



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](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)

<https://t.me/learningnets>

APPLE WATCH IDENTIFICATION

[HTTPS://SUPPORT.APPLE.COM/EN-US/HT204507](https://support.apple.com/en-us/HT204507)

1^o Generation

Apple Watch 1

Apple Watch 2

Ap



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

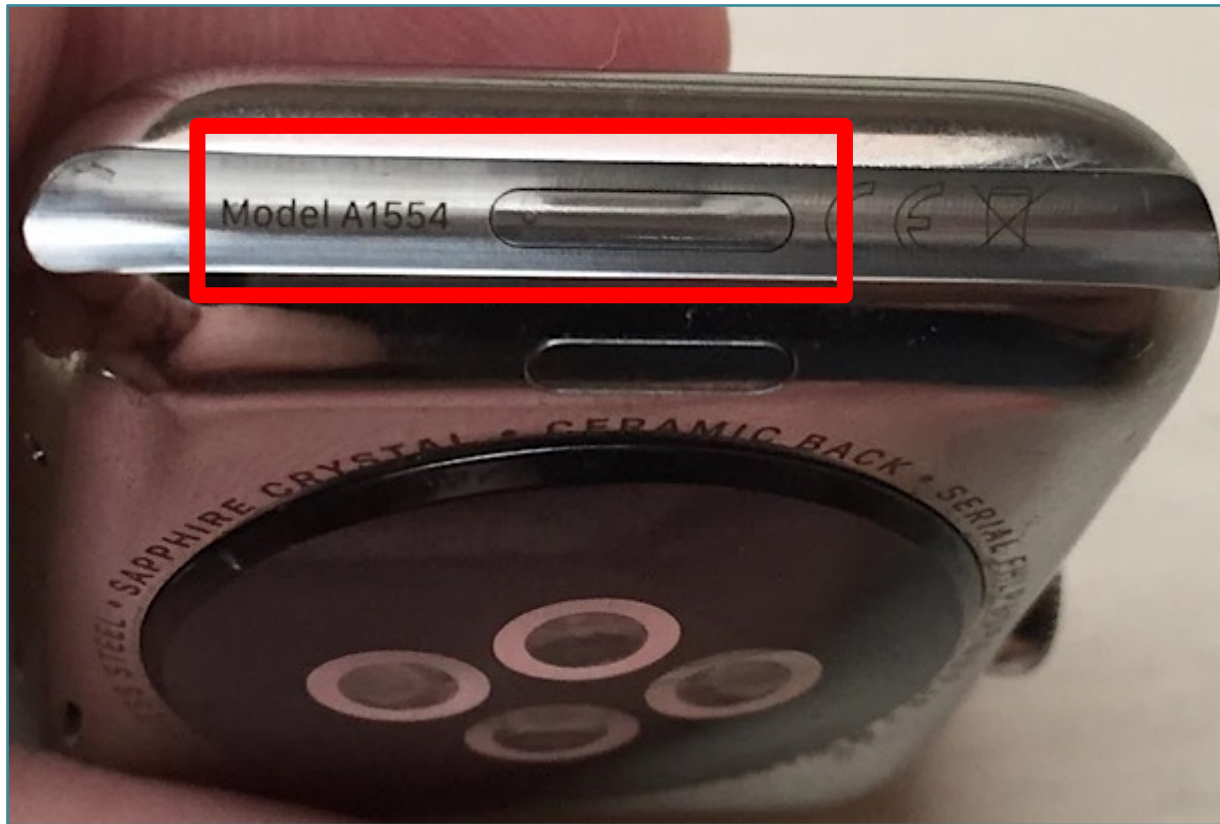
SANS DFIR EU SUMMIT

PRAGUE, 29 SEPTEMBER 2019

APPLE WATCH

THE “SECRET” (DIAGNOSTIC) PORT!

[HTTPS://WWW.IDOWNLOADBLOG.COM/2015/04/13/APPLE-WATCH-DIAGNOSTIC-PORT/](https://www.idownloadblog.com/2015/04/13/apple-watch-diagnostic-port/)



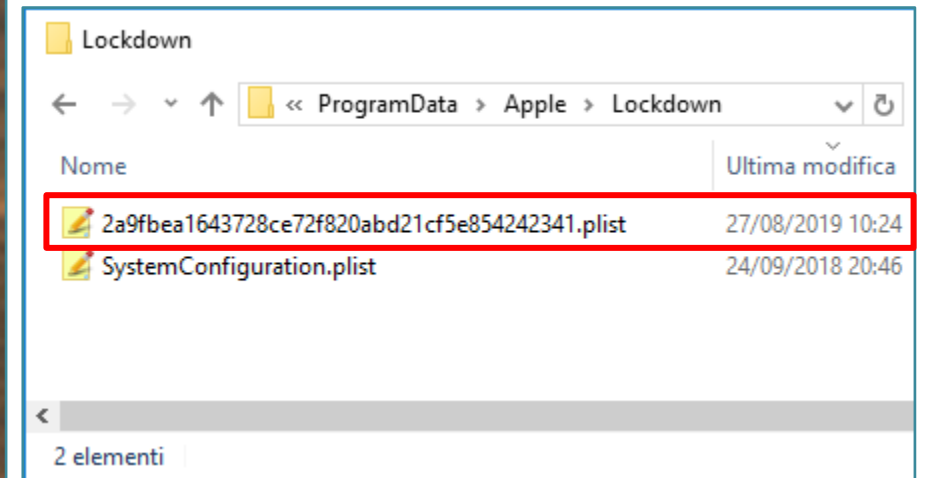
APPLE WATCH CONNECTION WITH IBUS

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



<https://t.me/learningnets>

APPLE WATCH PAIRING

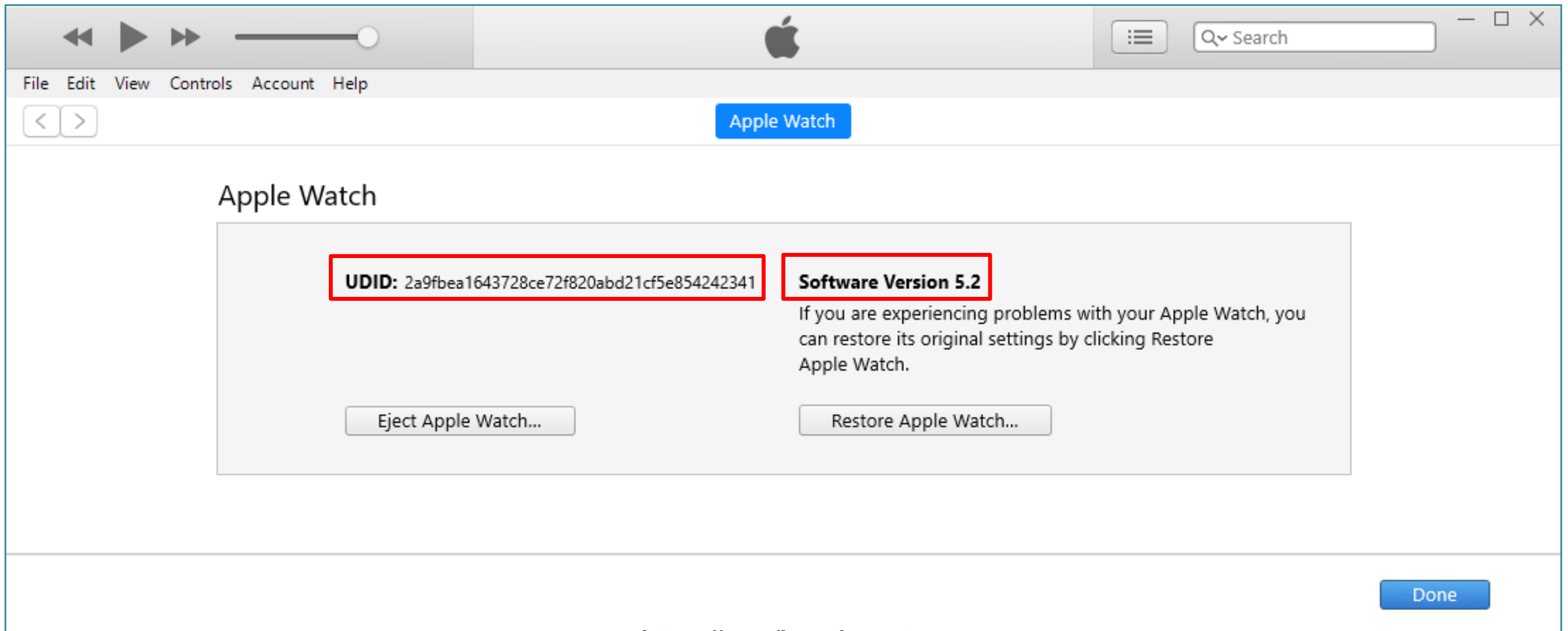


APPLE WATCH DEVICE ACQUISITION

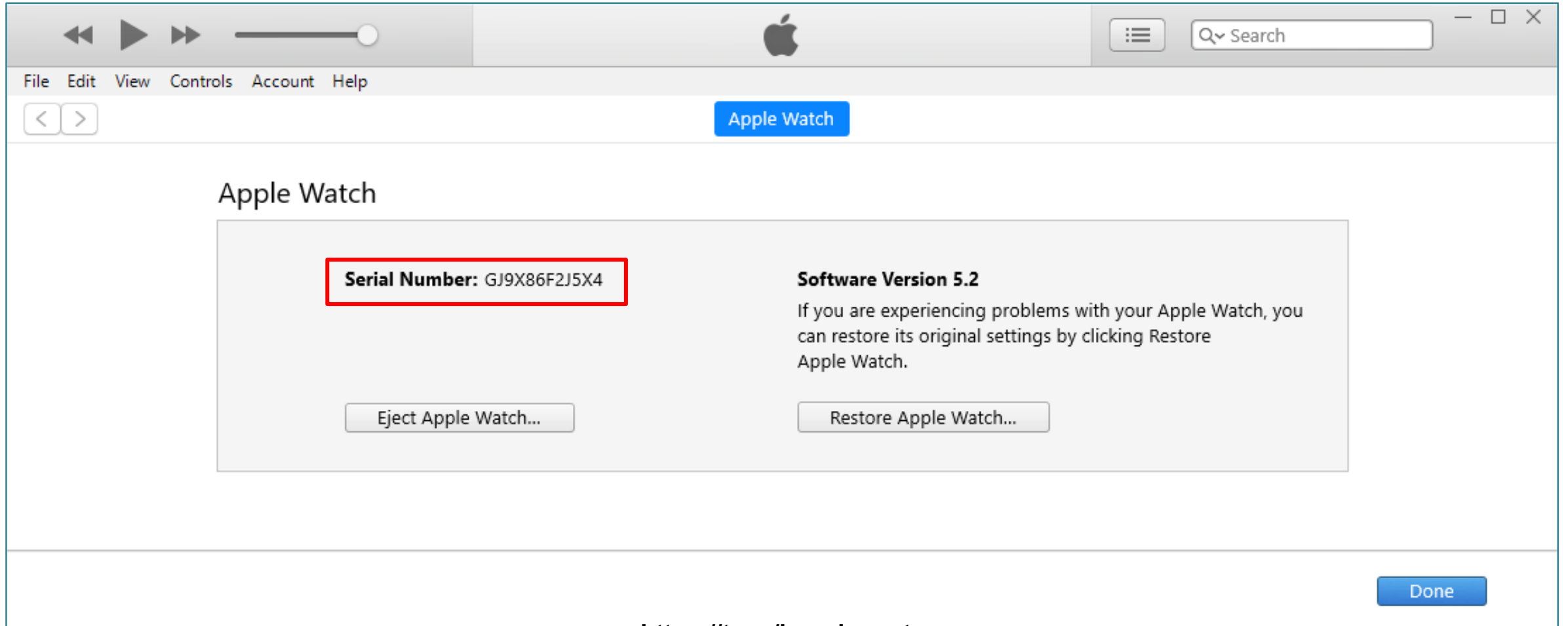
- **No backup service is running on watchOS**
- Possible acquisitions:
 - Device information and list of installed applications
 - AFC protocol (Apple File Conduit)
 - Crash logs (and sysdiagnose!)

- 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/>

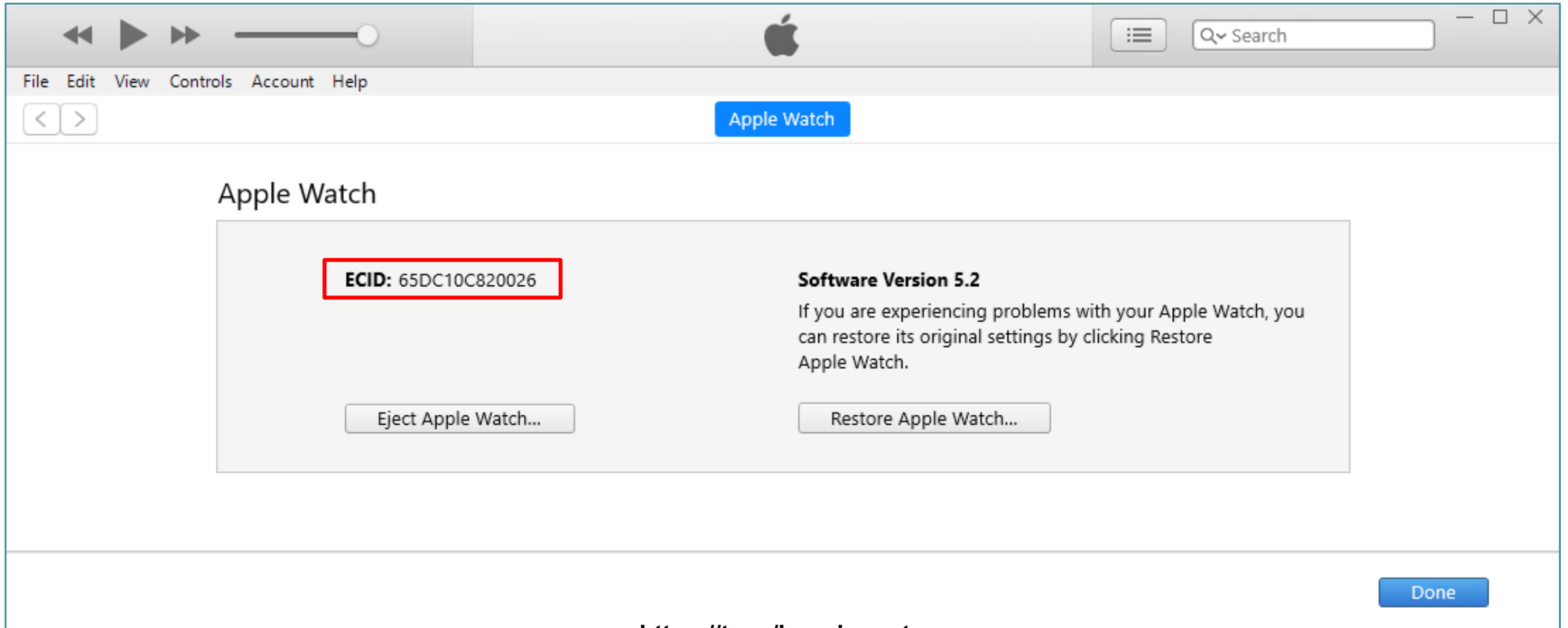
APPLE WATCH EXTRACTING BASIC DEVICE INFORMATION



APPLE WATCH EXTRACTING BASIC DEVICE INFORMATION



APPLE WATCH EXTRACTING BASIC DEVICE INFORMATION

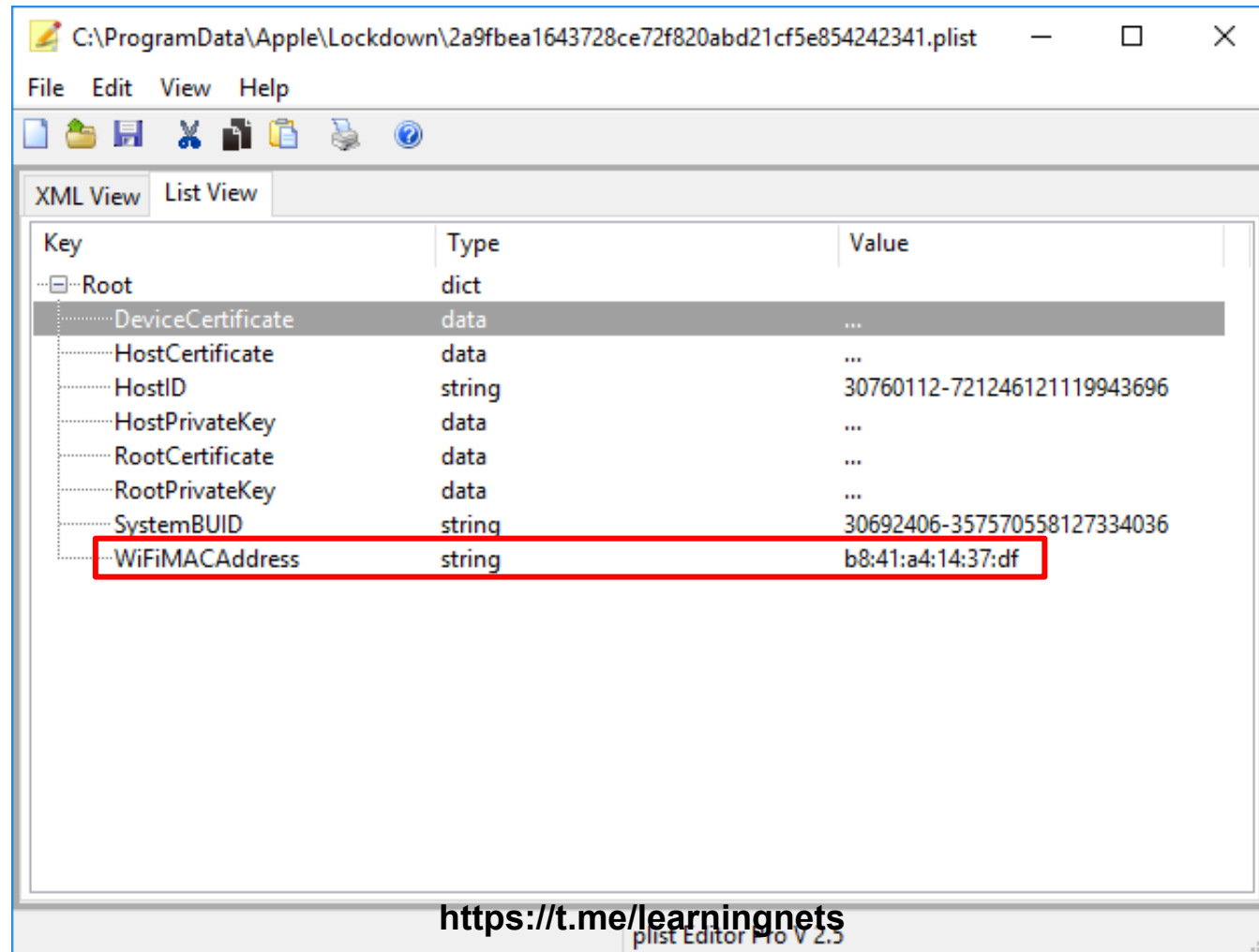


The screenshot shows the Apple Watch settings window in macOS. The window title is "Apple Watch". The main content area displays the following information:

- ECID:** 65DC10C820026 (highlighted with a red box)
- Software Version 5.2**
- Text: "If you are experiencing problems with your Apple Watch, you can restore its original settings by clicking Restore Apple Watch."
- Buttons: "Eject Apple Watch..." and "Restore Apple Watch..."

At the bottom right of the window, there is a "Done" button.

APPLE WATCH EXTRACTING BASIC DEVICE INFORMATION



The screenshot shows a window titled "C:\ProgramData\Apple\Lockdown\2a9fbea1643728ce72f820abd21cf5e854242341.plist" with a menu bar (File, Edit, View, Help) and a toolbar. The window displays a table of keys and values in a "List View" format. The "WiFiMACAddress" key is highlighted with a red box.

Key	Type	Value
Root	dict	
DeviceCertificate	data	...
HostCertificate	data	...
HostID	string	30760112-721246121119943696
HostPrivateKey	data	...
RootCertificate	data	...
RootPrivateKey	data	...
SystemBUID	string	30692406-357570558127334036
WiFiMACAddress	string	b8:41:a4:14:37:df

<https://t.me/learningnets>
plist Editor Pro V 2.3

APPLE WATCH

EXTRACTING BASIC DEVICE INFORMATION

C:\ Seleziona C:\Windows\System32\cmd.exe

```
D:\ForensicTools\Libimobiledevice>ideviceinfo -s
BoardId: 26
BuildVersion: 16T225
ChipID: 32772
DeviceClass: Watch
DeviceColor: 1
DeviceName: Mattia's Apple Watch
DieID: 1791933580181542
HardwareModel: N121bAP
PartitionType: GUID_partition_scheme
ProductName: Watch OS
ProductType: Watch3,4
ProductVersion: 5.2
ProductionSOC: true
ProtocolVersion: 2
TelephonyCapability: false
UniqueChipID: 1791933580181542
UniqueDeviceID: 2a9fbea1643728ce72f820abd21cf5e854242341
WiFiAddress: b8:41:a4:14:37:df
```

APPLE WATCH DEVICE INFORMATION (ELCOMSOFT)

```
mattiaepifani — Toolkit.command — tee - Toolkit.command — 82x34

-----
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 di Mattia
Hardware model: N121bAP
Serial number: GJ9X86F2J5X4
iOS version: 5.2
Device ID: 2a9fbea1643728ce72f820abd21cf5e854242341

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>:

Getting basic device information...

Getting installed applications list...

Getting full installed applications info...

Press 'Enter' to continue
█
```

<https://t.me/learningnets>

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
DiellD	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	

<https://t.me/learningnets>

APPLE WATCH DEVICE INFORMATION (ITOOOLS)



The screenshot displays the iTools software interface for managing an Apple Watch. The main window is titled "Mattia's Apple Watch" and shows a sidebar with navigation options: My Device, Apps, Photos, Music, Videos, Books, Info, and File Explorer. The central area is divided into two tabs: "Device Information" (selected) and "Device Verification". The "Device Information" tab displays the following details:

Device Information		Device Verification	
Device:	(8GB)	Country:	Unknown
iOS:	5.2	Accessibility:	Off Details
Activation:	Activated	Battery capacity:	60% Battery Master
IMEI:	N/A	Hard Disk Type:	MLC Hard Disk Details
Serial No.:	GJ9X86F2J5X4	Wi-Fi type:	Unknown Details
Verify UDID:	Yes	iCloud:	Off iCloud Details

At the bottom of the interface, there is a "More Info" link and a navigation bar with options: Maker, Manager, Explorer, Transfer, and Converter. A URL is visible at the bottom center: <https://t.me/learningnets>.

APPLE WATCH DEVICE INFORMATION (3UTOOLS)

3uTools www.3u.com

iDevice Apps Ringtones

Mattia's Apple Watch

- Info
- Apps (0)
- Photos
- Music
- Ringtones
- Videos
- Books
- UDisk
- Data
- Files
- More

Mattia's Apple Watch

Reboot Turn Off Refresh

Back up/Restore 3uAirPlayer

Operation Fails Frequently?

Close iTunes

8GB	Unknown	Not Charging 13%	
iOS Version	5.2 (16T225)	Apple ID Lock	N/A Online Query
Jailbroken	No Jailbreak Now	iCloud	Off Details
Activated	Yes	Prod. Date	8/26/2018
Product Type	Watch3,4 (A1859)	Warranty Date	Online Query
Sales Model	MQL12 QL/A	Sales Region	QL/A
IMEI	N/A	CPU	N/A Details
Serial No.	GJ9X86F2J5X4	Disk Type	MLC Details
ECID	00065DC10C820026	Charge Times	101 Times
Verify UDID	Yes	Battery Life	96% Details
UDID	2A9FBEA1643728CE72F820ABD21CF5E854242341		

[View Verification Report](#) [View iDevice Details](#)

System Space 3.21 GB / 3.21 GB Data Space 1.91 GB / 4.24 GB

System Free Apps Photos UDisk Used

<https://t.me/learningnets>

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	
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
CFBundleDevelopmentRegion	string	en
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)

```
mattiaepifani — Toolkit.command — tee < Toolkit.com
-----
Welcome to Elcomsoft iOS Forensic Toolki
This is driver script version 5.0/Mac for 64bit

(c) 2011-2019 Elcomsoft Co. Ltd.
-----

Device connected: Apple Watch di Mattia
Hardware model: N121bAP
Serial number: GJ9X86F2J5X4
iOS version: 5.2
Device ID: 2a9fbea1643728ce72f820abd21cf5e854242341

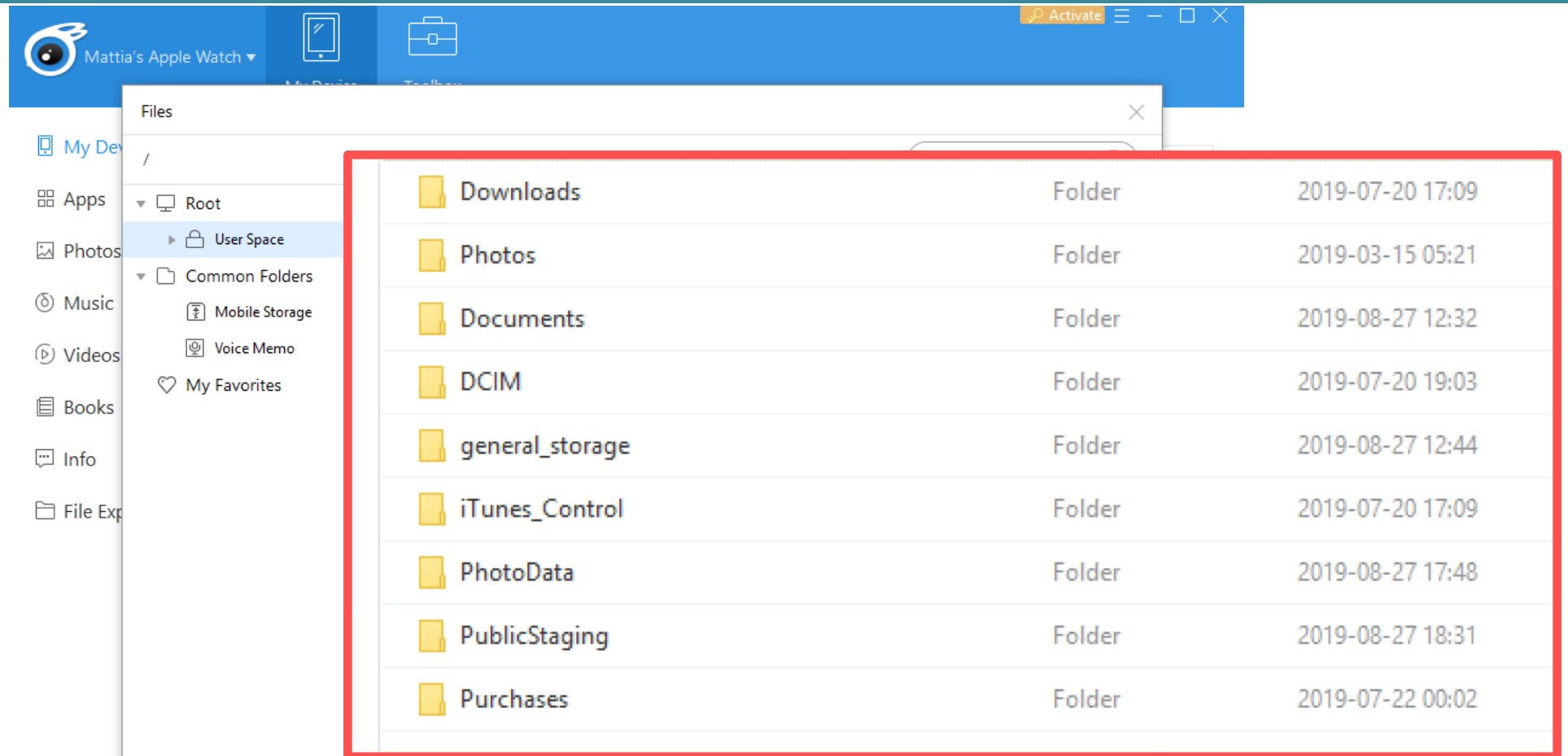
Device paired
Write copied files to directory <~/AFC>: █
```

```
mattiaepifani — Toolkit.command — tee < Toolkit.command — 82x34
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0936.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0937.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0928.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0939.JPG/5003.JPG: OK
Copying file /PhotoData/Thumbnails/V2/DCIM/100APPLE/IMG_0938.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 file /Purchases/6117677501144294588.m4a: OK
Copying file /Purchases/6117677501144294589.m4a: OK
Copying file /Purchases/6117677501144294599.m4a: OK
Copying file /Purchases/6117677501144294598.m4a: OK
Copying file /Purchases/6117677501144294595.m4a: OK
Copying file /Purchases/6117677501144294582.m4a: OK
Copying file /Purchases/6117677501144294596.m4a: OK
Copying file /Purchases/6117677501144294597.m4a: OK
Copying file /Purchases/6117677501144294587.m4a: OK
Copying file /Purchases/6117677501144294593.m4a: OK
Copying file /Purchases/6117677501144294592.m4a: OK
Copying file /Purchases/6117677501144294586.m4a: OK
Copying file /Purchases/6117677501144294590.m4a: OK
Copying file /Purchases/6117677501144294584.m4a: OK
Copying file /Purchases/6117677501144294585.m4a: OK
Copying file /Purchases/6117677501144294591.m4a: OK

Copying finished

Statistics:
Total files: 164
Copy OK: 164
Copy FAILED: 0
Press 'Enter' to continue
```

APPLE WATCH AFC ACQUISITION (ITOOOLS)



The screenshot shows the iTools interface with the 'Files' window open. The left sidebar shows the navigation pane with 'User Space' selected. The main pane displays a list of folders with their creation dates. A red box highlights the following data:

Folder Name	Type	Creation Date
Downloads	Folder	2019-07-20 17:09
Photos	Folder	2019-03-15 05:21
Documents	Folder	2019-08-27 12:32
DCIM	Folder	2019-07-20 19:03
general_storage	Folder	2019-08-27 12:44
iTunes_Control	Folder	2019-07-20 17:09
PhotoData	Folder	2019-08-27 17:48
PublicStaging	Folder	2019-08-27 18:31
Purchases	Folder	2019-07-22 00:02

<https://t.me/learningnets>

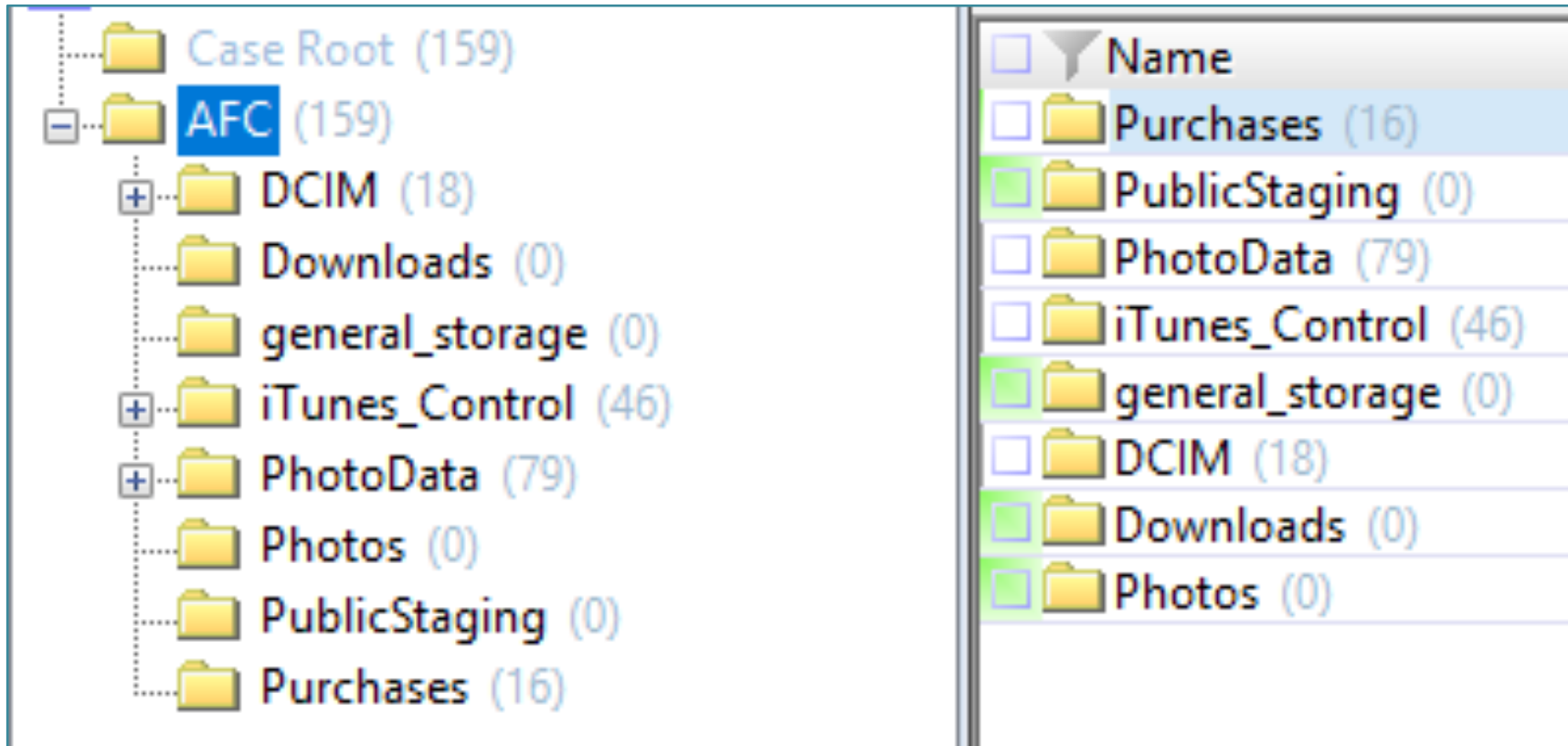
APPLE WATCH AFC ACQUISITION (3UTOOLS)

The screenshot shows the 3uTools interface for an Apple Watch. The top navigation bar includes icons for iDevice, Apps, Ringtones, Wallpapers, Flash & JB, Toolbox, and Tutorials. The left sidebar lists various categories like Info, Apps, Photos, Music, etc. The main area displays the file system of 'Mattia's Apple Watch'. A table of folders is highlighted with a red box, showing the following data:

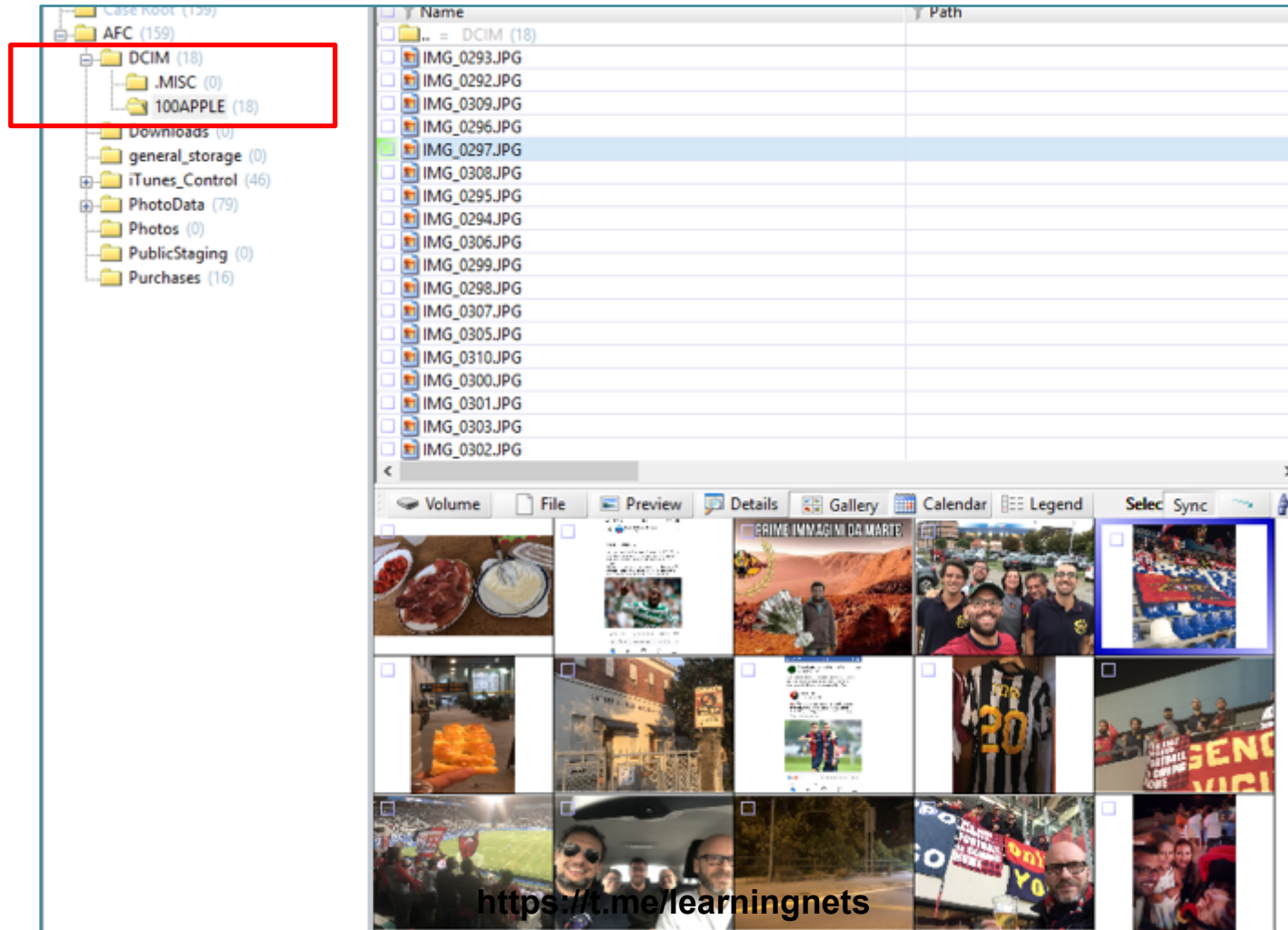
File Name	Modified Date	Type	Size
DCIM	2019-07-20 19:03:00	Folder	--
Documents	2019-08-27 12:32:13	Folder	--
Downloads	2019-07-20 17:09:48	Folder	--
iTunes_Control	2019-07-20 17:09:48	Folder	--
PhotoData	2019-08-26 20:32:04	Folder	--
Photos	2019-03-15 05:21:37	Folder	--
Purchases	2019-07-22 00:02:55	Folder	--

At the bottom of the interface, there is a status bar with 'Close iTunes', '7 items', a URL <https://t.me/learningnets>, 'V2.36', 'Feedback', and 'Check Update' buttons.

APPLE WATCH AFC ACQUISITION



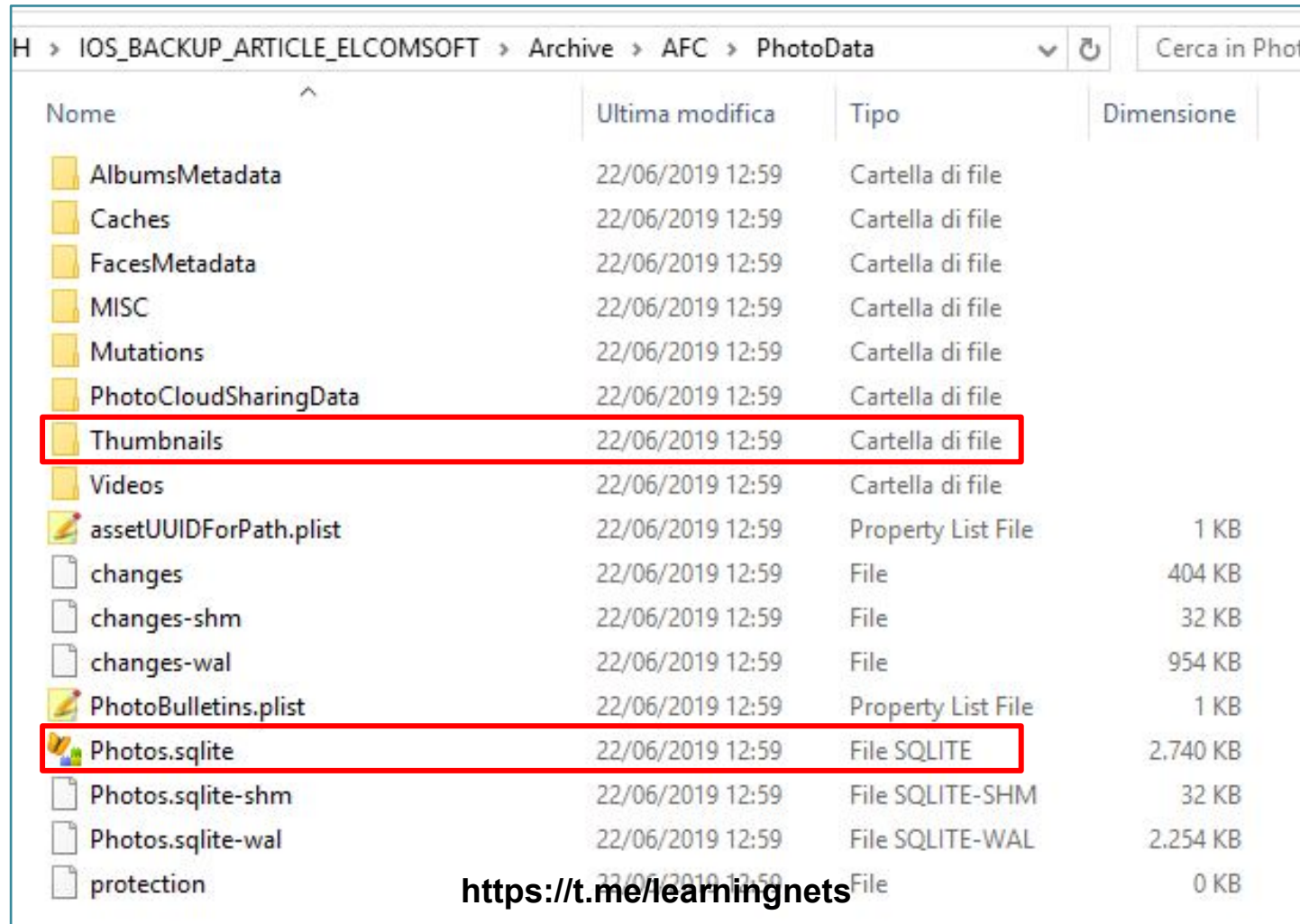
APPLE WATCH DCIM FOLDER



APPLE WATCH DCIM FOLDER

```
D:\ForensicTools\exiftool(-k).exe
ExifTool Version Number      : 10.80
File Name                    : IMG_0935.JPG
Directory                    : M:/RICERCHE/APPLE_WATCH/IOS_BACKUP_ARTICLE_ELCOMSOFT/Archive/AFC/DCIM/100APPLE
File Size                    : 110 kB
File Modification Date/Time  : 
File Access Date/Time       : 
File Creation Date/Time     : 
File Permissions             : 
File Type                    : 
File Type Extension         : 
MIME Type                    : 
Exif Byte Order              : Little-endian (Motorola)
Make                         : Apple
Camera Model Name           : iPhone X
Orientation                  : Horizontal (normal)
X Resolution                 : 72
Y Resolution                 : 72
Resolution Unit              : inches
Software                     : 12.2
Modify Date                  : 2019:05:11 18:22:12
Y Cb Cr Positioning         : Centered
Exposure Time                : 1/440
F Number                     : 1.8
Exposure Program            : Program AE
ISO                           : 20
Exif Version                 : 0221
Date/Time Original          : 2019:05:11 18:22:12
Create Date                  : 2019:05:11 18:22:12
Components Configuration    : Unknown (2)
Shutter Speed Value         : 203
Aperture Value              : 203
Brightness Value           : 0100
Exposure Compensation       : 
Metering Mode               : 
Flash                       : 
Focal Length                : 
Subject Area                : 
Run Time Flags              : 
Run Time Value              : 
Run Time Scale              : 
Run Time Epoch              : 
Acceleration Vector         : 
NDR Image Type              : Unknown (2)
Sub Sec Time Original       : 203
Sub Sec Time Digitized     : 203
Flashpix Version           : 0100
Color Space                 : Uncalibrated
Exif Image Width            : 772
Exif Image Height          : 578
Sensing Method              : One-chip color area
```

APPLE WATCH PHOTODATA FOLDER



H > IOS_BACKUP_ARTICLE_ELCOMSOFT > Archive > AFC > PhotoData

Nome	Ultima modifica	Tipo	Dimensione
AlbumsMetadata	22/06/2019 12:59	Cartella di file	
Caches	22/06/2019 12:59	Cartella di file	
FacesMetadata	22/06/2019 12:59	Cartella di file	
MISC	22/06/2019 12:59	Cartella di file	
Mutations	22/06/2019 12:59	Cartella di file	
PhotoCloudSharingData	22/06/2019 12:59	Cartella di file	
Thumbnails	22/06/2019 12:59	Cartella di file	
Videos	22/06/2019 12:59	Cartella di file	
assetUUIDForPath.plist	22/06/2019 12:59	Property List File	1 KB
changes	22/06/2019 12:59	File	404 KB
changes-shm	22/06/2019 12:59	File	32 KB
changes-wal	22/06/2019 12:59	File	954 KB
PhotoBulletins.plist	22/06/2019 12:59	Property List File	1 KB
Photos.sqlite	22/06/2019 12:59	File SQLITE	2.740 KB
Photos.sqlite-shm	22/06/2019 12:59	File SQLITE-SHM	32 KB
Photos.sqlite-wal	22/06/2019 12:59	File SQLITE-WAL	2.254 KB
protection	22/06/2019 12:59	File	0 KB

<https://t.me/learningnets>

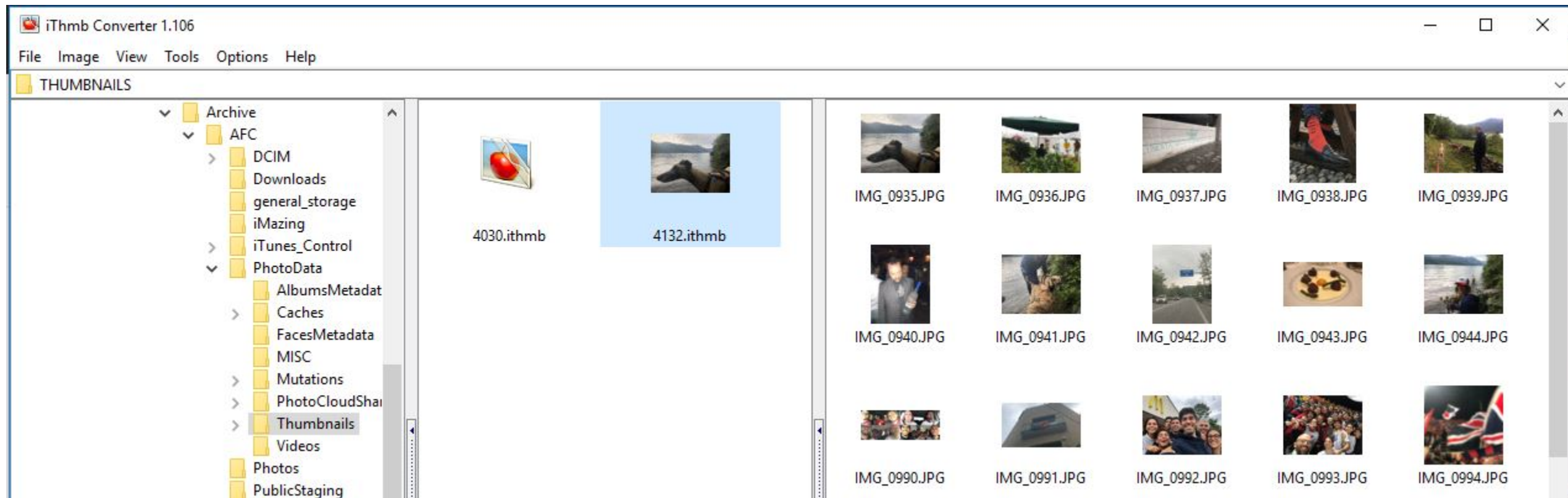
APPLE WATCH THUMBNAILS FOLDER

ACKUP_ARTICLE_ELCOMSOFT > Archive > AFC > PhotoData > Thumbnails

Nome	Ultima modifica	Tipo	Dimensione
V2	22/06/2019 12:59	Cartella di file	
4030.ithmb	22/06/2019 12:59	Apple ITHMB ima...	2.071 KB
4132.ithmb	22/06/2019 12:59	Apple ITHMB ima...	257 KB
thumbnailConfiguration	22/06/2019 12:59	File	1 KB

APPLE WATCH THUMBNAILS

[HTTP://WWW.ITTHUMBCONVERTER.COM/](http://www.itthumbconverter.com/)



<https://t.me/learningnets>

APPLE WATCH PHOTOS.SQLITE

Forensic Browser for SQLite v3.3.0 (c) Sanderson Forensics Ltd. 2018 - Licensed : ONLY for use by : Mattia Epifani - SANS Training Licence

File View Export Report Queries Search Tools Extensions About

Visual query

Main

Fields

- FROM
- ZGENERICASSET

ZCOLORSPACE

ZCOMPUTEDASSETATTRIBUTES

ZDEFERREDBUILDFACE

ZDETECTEDFACE

ZDETECTEDFACEGROUP

ZDETECTEDFACEPRINT

ZFACECROP

ZGENERICBUM

ZGENERICASSET

ZINTERNALRESOURCE

ZINTERNALRESOURCECLOUDATTRIB

ZKEYWORD

ZLEGACYFACE

ZMEDIAANALYSISASSETATTRIBUTES

ZMEMORY

ZMOMENT

ZMOMENTLIST

Output	Expression	Alias	Sort Type	Sort Order	Aggregate	Grouping	Criteria	Or...	Or...
--------	------------	-------	-----------	------------	-----------	----------	----------	-------	-------

SQL

```
1 SELECT *
2 FROM ZGENERICASSET
```

Results, Rows = 204

Enter text to search... Find Clear

ID	ZHDRGAIN	ZHIGHLIGHTCURATIONSSCORE	ZLASTSHAREDATE	ZDIRECTORY	ZFILENAME	ZLATITUDE	ZLONGITUDE	ZMODIFICATIONDATE	ZOVERALLAESTHETICSCORE	ZPROMOTIONSORE	ZSORTTOKEN	ZTRASHEDDATE	ZAVA
1,56887304782867		0		DCIM/100APPLE	IMG_0935.JPG	-180	-180	579305008.067878	0,5	0	579284532,203		
	0	0		DCIM/100APPLE	IMG_0936.JPG	-180	-180	579264407.530763	0,5	0	580756925,446156		
	0	0		DCIM/100APPLE	IMG_0937.JPG	-180	-180	579305008.059267	0,5	0	579257837,053		
	0	0		DCIM/100APPLE	IMG_0938.JPG	-180	-180	579305008.097148	0,5	0	580756928,356935		
	0	0		DCIM/100APPLE	IMG_0939.JPG	-180	-180	579877268.619892	0,5	0	580756929,332902		
	0	0		DCIM/100APPLE	IMG_0940.JPG	-180	-180	579262059.71897	0,5	0	580867495,671491		
1,56887304782867		0		DCIM/100APPLE	IMG_0941.JPG	-180	-180	579284562.581347	0,5	0	579284562,562		
	0	0		DCIM/100APPLE	IMG_0942.JPG	-180	-180	579275930.397161	0,5	0	579275930,391		
	0	0		DCIM/100APPLE	IMG_0943.JPG	-180	-180	579294942.897317	0,5	0	579294942,881		
	0	0		DCIM/100APPLE	IMG_0944.JPG	-180	-180	579299252.327268	0,5	0	580867511,251616		
	0	0		DCIM/100APPLE	IMG_0940.JPG	-180	-180	5827751485.887846	0,5	0	582683478.735399		

<Filter is Empty> Customize...

Execute SQL Create report Detach results Display all blobs as images Show Find Panel

Results, Rows = 204 Summary tables Search Results Case Log Hex

Query complete Rows returned = 204

<https://t.me/learningnets>

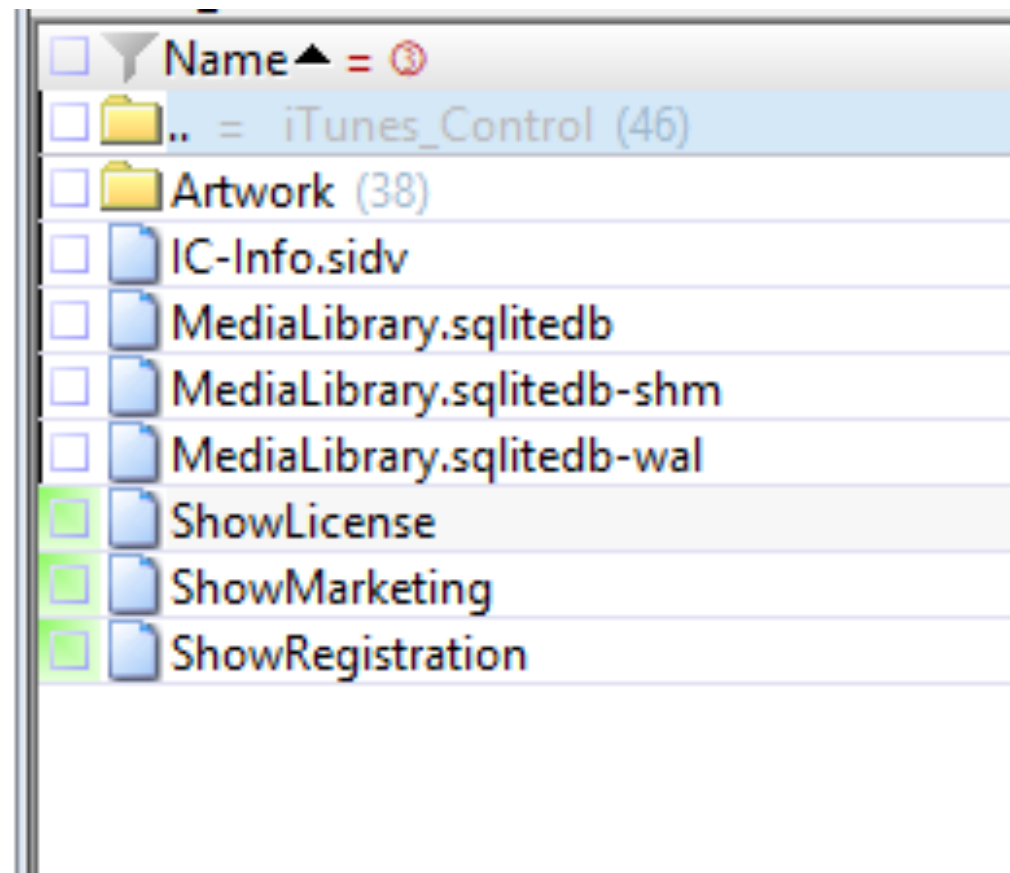
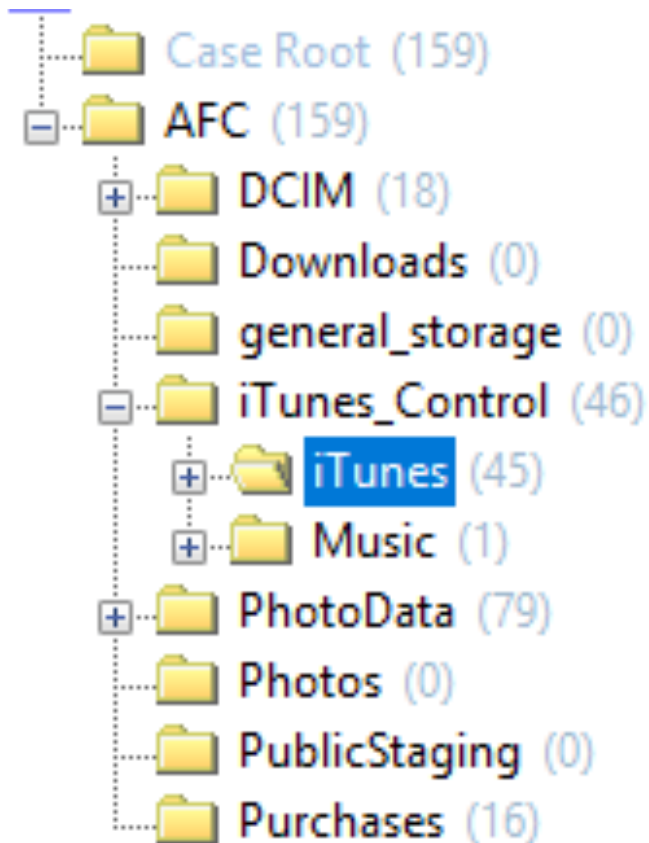
APPLE WATCH PHOTOS

```
SQL
1 | SELECT ZGENERICASSET.ZHEIGHT,
2 | ZGENERICASSET.ZWIDTH,
3 | ZGENERICASSET.ZLATITUDE,
4 | ZGENERICASSET.ZLONGITUDE,
5 | ZGENERICASSET.ZADDEDDATE,
6 | StrfTime('%Y-%m-%d %H:%M', DateTime(ZGENERICASSET.ZADDEDDATE + 978307200, 'unixepoch')) AS ZADDEDDATE_TIME,
7 | ZGENERICASSET.ZDATECREATED,
8 | StrfTime('%Y-%m-%d %H:%M', DateTime(ZGENERICASSET.ZDATECREATED + 978307200, 'unixepoch')) AS ZDATECREATED_TIME,
9 | ZGENERICASSET.ZDIRECTORY,
10 | ZGENERICASSET.ZFILENAME
11 | FROM ZGENERICASSET
```

Results, Rows = 204

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
577	768	-180	-180	580756928.000000	2019-05-28 17:22	579264405	2019-05-11 10:46	DCIM/100APPLE	IMG_0937.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	582683765.000000	2019-05-26 23:22	580596123	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

<https://t.me/learningnets>

APPLE WATCH MEDIALIBRARY.SQLITEDB

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

APPLE WATCH MEDIALIBRARY.SQLITEDB

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	61176775011 44294585.m4 a	320027	11034161	2012	1321761630	04/01/2012 02:28:06	230000997371840
29	Prisencolinensinainciusol (Remix)	1	m4a	61176775011 44294585.m4 a	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

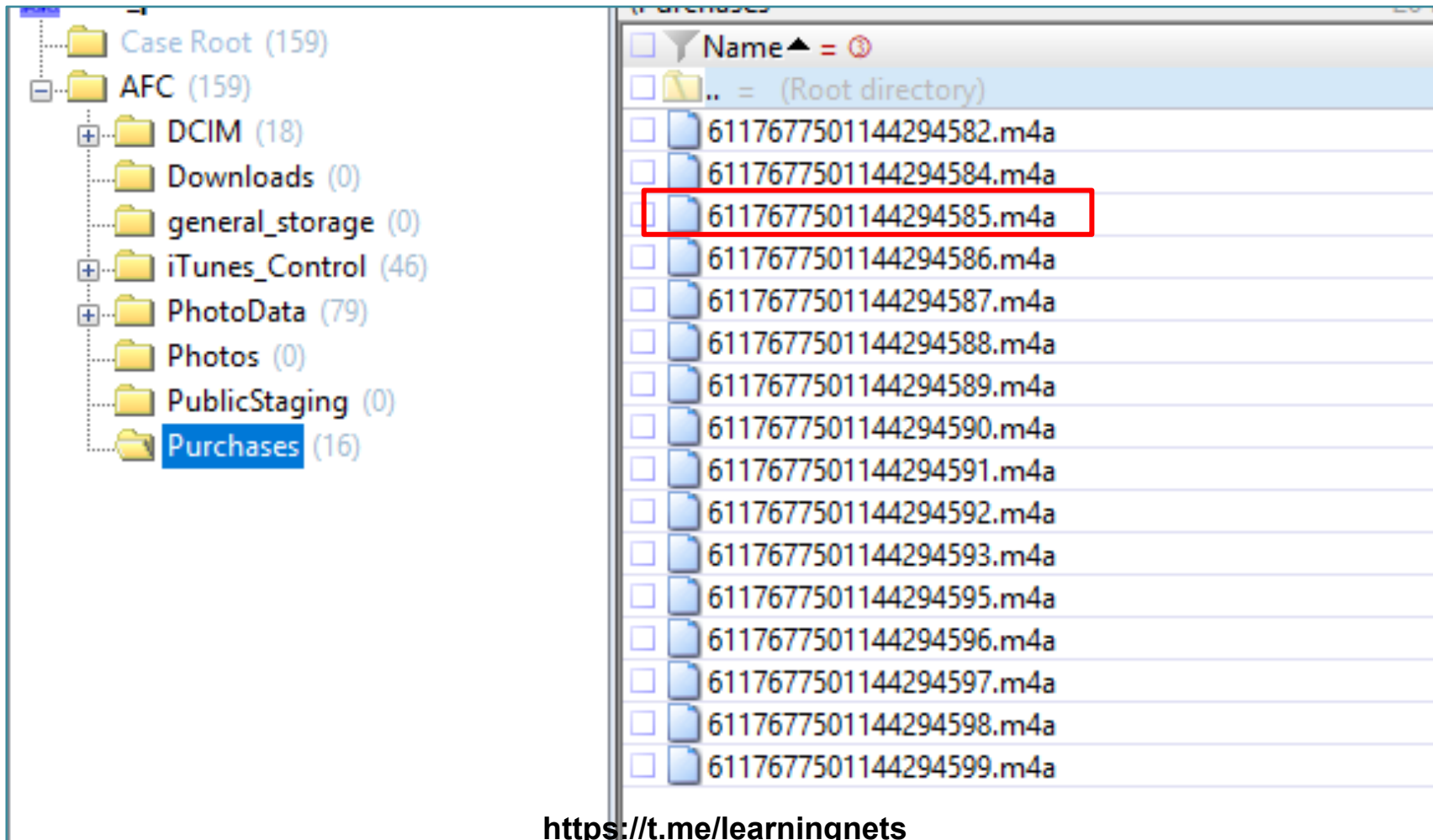
<https://t.me/learningnets>

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

<https://t.me/learningnets>

APPLE WATCH PURCHASES FOLDER



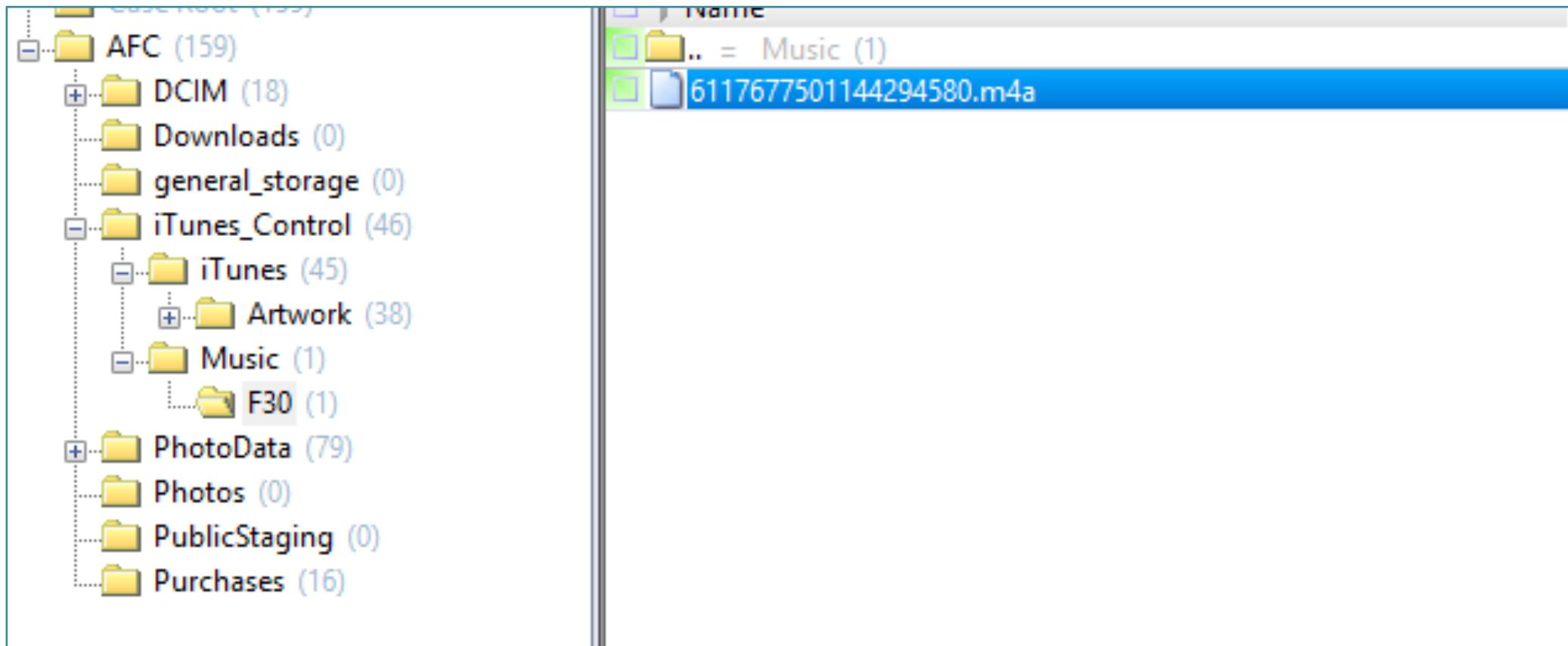
APPLE WATCH ITUNES_CONTROL/ITUNES/ARTWORK/ORIGINALS

The screenshot shows a file explorer window with a sidebar on the left and a main pane on the right. The sidebar displays a hierarchical tree view of the file system, with the path `Case Root (159) > AFC (159) > iTunes_Control (46) > iTunes (45) > Artwork (38) > Originals (6)` selected. The main pane shows a list of files with columns for Name and Partial path. The files listed are:

Name	Partial path
.. = Artwork (38)	
21ce1ad80a9560f5f8e86a541964e6d1d5f0b8	
461aa8373db3866fd357fdaf175c9168a02655	
b82609c01974d33bd7a33d5d59bc2c741fc435	
94701b49a57ffb13f271911465878507fa9278	
68e3f853d406a7056631bbb02e18a97fc78387	
61491a0a63a99d040c0a28490fae002982c279	

At the bottom of the window, a toolbar contains icons for Volume, File, Preview, Details, Gallery, Calendar, Legend, Select, and Sync. Below the toolbar, a row of album art thumbnails is visible, including one for Celentano and another for Adriano Celentano. A watermark <https://t.me/learnings> is overlaid on the bottom of the image.

APPLE WATCH ITUNES_CONTROL/MUSIC



APPLE WATCH LOGS ACQUISITION (ELCOMSOFT)

```
mattiaepifani — Toolkit.command — tee • Toolkit.command — 82x34

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

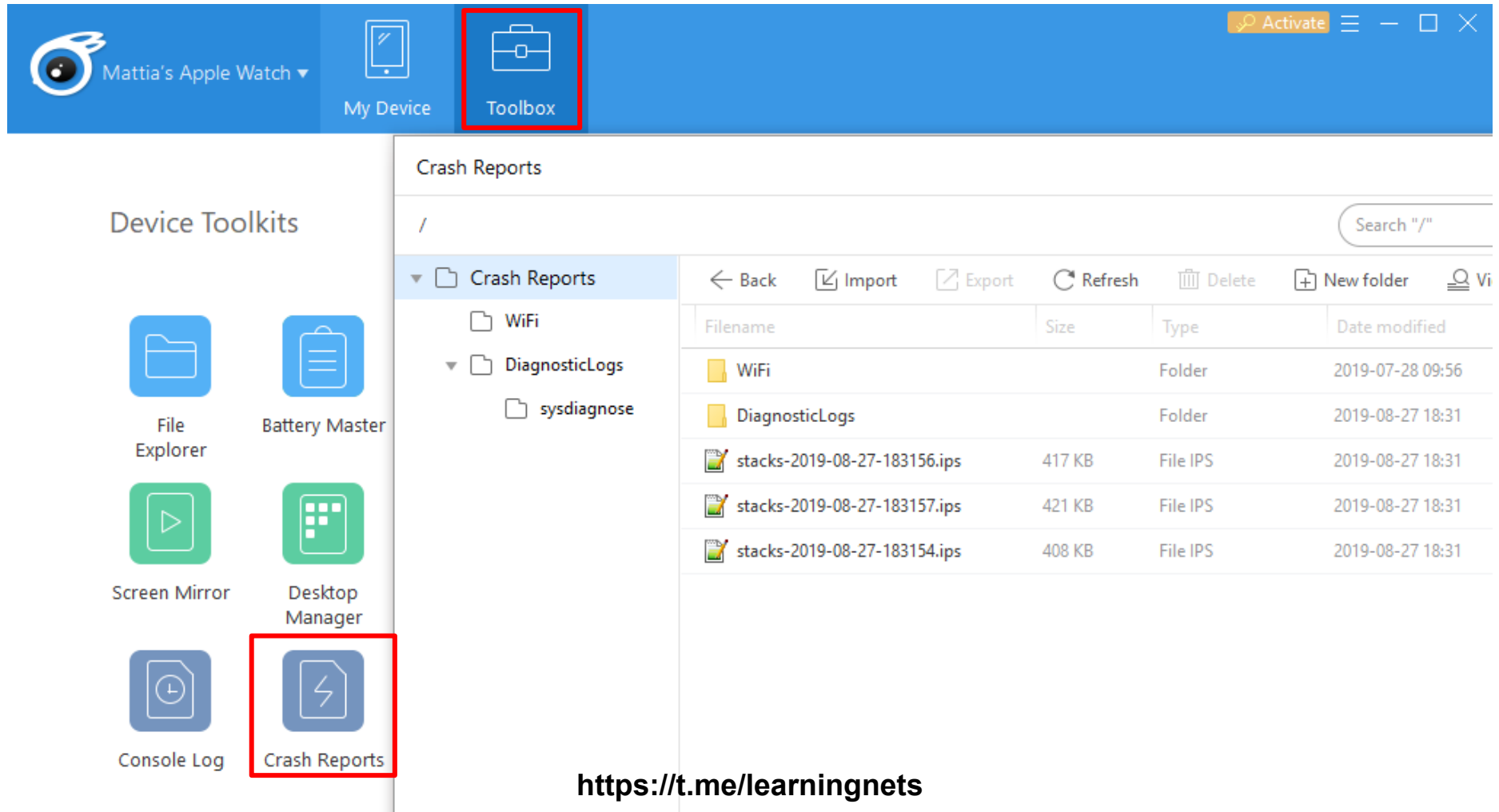
(c) 2011-2019 Elcomsoft Co. Ltd.
-----

Device connected: Apple Watch di Mattia
Hardware model: N121bAP
Serial number: GJ9X86F2J5X4
iOS version: 5.2
Device ID: 2a9fbea1643728ce72f820abd21cf5e854242341

Device paired
[Write copied files to directory <~/Logs>:
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Metadata/system.plist
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Metadata/capture.plist
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/IOReporters.xml
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.iokit.IO80211Family/IO80211AWDLPeerManager/[2019-06-22_12,56,10.864410]-io80211Family-001.pcapng.gz
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.iokit.IO80211Family/OneStats/[2019-06-22_12,52,12.051636]-CCIOReporter-001.xml.gz
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.iokit.IO80211Family/AssociationEventHistory/AssociationHistory.xml
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.iokit.IO80211Family/ControlPath/[2019-06-22_12,56,10.761451]-ControlPath-001.pcapng.gz
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.driver.ACiWiFiDriver/StateSnapshots/CoreState.txt
```

<https://t.me/learningnets>

APPLE WATCH LOGS ACQUISITION (ITOOOLS)



Mattia's Apple Watch ▾ My Device **Toolbox** Activate

Device Toolkits

- File Explorer
- Battery Master
- Screen Mirror
- Desktop Manager
- Console Log
- Crash Reports**

Crash Reports

/ Search "/"

Back Import Export Refresh Delete New folder Vi

Filename	Size	Type	Date modified
WiFi		Folder	2019-07-28 09:56
DiagnosticLogs		Folder	2019-08-27 18:31
sysdiagnose		Folder	
stacks-2019-08-27-183156.ips	417 KB	File IPS	2019-08-27 18:31
stacks-2019-08-27-183157.ips	421 KB	File IPS	2019-08-27 18:31
stacks-2019-08-27-183154.ips	408 KB	File IPS	2019-08-27 18:31

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](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 to transfer the profile to the iPhone.

2. Tap the profile in the body of the email.
3. Choose 'Apple Watch' when prompted.
4. Tap Install (enter passcode, if prompted), agree to the terms and conditions.
5. Reproduce the issue.
6. Trigger a sysdiagnose by pressing and holding the side button 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.

<https://t.me/learningnets>

APPLE WATCH SYSDIAGNOSE

H > IOS_BACKUP_ARTICLE_ELCOMSOFT > Archive > Logs > DiagnosticLogs > sysdiagnose > sysdiagnose_2019.06.22_12-55-36+0200_Watch_OS_Watch_16T225

Nome	Ultima modifica	Tipo	Dimensione
ASPSnapshots	22/06/2019 15:43	Cartella di file	
crashes_and_spins	22/06/2019 15:43	Cartella di file	
errors	22/06/2019 15:43	Cartella di file	
ioreg	22/06/2019 15:43	Cartella di file	
logs	22/06/2019 15:43	Cartella di file	
PaxHeader	22/06/2019 15:43	Cartella di file	
Preferences	22/06/2019 15:43	Cartella di file	
summaries	22/06/2019 15:43	Cartella di file	
system_logs.logarchive	22/06/2019 15:43	Cartella di file	
WiFi	22/06/2019 15:43	Cartella di file	
apfs_stats.txt	22/06/2019 12:56	File TXT	10 KB
disks.txt	22/06/2019 12:55	File TXT	1 KB
error_log.txt	22/06/2019 12:55	File TXT	0 KB
hidutil.plist	22/06/2019 12:55	Property List File	278 KB
microstackshots	22/06/2019 12:56	File	62 KB
mount.txt	22/06/2019 12:55	File TXT	1 KB
oslog_archive_error.log	22/06/2019 12:56	File LOG	1 KB
pcstatus.txt	22/06/2019 12:56	File TXT	36 KB
ps.txt	22/06/2019 12:55	File TXT	26 KB
ps_thread.txt	22/06/2019 12:55	File TXT	84 KB
smcDiagnose.txt	22/06/2019 12:55	File TXT	1 KB
spindump-nosymbols.txt	22/06/2019 12:55	File TXT	821 KB
sysdiagnose.log	22/06/2019 12:56	File LOG	102 KB
taskinfo.txt	22/06/2019 12:55	File TXT	1 KB
taskSummary.csv	22/06/2019 12:56	File con valori sep...	8 KB
...	22/06/2019 12:55	File TXT	6 KB

APPLE WATCH MOBILE ACTIVATION LOGS

```
sysdiagnose — -bash — 153x55
[MacBook-Air-di-Mattia:sysdiagnose mattiaepifani$ python3 sysdiagnose-mobileactivation.py -i ../../../../Desktop/Sysdiagnose\ test/sysdiagnose_2019.06.22_12-]
55 26:0200 Watch_OS Watch_16T225 (/logs/MobileActivation/mobileactivation_log_0

sysdiagnose — -bash — 153x29
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
3 May 2019 21:52:33 Mobile Activation Product Type = Watch3,4
3 May 2019 21:52:33 Mobile Activation Device Class = Watch

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

```
sysdiagnose — -bash — 153x13
[MacBook-Air-di-Mattia:sysdiagnose mattiaepifani$ python3 sysdiagnose-mobilecontainermanager.py -i
22_12-55-36+0200_Watch_OS_Watch_16T225/logs/MobileContainerManager/containermanagerd.log.0
Running sysdiagnose-mobilecontainermanager.py v2019-05-05 Initial Version

2 Oct 2018 14:35:03 Removed group.ph.telegra.Telegraph [line 44]
8 Nov 2018 01:52:14 Removed group.com.airbnb.shared [line 69]
13 Nov 2018 08:28:34 Removed group.com.agilebits.onepassword [line 89]
28 Feb 2019 22:29:57 Removed group.com.tencent.xin [line 142]
30 Apr 2019 17:12:59 Removed group.com.tencent.xin [line 186]

Found 5 group removal entries

MacBook-Air-di-Mattia:sysdiagnose mattiaepifani$
```

APPLE WATCH MOBILE INSTALLATION

[HTTPS://ABRIGNONI.BLOGSPOT.COM](https://abrignoni.blogspot.com)

```
MacBook-Air-di-Mattia  
  
iOS Mobile Installation  
By: @AlexisBrignoni  
Web: abrignoni.com  
  
Logs processed: 2  
Lines processed: 253  
  
Total apps: 29  
Total installed apps:  
Total uninstalled apps:  
Total historical apps:  
Total system state ev  
MacBook-Air-di-Mattia
```

DB Browser for SQLite - /Users/mattiaepifani/Desktop/Sysdiagnose test/sysdiagnose_2019.06.22_12-55-36+0

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragmas Execute SQL

Table: dimm

New Record Delete Record

	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.reisplannerextra.watchkitapp	
21	2019-06-22 07:53:00	Data container moved	com.facebook.Messenger.watchkitapp	/private/var/mobile/Contain

<https://t.me/learningnets>

APPLE WATCH POWER LOGS

[HTTPS://GITHUB.COM/MAC4N6/APOLLO](https://github.com/MAC4N6/APOLLO)

```
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
```

<https://t.me/learningnets>

APPLE WATCH POWER LOGS

[HTTPS://GITHUB.COM/MAC4N6/APOLLO](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 /I
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 /I
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 /I
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 /I
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_ /I
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_ /I
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 /I
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 /I
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 /I
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 /I
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_ /I
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_ /I
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_SCRE /I
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_ /I
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 /I
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 /I
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 /I
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 /I
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, /I
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_ /I
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 /I
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, /I

<https://t.me/learningnets>

APPLE WATCH POWER LOGS

[HTTPS://GITHUB.COM/MAC4N6/APOLLO](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_TII /
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_SCREEE /
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: 69.9999988079] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 1970-10-07 07:16:28] [OFFSET_TIMEST, /

<https://t.me/learninghats>

APPLE WATCH POWER LOGS

[HTTPS://GITHUB.COM/MAC4N6/APOLLO](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 /I
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/I
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_TIP/I
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_SCREEE/I
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/I
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/I
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/I
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_/I
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_/I
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/I
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/I
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/I
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/I
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_/I
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_/I
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] [SCREENV
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] [SCREENV
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] [H
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

<https://t.me/learningnets>

APPLE WATCH WIFI LOGS

.....BSSID	string	80:2a:a8:1a:3:e9
.....IS_NETWORK_EAP	boolean	false
.....AP_MODE	integer	2
.....USER_ROLE	integer	1
.....ORIG_AGE	integer	193
.....WEP	boolean	false
.....CHANNEL	integer	6
.....QBSS_LOAD_IE	dict	
.....FT_ENABLED	boolean	true
.....Strength	real	0.441479
.....RATES	array	
.....FT_CAPS_IE	dict	
.....networkUsage	real	12177.636478
.....EXT_CAPS	dict	
.....ScaledRSSI	real	0.441479
.....enabled	boolean	true
.....AGE	integer	193
.....knownBSSUpdatedDate	date	2019-05-30 17:14:56
.....IS_NETWORK_APPBASED	boolean	false
.....FAST_ENTERPRISE_NETWORK_SUPPORTED_DEVICE	boolean	true
.....GUESSED_2ghzBSSID1	string	82:2a:a8:1b:3:e8
.....SSID	data	...
.....networkKnownBSSLListKey	array	
.....CaptiveNetwork	boolean	false
.....IS_NETWORK_CONFIGURED	boolean	false
.....SHARE_MODE	integer	3
.....WiFiManagerKnownNetworksEventType	integer	3
.....lastAutoJoined	date	2019-05-30 17:07:06

<https://t.me/learningnets>

APPLE WATCH WIFI LOGS



Stats Tools

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

SSID / Network Name (exact match): foobar

SSID / Network Name (wildcards¹: % and _): foobar%

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.

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	2016-09-23T00:00:00	2018-01-01T00:00:00		43.79183578	11.22836018	6	0	2

<https://t.me/learningnets>

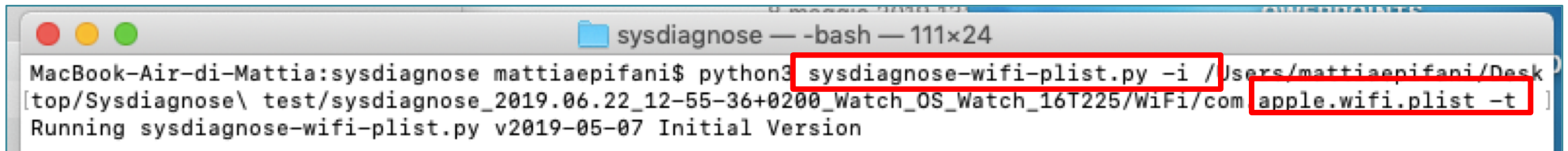
APPLE WATCH WIFI LOGS

·80211W_ENABLED	boolean	true
·WiFiNetworksAutoJoined	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	

<https://t.me/learningnets>

APPLE WATCH WIFI LOGS

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



A terminal window titled "sysdiagnose — -bash — 111x24" on a MacBook-Air-di-Mattia. The prompt is "mattiaepifani\$". The command "python3 sysdiagnose-wifi-plist.py -i /Users/mattiaepifani/Desktop/top/Sysdiagnose/test/sysdiagnose_2019.06.22_12-55-36+0200_Watch_OS_Watch_16T225/WiFi/com.apple.wifi.plist -t" is entered. The output is "Running sysdiagnose-wifi-plist.py v2019-05-07 Initial Version".

```
MacBook-Air-di-Mattia:sysdiagnose mattiaepifani$ python3 sysdiagnose-wifi-plist.py -i /Users/mattiaepifani/Desktop/top/Sysdiagnose/test/sysdiagnose_2019.06.22_12-55-36+0200_Watch_OS_Watch_16T225/WiFi/com.apple.wifi.plist -t  
Running sysdiagnose-wifi-plist.py v2019-05-07 Initial Version
```

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

APPLE WATCH WIFI LOGS

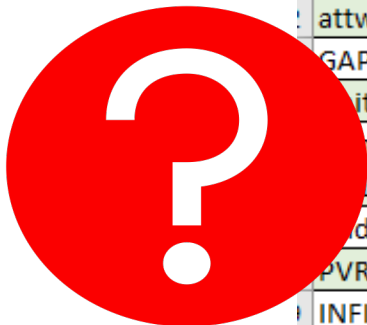
```
sysdiagnose — bash — 111x24
MacBook-Air-di-Mattia:sysdiagnose mattiaepifani$ python3 sysdiagnose-wifi-plist.py -i /Users/mattiaepifani/Desktop/Sysdiagnose/test/sysdiagnose_2019.06.22_12-55-36+0200_Watch_OS_Watch_16T225/WiFi/com.apple.wifi.plist -t
Running sysdiagnose-wifi-plist.py v2019-05-07 Initial Version
```

A	B	C	D	E	F
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	6.30129897554519	NL	2019-03-28 04:12:37.300878	2018-11-19 16:38:02.600754

APPLE WATCH WIFI LOGS

```
sysdiagnose — bash — 111x24
MacBook-Air-di-Mattia:sysdiagnose mattiaepifani$ python3 sysdiagnose-wifi-plist.py -i /Users/mattiaepifani/Desktop/Sysdiagnose/test/sysdiagnose_2019.06.22_12-55-36+0200_Watch_OS_Watch_16T225/WiFi/com.apple.wifi.plist -t
Running sysdiagnose-wifi-plist.py v2019-05-07 Initial Version
```

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
hit 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_FODA	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-f	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	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



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](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**

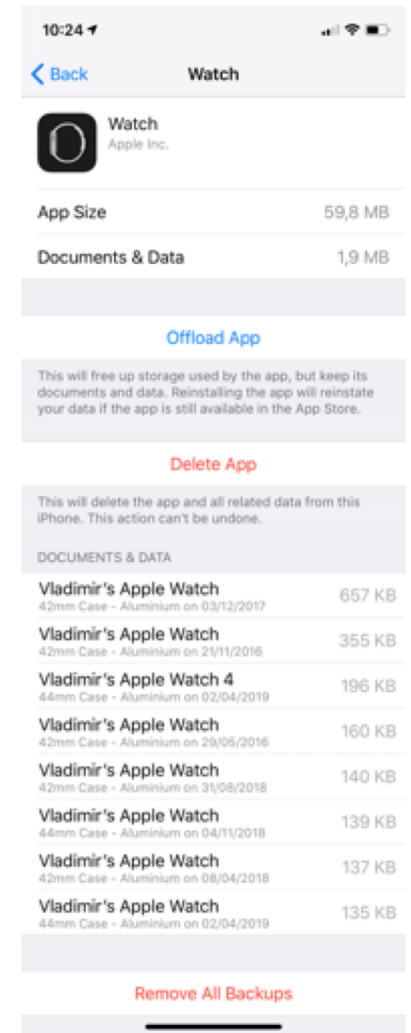
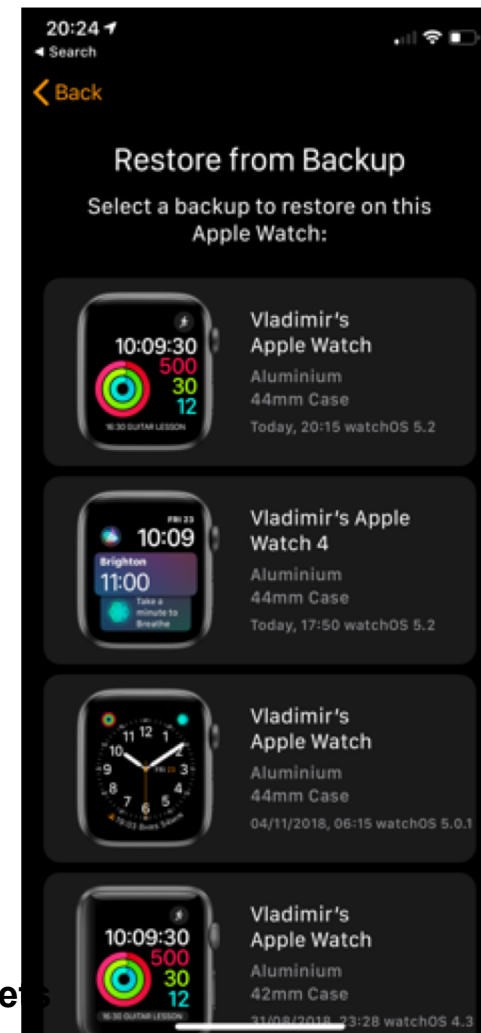
APPLE WATCH BACKUP AND UNPAIR

- 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!!)**

<https://t.me/learningnes>



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

The screenshot shows the iBackupBot interface for an iPad iPhone backup. The left pane displays the file tree under 'EpiphoneX (12/31/18 14:31:34)'. The 'DeviceRegistry.state' folder is selected. The main pane shows a list of files with the following columns: Name, Size, Permission, Date Modified, and Date Created. The 'history.plist' file is highlighted with a red box.

Name	Size	Permission	Date Modified	Date Created
ClassAFile.txt	13	-rw-r--r--	11/04/17 11:47:30	11/04/17 11:47:30
UDIDChangeTracker.plist	272	-rw-r--r--	08/27/18 14:48:13	08/27/18 14:48:13
activeStateMachine.plist	1.3 kB	-rw-r--r--	12/28/18 11:17:37	12/28/18 11:17:37
history.plist	3.6 kB	-rw-r--r--	12/27/18 15:27:57	12/27/18 15:27:57
historySecureProperties.plist	1.1 kB	-rw-r--r--	09/15/18 09:48:46	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	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	09/15/18 09:51:20

https://t.me/learningnets
Total: 7 Selected: 2 Selected Size: 2.4 kB

APPLE WATCH HISTORY.PLIST

The image shows a plist editor window titled "HomeDomain/Library/DeviceRegistry.state/history.plist". The left pane shows a tree view with "List View" selected. The right pane shows a hex dump of the "NS.data" field.

Key	Type	Value
Root	dict	
\$version	integer	100000
\$subjects	array	
	string	Null
	dict	
	dict	
NS.data	data	...
\$class	dict	
	dict	
	dict	
\$archiver	string	NSKeyedArchiver
\$stop	dict	

NS.data (Position: 0 / CFA (0%))

Hex	Value
00000000:	08 31 12 91 15 08 31 11 11 34 DA 83 04 E6 C0
0000000F:	41 1A 83 15 0A 10 24 62 0D 1C 60 16 43 78 B7
0000001E:	E9 71 98 D7 F0 C7 18 12 EE 14 08 00 12 E9 14
0000002D:	0A 0A 68 77 4D 6F 64 65 6C 53 74 72 0A 0C 5F
0000003C:	6B 65 79 63 68 61 69 6E 4F 66 66 0A 09 70 61
0000004B:	69 72 69 6E 67 49 44 0A 0D 73 79 73 74 65 6D
0000005A:	56 65 72 73 69 6F 6E 0A 12 73 79 73 74 65 6D
00000069:	42 75 69 6C 64 56 65 72 73 69 6F 6E 0A 0A 43
00000078:	50 55 53 75 62 54 79 70 65 0A 05 63 6C 61 73
00000087:	73 0A 19 6C 6F 63 61 6C 50 61 69 72 69 6E 67
00000096:	44 61 74 61 53 74 6F 72 65 50 61 74 68 0A 0E
000000A5:	61 64 76 65 72 74 69 73 65 64 4E 61 6D 65 0A
000000B4:	19 6D 61 72 6B 65 74 69 6E 67 48 61 72 64 77
000000C3:	61 72 65 42 65 68 61 76 69 6F 72 0A 14 6D 69
000000D2:	67 72 61 74 69 6F 6E 4B 65 79 52 65 76 69 73
000000E1:	69 6F 6E 0A 0C 74 6F 74 61 6C 53 74 6F 72 61
000000F0:	67 65 0A 0B 73 63 72 65 65 6E 53 63 61 6C 65
000000FF:	0A 0E 57 49 46 49 4D 41 43 41 64 64 72 65 73
0000010E:	73 0A 0C 73 65 72 69 61 6C 4E 75 6D 62 65 72
0000011D:	0A 12 70 72 65 66 65 72 72 65 64 4C 61 6E 67

Byte: 8 BE Word: 2097 BE Dword: 137433745
LE Word: 12552 LE Dword: 2433888520

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
modelName	A1859
deviceNameString	Watch3,4

APPLE WATCH DEVICEREGISTRY.STATE FOLDER

The screenshot shows the iBackupBot interface for an iPad iPhone backup. The left pane displays the file structure under 'System Files', with 'DeviceRegistry.state' selected. The right pane shows a list of files with the following details:

Name	Size	Permission	Date Modified	Date Created
ClassAFile.txt	13	-rw-r--r--	11/04/17 11:47:30	11/04/17 11:47:30
UDIDChangeTracker.plist	272	-rw-r--r--	08/27/18 14:48:13	08/27/18 14:48:13
activeStateMachine.plist	1.3 kB	-rw-r--r--	12/28/18 11:17:37	12/28/18 11:17:37
history.plist	3.6 kB	-rw-r--r--	12/27/18 15:27:57	12/27/18 15:27:57
historySecureProperties.plist	1.1 kB	-rw-r--r--	09/15/18 09:48:46	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	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	09/15/18 09:51:20

At the bottom of the window, the text 'Welcome to iBackupBot for iPad iPhone' is visible on the left, and a URL 'https://t.me/learningnets' is centered. The status bar at the bottom right indicates 'Total: 7 Selected: 2 Selected Size: 2.4 kB'.

APPLE WATCH HISTORYSECUREPROPERTIES.PLIST

HomeDomain/Library/DeviceRegistry.state/historySecureProperties.plist

XML View List View

Key	Type	Value
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	dict	
	string	Unknown
	string	B825F542-BCC2-46DD-A290-E80B472ABE29
	string	b8:41:a4:14:37:df
	string	04613B9BD249800180981429749463243BAA5B7A15DB60B9
	string	b8:41:a4:12:e6:b7
	string	GJ9X86F2J5X4
	string	2a9fbea1643728ce72f820abd21cf5e854242341
	dict	

WiFi Mac Address

BT Mac Address

Serial Number

UDID

<https://t.me/learningnets>

APPLE WATCH DEVICEREGISTRY.STATE FOLDER

The screenshot shows the iBackupBot interface for an iPad iPhone backup. The left pane displays a tree view of system files, including folders like CameraRollDomain, DatabaseDomain, HealthDomain, HomeDomain, and Library. The right pane shows a detailed list of files with columns for Name, Size, Permission, Date Modified, and Date Created. The file 'stateMachine-24620D1C-6016-4378-B7E9-7198D7F0C718.plist' is highlighted with a red border.

Name	Size	Permission	Date Modified	Date Created
ClassAFile.txt	13	-rw-r--r--	11/04/17 11:47:30	11/04/17 11:47:30
UDIDChangeTracker.plist	272	-rw-r--r--	08/27/18 14:48:13	08/27/18 14:48:13
activeStateMachine.plist	1.3 kB	-rw-r--r--	12/28/18 11:17:37	12/28/18 11:17:37
history.plist	3.6 kB	-rw-r--r--	12/27/18 15:27:57	12/27/18 15:27:57
historySecureProperties.plist	1.1 kB	-rw-r--r--	09/15/18 09:48:46	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	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	09/15/18 09:51:20

https://t.me/learningnets
Total: 7 Selected: 2 Selected Size: 2.4 kB

APPLE WATCH STATEMACHINE-<GUID>.PLIST

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

XML View List View

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
+	dict	
NS.time	real	
+\$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)

<https://t.me/learningnets>

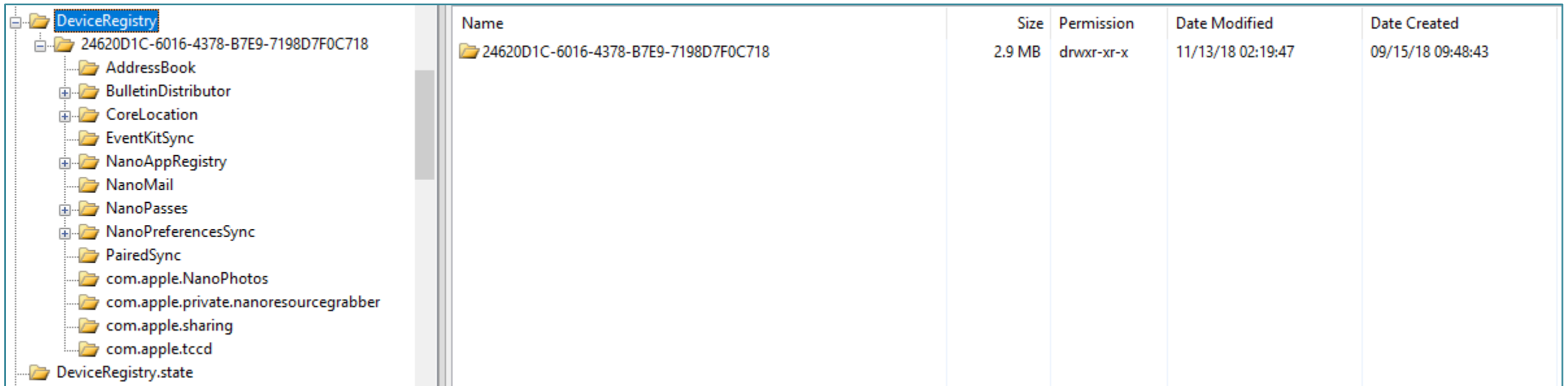
APPLE WATCH DEVICEREGISTRY.STATE FOLDER

The screenshot shows the iBackupBot interface for an iPad iPhone backup. The left pane displays the file tree under 'EpiphoneX (12/31/18 14:31:34)'. The 'DeviceRegistry.state' folder is selected. The main pane shows a list of files with the following columns: Name, Size, Permission, Date Modified, and Date Created. The 'activeStateMachine.plist' file is highlighted with a red box.

Name	Size	Permission	Date Modified	Date Created
ClassAFile.txt	13	-rw-r--r--	11/04/17 11:47:30	11/04/17 11:47:30
UDIDChangeTracker.plist	272	-rw-r--r--	08/27/18 14:48:13	08/27/18 14:48:13
activeStateMachine.plist	1.3 kB	-rw-r--r--	12/28/18 11:17:37	12/28/18 11:17:37
history.plist	3.6 kB	-rw-r--r--	12/27/18 15:27:57	12/27/18 15:27:57
historySecureProperties.plist	1.1 kB	-rw-r--r--	09/15/18 09:48:46	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	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	09/15/18 09:51:20

https://t.me/learningnets
Total: 7 Selected: 2 Selected Size: 2.4 kB

APPLE WATCH DEVICEREGISTRY FOLDER



The image shows a file explorer window with the 'DeviceRegistry' folder selected. The left pane displays a tree view of the folder's contents, including subfolders like '24620D1C-6016-4378-B7E9-7198D7F0C718', 'AddressBook', 'BulletinDistributor', 'CoreLocation', 'EventKitSync', 'NanoAppRegistry', 'NanoMail', 'NanoPasses', 'NanoPreferencesSync', 'PairedSync', 'com.apple.NanoPhotos', 'com.apple.private.nanoresourcegrabber', 'com.apple.sharing', 'com.apple.tccd', and 'DeviceRegistry.state'. The right pane shows a table with the following data:

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

APPLE WATCH NANOAPPREGISTRY FOLDER

The image shows a file explorer window with a sidebar containing a tree view of the NanoAppRegistry folder. The main pane displays the XML view of an application bundle file (Application.dat). Two red boxes highlight specific data points in the XML view.

File Explorer Sidebar:

- NanoAppRegistry
 - Applications
 - 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
 - com.melodis.soundhound.free.watch

File Explorer Main Pane:

Name	Size	Permission	Date Modified	Date Created
Application.dat	1.0 kB	-rw-r--r--	12/28/18 22:08:29	12/28/18 22:08:29

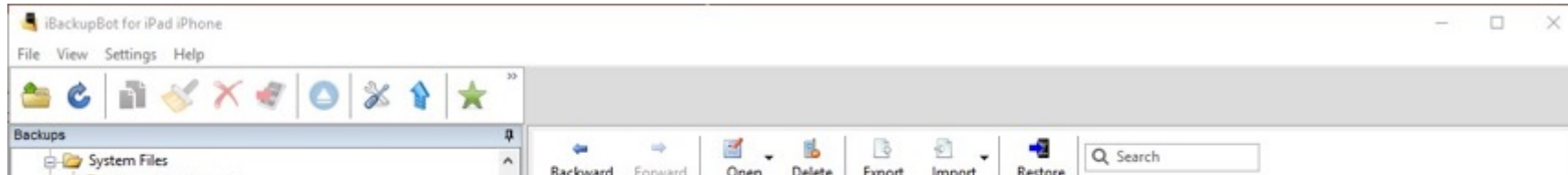
HomeDomain/Library/DeviceRegistry/24620D1C-6016-4378-B7E9-7198D7F0C718/NanoAppRegistry/Applications/com.facebook.Messen... X

XML View List View

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

<https://t.me/learningnets>

APPLE WATCH NANOMAIL\REGISTRY.SQLITE



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

Tables	ID	DISPLAY_NAME	SHOULD_ARCHIVE	EMAIL_ADDRESSES	RESEND_REQUESTED
ATTACHMENT_NOT_SYNCED	1	Digital Forensics	1	mattia.epifani@digital-forensics.it	0
COMPOSED_MESSAGE	2	Info reality	1		0
CONTROL	3	DFA	1		0
DELETED_MESSAGE	4	RealityNet	1		0
IDS_IDENTIFIER_NOT_YET_ACTIVATED	5	Segreteria	1		0
IDS_IDENTIFIER_OBJECT	6	Hotmail	0		0
MAILBOX	7	Outlook	0		0
MAILBOX_SYNC_VERSION					
SYNCED_ACCOUNT					



APPLE WATCH NANOMAIL\REGISTRY.SQLITE

The screenshot shows the iBackupBot application interface. The main window displays a SQLite database table named 'MAILBOX' located at the path: HomeDomain/Library/DeviceRegistry/24620D1C-6016-4378-B7E9-7198D7F0C718/NanoMail/registry.sqlite. The table has three columns: 'ID', 'ID', and 'ACCOUNT_ID'. The 'ID' column contains 8 rows of data, with the first three rows highlighted in red. The 'MAILBOX' table is selected in the left-hand 'Tables' pane.

	ID	ACCOUNT_ID
1	54A03817-58F4-4A6F-9A76-A2E80FB88B9D/Notes	54A03817-58F4-4A6F-9A76-A2E80FB88B9D
2	54A03817-58F4-4A6F-9A76-A2E80FB88B9D/[Gmail]	54A03817-58F4-4A6F-9A76-A2E80FB88B9D
3	54A03817-58F4-4A6F-9A76-A2E80FB88B9D/Speciali	54A03817-58F4-4A6F-9A76-A2E80FB88B9D
4	FB0F621D-BDD8-466E-8307-4E7050E029DA/Archives	FB0F621D-BDD8-466E-8307-4E7050E029DA
5	FB0F621D-BDD8-466E-8307-4E7050E029DA/Notes	FB0F621D-BDD8-466E-8307-4E7050E029DA
6	FB0F621D-BDD8-466E-8307-4E7050E029DA/Sent	FB0F621D-BDD8-466E-8307-4E7050E029DA
7	FB0F621D-BDD8-466E-8307-4E7050E029DA/Trash	FB0F621D-BDD8-466E-8307-4E7050E029DA
8	FB0F621D-BDD8-466E-8307-4E7050E029DA/[Gmail]	FB0F621D-BDD8-466E-8307-4E7050E029DA

The screenshot shows a file explorer window displaying the directory structure of the NanoMail folder. The directory tree includes the following items:

- CoreLocation
- EventKitSync
- NanoAppRegistry
- NanoMail
- NanoPasses
- NanoPreferencesSync
- NanoSystemSettings
- PairedSync
- com.apple.NanoPhotos
- com.apple.private.nanoresourcegrabber
- com.apple.sharing
- com.apple.tccd

At the bottom of the window, there is a URL bar containing the text: <https://t.me/learningnets>. The status bar at the bottom indicates: "Total: 1 Selected: 1 Selected Size: 840.0 kB".

APPLE WATCH NANOPASSES\NANOPASSES.SQLITE3

The screenshot shows a file explorer window with a sidebar on the left displaying a directory tree under 'Backups'. The tree includes folders like NanoAppRegistry, NanoMail, NanoPasses (expanded), NanoPreferencesSync, PairedSync, and various com.apple.* folders. 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>
IQx8nkFxxN4p+KDe8lZ0ViNjag=	pass.com.bestwestern.rewards	Best Western Rewards	563059511	Get. Rewarded.

APPLE WATCH 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 $top... ^u....[
0x0048 005C 005D 0076 007B 007C 0082 0088 0089 008C .\.]v.{.|. . . .
0x005A 008D 0094 0098 0047 00BA 00BB 00BC 00BD 00C1 . . . .G.°.».X.¼.Á
0x006C 00C4 00C5 0034 00C7 00C8 00CD 00D0 00D4 00B3 .Ä.Å.4.ç.È.Í.Ð.Ë.Ë
0x007E 00DF 00E0 00E1 00E2 00E6 00EA 00F5 00F6 00F7 .ß.à.á.â.æ.ê.ë.ö.÷
0x0090 00F8 00FD 004A 0108 0109 010A 010B 010C 011B .ø.ý.J.....
0x00A2 011C 011D 011E 011F 0120 0121 0126 012A 0134 ..... !.&*.4
0x00B4 00AB 013F 0140 0141 014C 014D 014E 014F 015A .«.¿.@.A.L.M.N.O.Z
0x00C6 015B 015C 015D 0168 0169 016A 016B 016C 0177 .[\.]h.i.j.k.l.w
0x00D8 0178 0179 017A 0185 0186 0187 0188 0193 0194 .x.y.z. . . . .
0x00EA 0195 0196 019B 019E 01A2 01A7 01AB 01AC 01AD . . . . ç. §.«.¬.-
0x00FC 01C2 01CC 01CF 01D1 01D4 01D5 01DA 01DB 01DC .À.Ì.Ï.Ñ.Ò.Û.Ü.Ü
0x010E 01DD 01DE 01DF 01E0 01E3 01E7 01F5 01F6 01F7 .Ý.Þ.ß.à.ä.ç.ë.ö.÷
0x0120 01F8 01FC 01FF 0202 0205 0208 5524 6E75 6C6C .ø.ü.ÿ.....U$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 https://t.me/learningnets activationDate
```

APPLE WATCH NANOPASSES\NANOPASSES.SQLITE3

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;
	string	€215,00
	integer	215
	string	New price is %@
	string	EUR
	dict	

APPLE WATCH NANOPREFERENCESYNC/NANODOMAINS/COM.APPLE.CAROUSEL

The screenshot shows a file explorer interface with a sidebar on the left displaying a directory tree under 'Backups'. The main pane shows a table of files, with 'com.apple.Carousel' selected. A preview window is open over this file, showing its XML content in 'List View'.

Name	Size	Permission	Date Modified	Date Created
.GlobalPreferences	139	-rw-r--r--	09/15/18 09:49:21	09/15/18 09:49:21
com.apple.Bridge	120	-rw-r--r--	12/23/18 15:50:17	12/23/18 15:50:17
com.apple.Carousel	3.8 kB	-rw-r--r--	12/03/18 00:12:02	12/03/18 00:12:02

HomeDomain/Library/DeviceRegistry/24620D1C-6016-4378-B7E9-7198D7F0C718/NanoPreferencesSync/NanoDomains/com.apple.Carousel

Key	Type	Value
Root	dict	
FavoriteApplications	array	
	string	com.apple.ActivityMonitorApp
	string	com.apple.HeartRate
	string	com.apple.SessionTrackerApp
	string	com.apple.NanoMusic
	string	com.apple.MobileSMS
	string	com.apple.private.NanoTimer
	string	com.apple.NanoCalendar
	string	com.apple.NanoMaps
MRUBasedDockLayout	boolean	true
IconPositions	data	...
MaximumFavoriteApplications	integer	10

<https://t.me/learningnets>

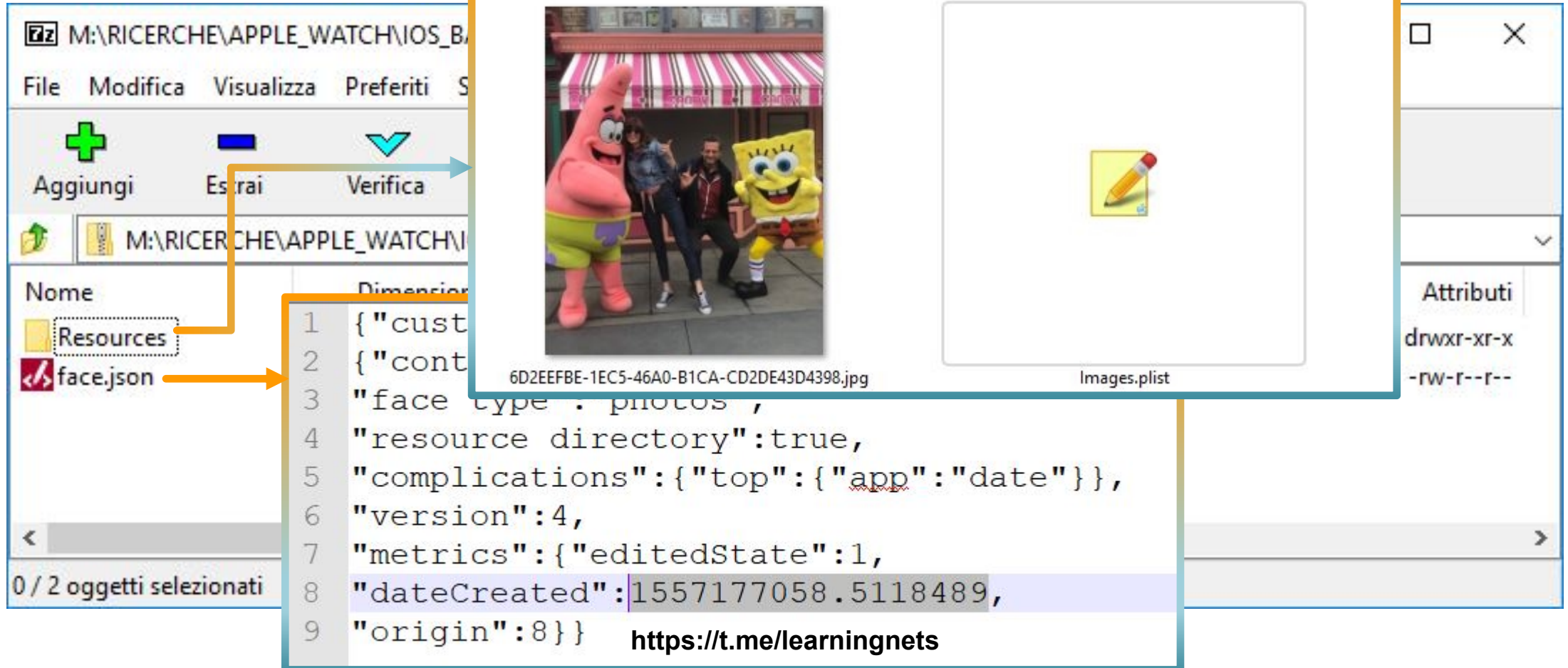
APPLE WATCH NANOPREFERENCESYNC\BACKUP\FILES FOLDER

The screenshot shows the iBackupBot for iPad iPhone application window. The main area displays a file list with columns for Name, Size, Permission, Date Modified, and Date Created. A red box highlights the file 10ED369A-CB3F-462A-9704-E2FEE07CFDAF, which is 82.4 kB in size and was last modified on 05/07/19 at 22:12:25. The left sidebar shows a tree view of the backup structure, with the selected file's path expanded to NanoPreferencesSync\Backup\Files. The status bar at the bottom indicates 'Total: 17 Selected: 1 Selected Size: 82.4 kB'.

Name	Size	Permission	Date Modified	Date Created
042FB8FD-9B25-4E74-8F6C-44FA5DB76AD2	8	-rw-rw-rw-	09/15/18 09:51:53	09/15/18 09:51:53
10ED369A-CB3F-462A-9704-E2FEE07CFDAF	82.4 kB	-rw-rw-rw-	05/07/19 22:12:25	05/07/19 22:07:26
187753DD-C0D3-44E1-AD04-2D2741E10B7D				
24620D1C-6016-4378-B7E9-7198D7F0C718				
AddressBook				
BulletinDistributor				
CoreLocation				
EventKitSync				
NanoAppRegistry				
NanoMail				
NanoPasses				
PaymentCards				
NanoPreferencesSync				
Backup				
Files				
UserDefaults				
Cache				
NanoDomains				
NanoSystemSettings				
Caches				
PairedSync				
com.apple.NanoPhotos				
com.apple.private.nanoresourcegrabber				
com.apple.sharing				
com.apple.tccd				
DeviceRegistry.state				
DoNotDisturb				
47AEBE15-8CF1-40CD-8C57-633877D7B236	256	-rw-rw-rw-	09/15/18 09:51:54	09/15/18 09:51:54
5C22B05E-7055-47BE-A9FA-B815D05B51D8	273	-rw-rw-rw-	04/26/19 12:24:45	04/26/19 12:24:45
5E7E31F2-C7CA-4E62-A11B-DB9E4E85388B	36	-rw-rw-rw-	06/22/19 12:48:20	06/22/19 12:48:20
8017ABF0-53EF-4770-9245-CC1E6659B50E	297	-rw-rw-rw-	09/15/18 09:51:53	09/15/18 09:51:53
8088F789-F20C-4736-B18C-96142F6635A0	195	-rw-rw-rw-	09/15/18 09:51:54	09/15/18 09:51:54
9124DD42-489F-407B-B24F-6E04A11F8BF7	266	-rw-rw-rw-	09/15/18 09:51:55	09/15/18 09:51:55
C392D2BA-4ECE-46C7-83C8-CAF1022EF848	313	-rw-rw-rw-	09/15/18 09:51:54	09/15/18 09:51:54
DB2BB439-DD07-4586-A863-5C61743E0718	357	-rw-rw-rw-	11/14/18 23:01:05	11/14/18 23:01:05
ECBB478D-CB07-4955-AB93-22FFD664454A	795	-rw-rw-rw-	05/07/19 22:12:25	05/07/19 22:12:25
F7FC0DF7-ADD3-4FE2-9AAE-3CC3A0CB0A1	59.3 kB	-rw-rw-rw-	03/13/19 19:15:16	03/13/19 19:15:16
index	3.6 kB	-rw-rw-rw-	05/07/19 22:12:25	05/07/19 22:12:25

<https://t.me/learningnets>

APPLE WATCH NANOPREFERENCESYNC\BACKUP\FILES FOLDER



APPLE_WATCH > IOS_BACKUP_ARTICLE_ELCOMSOFT > 10ED369A-CB3F-462A-9704-E2FEE07CFDAF > Resources

6D2EEFBE-1EC5-46A0-B1CA-CD2DE43D4398.jpg

Images.plist

```
1 {"cust
2 {"cont
3 "face type : photos ,
4 "resource directory":true,
5 "complications":{"top":{"app":"date"}},
6 "version":4,
7 "metrics":{"editedState":1,
8 "dateCreated":1557177058.5118489,
9 "origin":8}}
```

Attributi
drwxr-xr-x
-rw-r--r--

0 / 2 oggetti selezionati

<https://t.me/learningnets>

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>
<https://t.me/learningnets>



APPLE WATCH HEALTH DATA IN (ENCRYPTED) LOCAL BACKUP

The screenshot shows the Elcomsoft Phone Viewer Health application interface. The main window displays the 'Health' app data for an iPhone X. The interface includes a navigation menu on the left with options like 'Filter', 'Date', 'Source', and 'Device'. The main content area shows a summary of 78323 records and a table of individual health events. The table columns are Start Date, End Date, Date Added, Source, Device, Details, and Steps.

Start Date	End Date	Date Added	Source	Device	Details	Steps
27.08.2019 14:12:41 (UTC +2)	27.08.2019 14:22:40 (UTC +2)	27.08.2019 14:24:01 (UTC +2)	EpiphoneX	iPhone X (GSM)	Hardware v...	381
27.08.2019 13:47:16 (UTC +2)	27.08.2019 13:51:19 (UTC +2)	27.08.2019 13:58:42 (UTC +2)	EpiphoneX	iPhone X (GSM)	Hardware v...	216
27.08.2019 11:15:47 (UTC +2)	27.08.2019 11:21:56 (UTC +2)	27.08.2019 11:27:15 (UTC +2)	EpiphoneX	iPhone X (GSM)	Hardware v...	83
27.08.2019 10:23:42 (UTC +2)	27.08.2019 10:24:02 (UTC +2)	27.08.2019 10:35:03 (UTC +2)	EpiphoneX	iPhone X (GSM)	Hardware v...	33
27.08.2019 10:11:31 (UTC +2)	27.08.2019 10:21:21 (UTC +2)	27.08.2019 10:23:30 (UTC +2)	EpiphoneX	iPhone X (GSM)	Hardware v...	176
27.08.2019 10:08:57 (UTC +2)	27.08.2019 10:08:59 (UTC +2)	27.08.2019 10:17:54 (UTC +2)	Mattia's Apple Watch	Apple Watch Series 3	Hardware v...	4
27.08.2019 10:05:06 (UTC +2)	27.08.2019 10:05:24 (UTC +2)	27.08.2019 10:08:50 (UTC +2)	Mattia's Apple Watch	Apple Watch Series 3	Hardware v...	11
27.08.2019 10:02:07 (UTC +2)	27.08.2019 10:02:15 (UTC +2)	27.08.2019 10:08:50 (UTC +2)	Mattia's Apple Watch	Apple Watch Series 3	Hardware v...	12
27.08.2019 10:01:09 (UTC +2)	27.08.2019 10:02:07 (UTC +2)	27.08.2019 10:08:50 (UTC +2)	Mattia's Apple Watch	Apple Watch Series 3	Hardware v...	33
27.08.2019 10:00:10 (UTC +2)	27.08.2019 10:01:09 (UTC +2)	27.08.2019 10:08:50 (UTC +2)	Mattia's Apple Watch	Apple Watch Series 3	Hardware v...	62
27.08.2019 00:58:48 (UTC +2)	27.08.2019 10:00:50:26 (UTC +2)	27.08.2019 10:00:27 (UTC +2)	Mattia's Apple Watch	Apple Watch Series 3	Hardware v...	26

APPLE WATCH HEALTH DATA IN (ENCRYPTED) LOCAL BACKUP

UFED Physical Analyzer File Visualizza Strumenti Estrai Python Plug-in Rapporto Guida

Novità x Sommario estrazione (1) x Health (110270) x healthdb_secure.sqlite x

Health (110270)

Esporta Filters Actions Ricerca tabel

Nome	Proviene da	Valore	↓ Ora inizio	Ora fine	Posizione	Origine
Heart Rate	Dispositivo sincronizzato	76 BPM	29/07/2019 17:57(UTC+2)	29/07/2019 17:57(UTC+2)		Health
Heart Rate	Dispositivo sincronizzato	91 BPM	29/07/2019 17:52(UTC+2)	29/07/2019 17:52(UTC+2)		Health
Active Energy	Dispositivo sincronizzato	0,29 Chilocalorie	29/07/2019 17:49(UTC+2)	29/07/2019 17:50(UTC+2)		Health
Heart Rate	Dispositivo sincronizzato	72 BPM	29/07/2019 17:49(UTC+2)	29/07/2019 17:49(UTC+2)		Health
Active Energy	Dispositivo sincronizzato	3,01 Chilocalorie	29/07/2019 17:45(UTC+2)	29/07/2019 17:49(UTC+2)		Health
Active Energy	Dispositivo sincronizzato	1,53 Chilocalorie	29/07/2019 17:41(UTC+2)	29/07/2019 17:45(UTC+2)		Health
Heart Rate	Dispositivo sincronizzato	61 BPM	29/07/2019 17:41(UTC+2)	29/07/2019 17:41(UTC+2)		Health
Steps and Distance	Dispositivo sincronizzato	13 Passi 10 Metri	29/07/2019 17:39(UTC+2)	29/07/2019 17:39(UTC+2)		Health
Steps and Distance	Dispositivo sincronizzato	9 Passi	29/07/2019 17:36(UTC+2)	29/07/2019 17:36(UTC+2)		Health

<https://t.me/learningnets>



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

Elcomsoft Phone Breaker


Password Recovery Wizard **Tools**

[All tools](#) Download synced data from iCloud

Mattia Epifani (1321761630) – mattiaep@hotmail.it [Change user](#)

<input checked="" type="checkbox"/> Account info	<input checked="" type="checkbox"/> Contacts	<input checked="" type="checkbox"/> Notes
<input checked="" type="checkbox"/> Apple Maps	<input checked="" type="checkbox"/> Health	<input checked="" type="checkbox"/> Safari
<input checked="" type="checkbox"/> Calendars	<input checked="" type="checkbox"/> iBooks	<input checked="" type="checkbox"/> Wallet
<input checked="" type="checkbox"/> Calls	<input checked="" type="checkbox"/> Messages	<input checked="" type="checkbox"/> Wi-Fi

[Check all](#) [Uncheck all](#)

 To download categories marked orange from the list above you will need to provide a passcode for a trusted device linked to the account. Otherwise, the data might be downloaded partially or not be downloaded at all.

[Download...](#)

<https://t.me/learningnets>

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://t.me/learningnets> <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](https://twitter.com/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://twitter.com/dfirfpi)

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

 <http://www.realitynet.it>

 <http://blog.digital-forensics.it>

<https://t.me/learningnets>