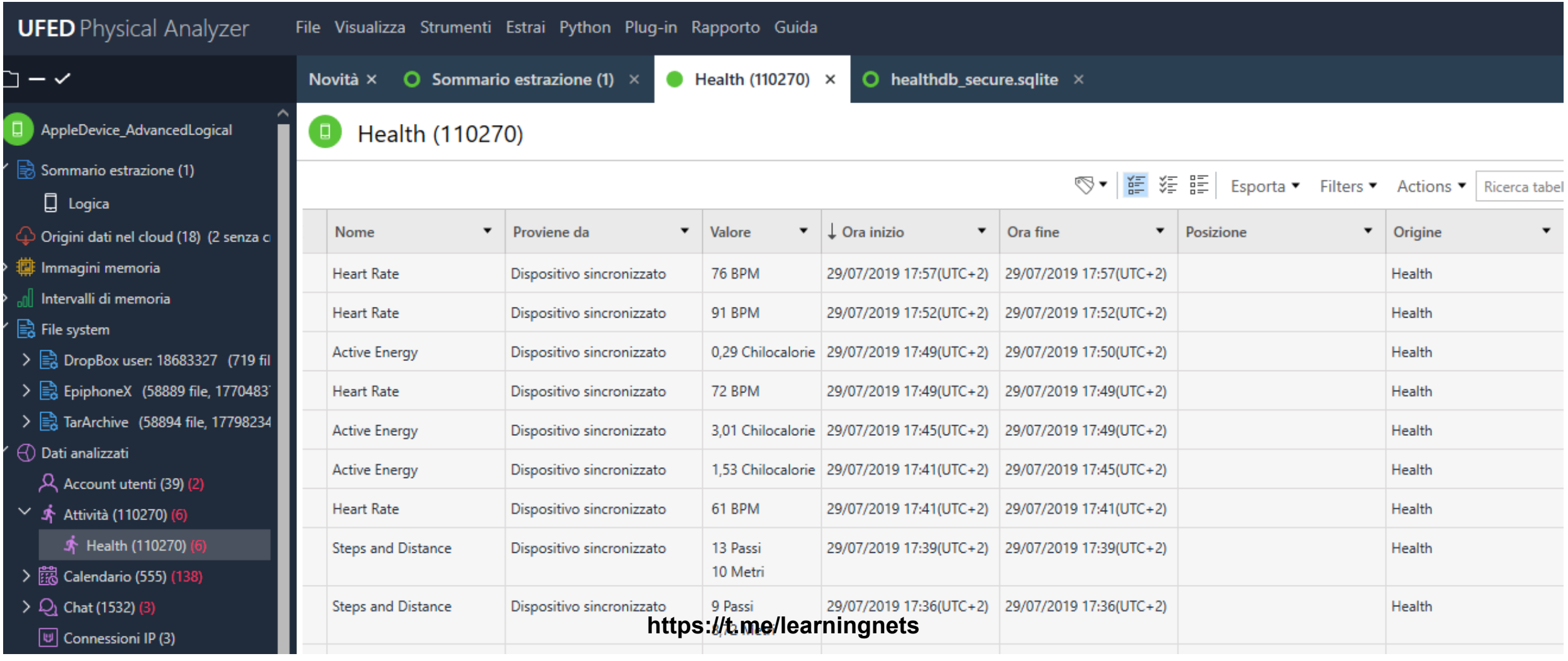
APPLE WATCH HEALTH DATA

- Apple Health was introduced by Apple in 2014 with iOS 8
- Pre-installed on all iPhones
- Support the Apple Watch for data collection
- **A Forensic Exploration of iOS Health Data**, presentation by Sarah Edwards and Heather Mahalik at DFIR US SUMMIT 2018
- **Apple Health** presentation by Vladimir Katalov at ROOTCON 20018
  https://media.rootcon.org/ROOTCON%2012/Talks/Apple%20Health.pdf
- **The iPhone Health App from a forensic perspective** by NFI (DFRWS EU 2019)
  https://www.sciencedirect.com/science/article/pii/S1742287619300313

APPLE WATCH
HEALTH DATA IN (ENCRYPTED) LOCAL BACKUP



APPLE WATCH
HEALTH DATA IN (ENCRYPTED) LOCAL BACKUP



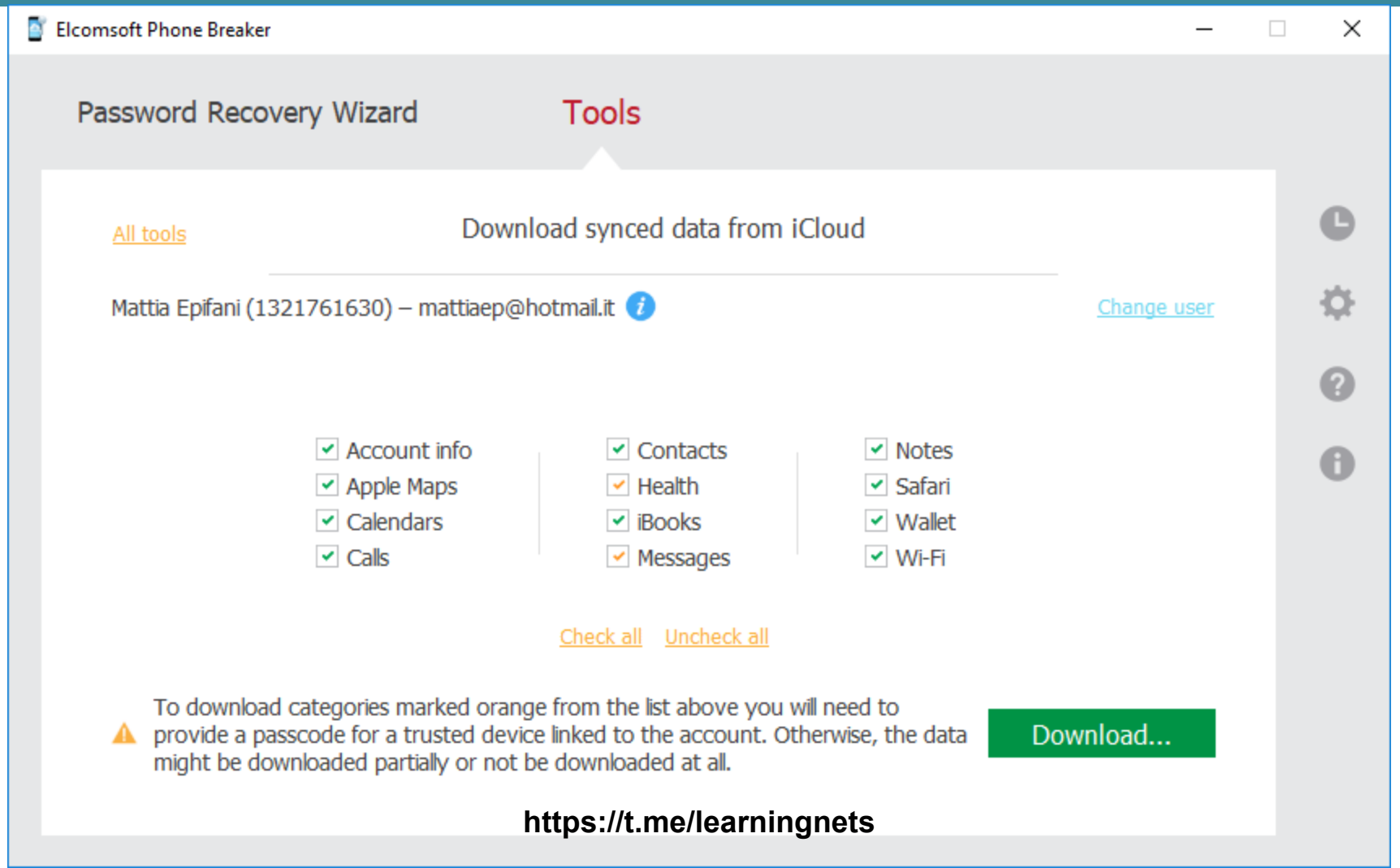
APPLE WATCH FORENSICS – SYNCED ICLOUD

MATTIA EPIFANI – FRANCESCO PICASSO

SANS DFIR EU SUMMIT

PRAGUE, 29 SEPTEMBER 2019

APPLE WATCH
HEALTH DATA SYNCED WITH THE CLOUD



APPLE WATCH FORENSICS GUIDELINES

Apple Watch 1st gen/1/2/3

1. Connect the device with MFC IBUS adapter
    1. Extract **device information**
    2. Extract data with **AFC protocol**
    3. Generate **sysdiagnose**
    4. Extract **logs**
2. Perform **manual investigation**
3. If the synced iPhone is available, **extract Watch data**
4. Eventually, **extract data from iCloud**
5. Evaluate **jailbreaking** options

Apple Watch 4

1. If the synced iPhone is available
    1. Generate **sysdiagnose**
    2. Extract **logs**
    3. Extract **device information** from the iPhone
    4. **Extract Watch data** from the iPhone
2. Perform **manual investigation**
3. Eventually, **extract data from iCloud**

APPLE WATCH USEFUL TOOLS

- **Elcomsoft iOS Toolkit** https://www.elcomsoft.com/eift.html
- **Elcomsoft Phone Breaker** https://www.elcomsoft.com/eppb.html
- **Elcomsoft Phone Viewer** https://www.elcomsoft.com/epv.html
- **Cellebrite Physical Analyzer** https://www.cellebrite.com/en/ufed-ultimate/
- **iTools** https://www.itools4.com/
- **iExplorer** https://macroplant.com/iexplorer
- **3u Tools** http://www.3u.com/
- **plist Editor for Windows** https://www.icopybot.com/plist-editor.htm
- **DB Browser for SQLite** https://sqlitebrowser.org/
- **iBackupBot** http://www.icopybot.com/itunes-backup-manager.htm
- **Jailbreak**
  - **jelbrekTime** watchOS 4.1 https://github.com/tihmstar/jelbrekTime
  - **Brenbreak** watchOS 4.0 – 5.1.2 https://please.brenbreak.today/

Q&A?

Mattia Epifani

- Digital Forensics Analyst
- CEO @ REALITY NET – System Solutions
- GCFA, GCFE, GASF, GMOB, GNFA, GREM, GCWN
- SANS Instructor, FOR585 / FOR500


mattia.epifani@realitynet.it


@mattiaep


http://www.linkedin.com/in/mattiaepifani


http://www.realitynet.it


http://blog.digital-forensics.it

Francesco Picasso

- Digital Forensics Analyst
- CTO @ REALITY NET – System Solutions
- GCFA, GCIH
- SANS Instructor, FOR508


francesco.picasso@realitynet.it


@dfirfpi


https://it.linkedin.com/in/francescopicasso


http://www.realitynet.it


http://blog.digital-forensics.it