

# APPLE HOMEPOD AND HOMEKIT FORENSICS

MATTIA EPIFANI

SANS DFIR SUMMIT

17<sup>TH</sup> JULY 2020



# WHO AM I

- I live and work in Italy
- Master's Degree in IT in 2002
- Founder and CEO @ REALITY NET
- Digital Forensics Analyst
- SANS Instructor FOR585/FOR500
- Researcher at IGSG – CNR  
(Italian National Council of Research)



# APPLE HOMEKIT

- Software framework for **home automation**
- **Apple-certified** smart accessories
- Accessories are grouped by **Rooms**



# CASE STUDY SCENARIO



1. Eve Door Sensor
2. Apple HomePod
3. Apple iPhone 7

# APPLE HOMEPOD

- **Smart Speaker** developed by Apple
- Designed to work with other Apple devices (i.e. iPhone and iPad)
- It works with **Apple Music** and the **Home** app
- It integrates **Siri** and other **HomeKit devices**



# EVE DOOR SENSOR

- Connected via **Bluetooth**
- **Apple HomeKit** enabled
- Remotely controlled by the **HomePod**



# DEVICE IDENTIFICATION

MATTIA EPIFANI

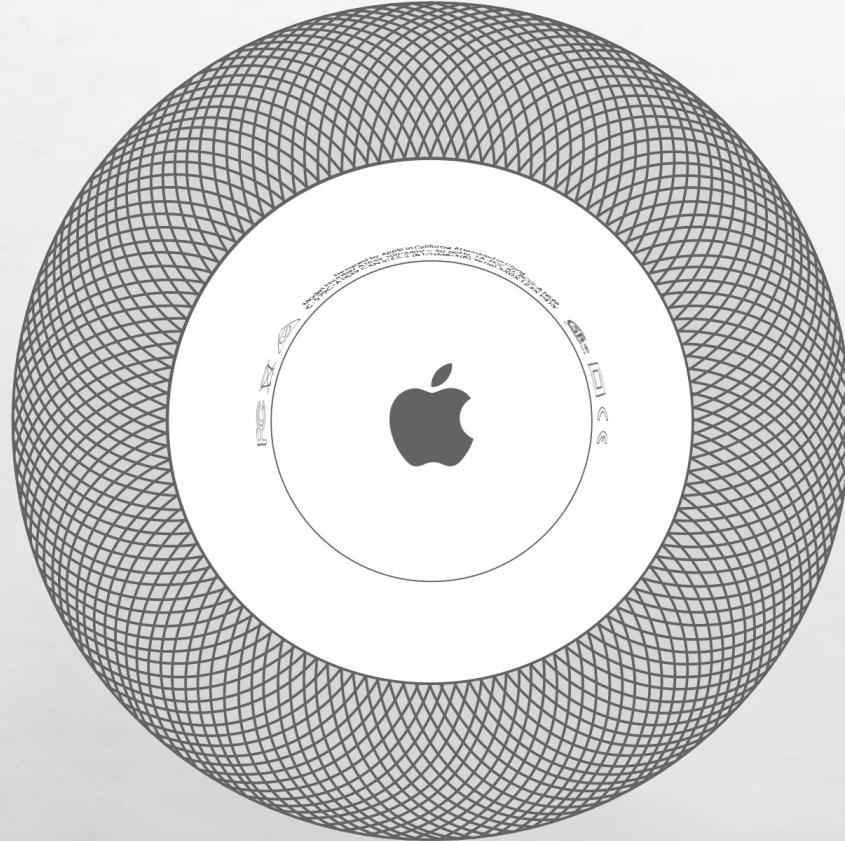
SANS DFIR SUMMIT

17<sup>TH</sup> JULY 2020



# APPLE HOMEPOD – IDENTIFICATION (DEVICE)

<https://support.apple.com/en-us/HT208347>

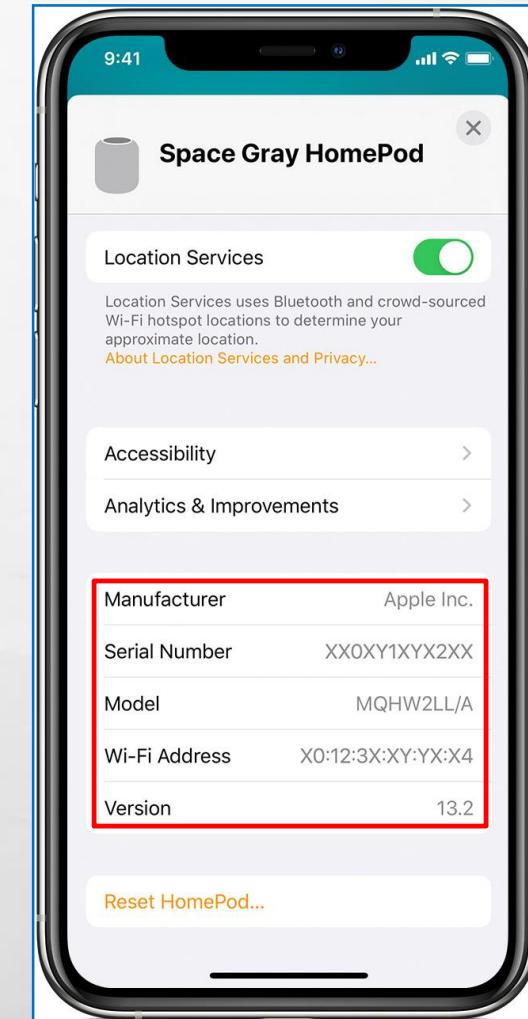


The **Serial Number** and the  
**Model Number** are on the  
bottom of the HomePod

# APPLE HOMEPOD – IDENTIFICATION (IPHONE)

<https://support.apple.com/en-us/HT208347>

**Serial number, Model Number,  
Wi-Fi Address and iOS/tvOS version  
are available in the Home app**



# DATA EXTRACTION

MATTIA EPIFANI

SANS DFIR SUMMIT

17<sup>TH</sup> JULY 2020

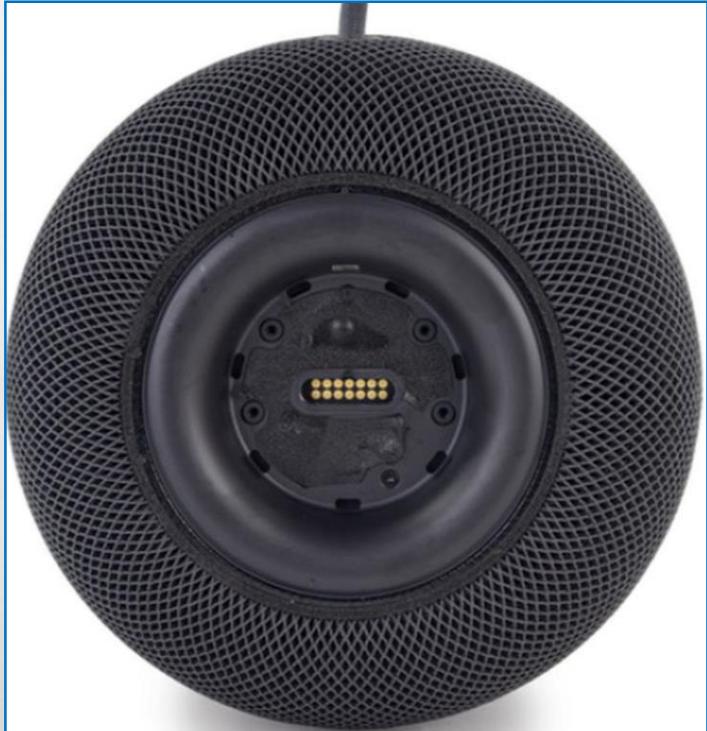


# APPLE HOMEKIT / HOMEPOD ACQUISITION

- **HomePod**
  - Direct connection (?)
  - HomePod Sysdiagnose
- **Synced iPhone(s)/iPad(s)**

# APPLE HOMEPOD – THE HIDDEN 14-PIN PORT

<https://www.macrumors.com/2018/02/12/homepod-teardown-ifixit/>



*[...] iFixit found a hidden **14-pin connector** that they speculate is probably used to test or program HomePods on pogo pins during assembly [...].*

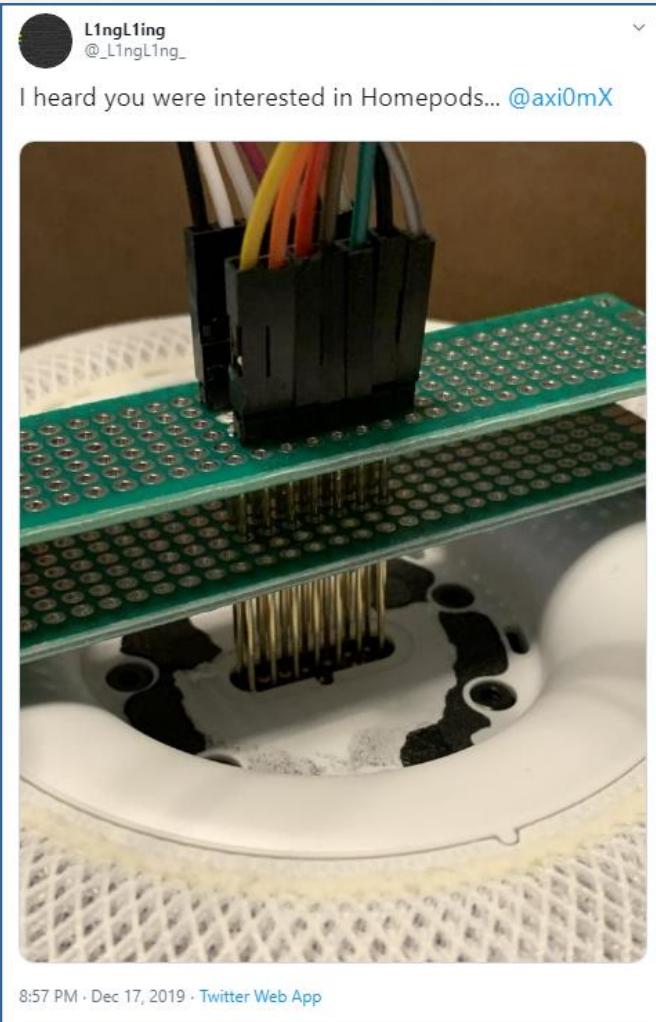
*Given the port sits below a layer of strong adhesive, it's unclear if it will be used for any other purpose, such as **diagnostic testing**.*"

<https://www.ifixit.com/Teardown/HomePod+Teardown/103133>

[https://en.wikipedia.org/wiki/Pogo\\_pin](https://en.wikipedia.org/wiki/Pogo_pin)

# APPLE HOMEPOD – THE HIDDEN 14-PIN PORT

[https://mobile.twitter.com/\\_l1ngl1ng\\_/status/1207027058875875328](https://mobile.twitter.com/_l1ngl1ng_/status/1207027058875875328)



# APPLE SYSDIAGNOSE

- Apple provides “A web-based tool that developers can use to report issues with Apple software and services”
- To correctly use this tool it is mandatory to “collect and attach any relevant logs” extracted from the device

# APPLE SYSDIAGNOSE

## Using Apple “Bug Reporting” for forensic purposes

- Mattia Epifani, Heather Mahalik and @cheeky4n6monkey wrote a document describing their research about these logs

[HTTPS://WWW.FOR585.COM/SYSDIAGNOSE](https://www.for585.com/sysdiagnose)

- We also developed scripts to parse some of the files available in a sysdiagnose acquisition

[HTTPS://GITHUB.COM/CHEEKY4N6MONKEY/IOS\\_SYSDIAGNOSE\\_FORENSIC\\_SCRIPTS](https://github.com/cheeky4n6monkey/ios_sysdiagnose_forensic_scripts)

# SYSDIAGNOSE ON HOMEPOD

[https://download.developer.apple.com/iOS/iOS\\_Logs/HomePod\\_Logging\\_Instructions.pdf](https://download.developer.apple.com/iOS/iOS_Logs/HomePod_Logging_Instructions.pdf)



## HomePod

For issues with your HomePod, please follow the instructions below to gather logging.

### Enabling Logging

#### Notes:

- This profile will automatically delete from the device after 3 days. If the issue is not reproduced and a sysdiagnose is not triggered within that time, the profile will need to be re-installed.
- The HomePod must be running 11.4 or later.

1. Download the [profile](#) and install it on the iOS device.

If necessary, email the profile or use AirDrop to transfer the profile to the iOS device.

**Important:** Install logging profile onto the iOS device, not the HomePod. If the profile is installed on the HomePod the 'Export Analytics' button will not show up when collecting logs.

# SYSDIAGNOSE ON HOMEPOD

[https://download.developer.apple.com/iOS/iOS\\_Logs/HomePod\\_Logging\\_Instructions.pdf](https://download.developer.apple.com/iOS/iOS_Logs/HomePod_Logging_Instructions.pdf)



- 2. Restart the device if prompted.
- 3. Reproduce the issue.

**Important:** Note the date and time issue occurred and add this information to your report.

- 4. Trigger a sysdiagnose using the following steps:
  - 1. Open the 'Home' app on the iOS device.
  - 2. Long press on the HomePod tile to reveal options.
  - 3. Tap 'Settings' (Previously called 'Details').
  - 4. Tap 'Analytics'.
  - 5. Tap 'Export Analytics'.
  - 6. Wait for the logs to finish gathering. When logs are collected, the HomePod will AirDrop them to the iOS device.
  - 7. From the AirDrop menu, choose 'iCloud Drive' or the 'Files app' and tap 'Add'.
  - 8. Tap 'Done' when the file transfer has completed.

# SYSDIAGNOSE ON HOMEPOD

[https://download.developer.apple.com/iOS/iOS\\_Logs/HomePod\\_Logging\\_Instructions.pdf](https://download.developer.apple.com/iOS/iOS_Logs/HomePod_Logging_Instructions.pdf)



## HomePod

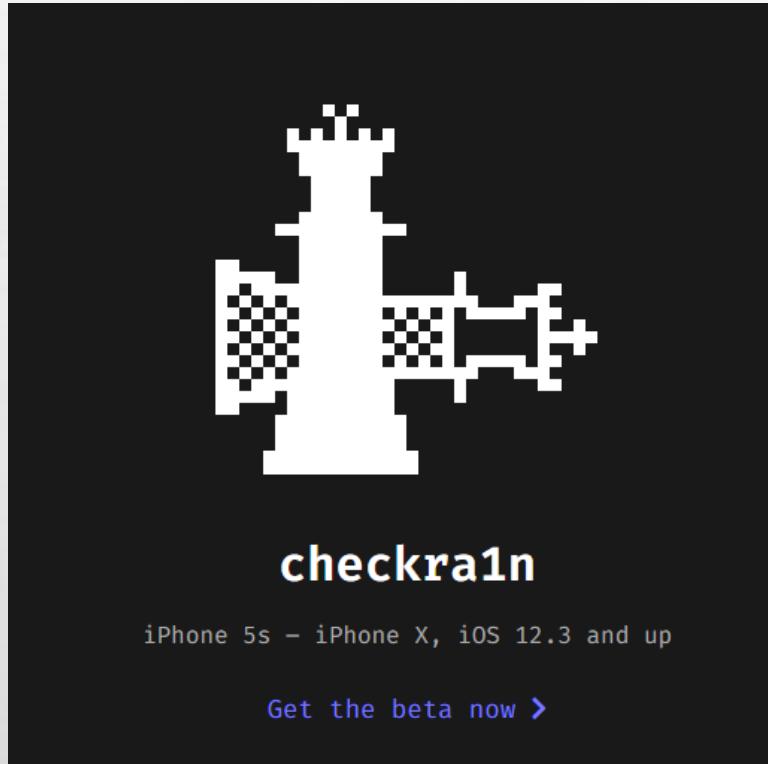
For issues with your HomePod, please follow the instructions below to gather logging.

### Uploading the Log File to Your Report

1. Locate the HomePod sysdiagnose file on iCloud Drive or the Files app on your iOS device (whichever location you saved the file to), and download or AirDrop the file to your macOS system.  
**Note:** Filename will be something like: sysdiagnose\_[Date]\_[Time]\_iPhone\_OS\_AudioAccessory\_[nnxnnn]
2. Attach the file to your report. <<https://feedbackassistant.apple.com/welcome>>

# SYNCED IPHONE

[https://github.com/RealityNet/ios\\_triage](https://github.com/RealityNet/ios_triage)



- Full file system acquisition using **checkra1n jailbreak**
  - Community project based on the '**checkm8**' bootrom exploit
  - **iPhone 5s – iPhone X, iOS 12.3 and up**
  - Open source script '**ios\_triage**' developed "to extract data from a "chekcra1ned" iOS device"

# DATA ANALYSIS - IPHONE

MATTIA EPIFANI

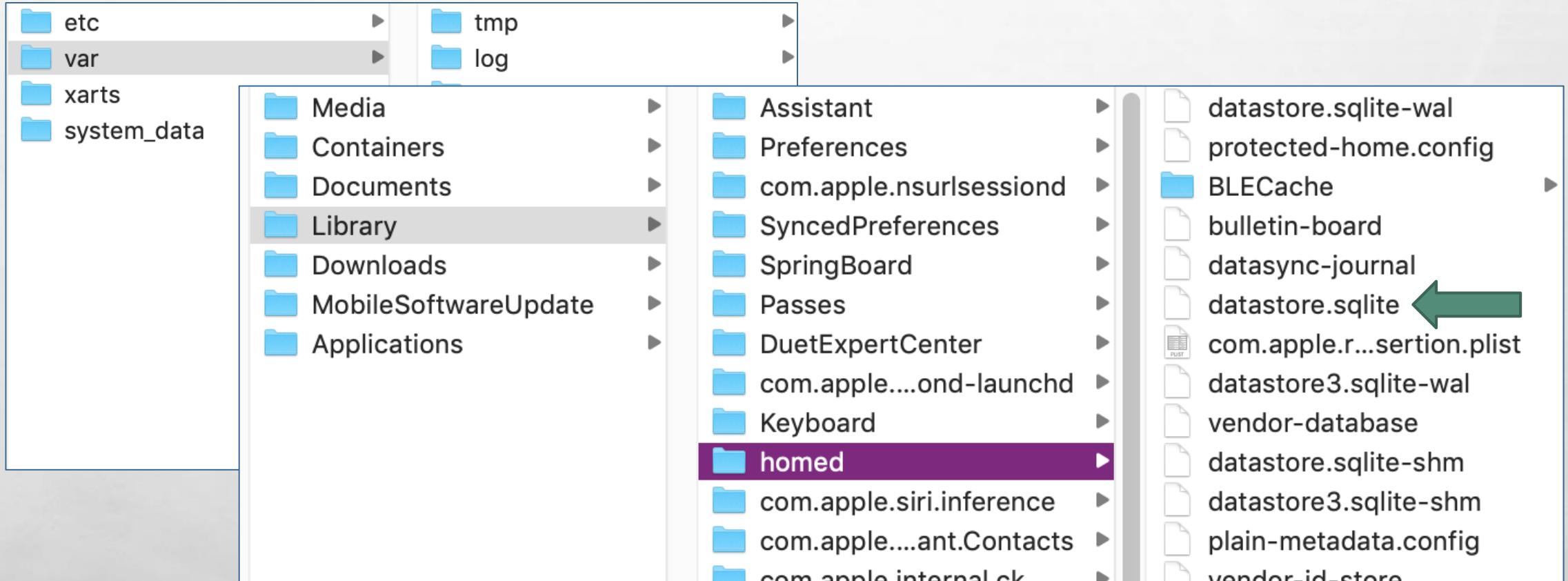
SANS DFIR SUMMIT

17<sup>TH</sup> JULY 2020



# HOMEKIT/HOMEPOD MAIN FOLDER

/private/var/mobile/Library/homed/



# DATASTORE.SQLITE

Database Structure    Browse Data

Create Table    Create Index

Name

- Tables (8)
  - record
  - sqlite\_sequence
  - store
  - xact
  - xact\_block
  - zone
  - zone\_group
  - zone\_share

# DATASTORE.SQLITE

## HMDHomeManagerModel / HMDHomeModel

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

	name	type	uuid	parent_uuid	encoding	record	data
1	9C3BF4D1-C7CF-4217-BCD2-0F7E96D5B300	HMDCloudLegacyModelObject	4E7C000B-1D44-4B71-BD60-02D244A91A9B	NULL	1	BLOB	BLOB
2	EAE83F8B-F492-4683-9593-DE83B17A1E58	HMDHomeManagerModel	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	NULL	1	BLOB	BLOB

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

	name	type	uuid	parent_uuid	encoding	record	data
15	BA9E0595-3ECD-4DDE-BB12-A2C492A93F4F	HMDApplicationDataModel	D162EAEF-8138-5E87-9A01-29F8B9A950A7	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB
16	D085FF04-C62E-43ED-BB51-7D5C74D4B702	HMDAccountModel	9FBF2C67-799C-5466-A728-B73931E44C15	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB
17	8E134E11-9C6F-42BF-B5AB-E2D80E407E5A	HMDCloudZoneInformationModel	2FE62FEA-AA25-5787-AD39-27647760D442	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB
18	351C6C93-6422-426E-9DF1-4CC7374B1D3A	HMDHAPMetadataModel	9C7B07AF-AB5F-58F8-99B8-22FD7732C292	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB
19	92FCA088-C8C9-453C-891B-511B0708B4E4	HMDHomeModel	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB

# HOME NAME, HOME GEOLOCATION AND USER ID

## HMDHomeModel

The image shows two side-by-side hex editors displaying plist data for the HMDHomeModel. Both editors have tabs for Hex and Plist.

**Left Editor (HMDHomeModel.plist):**

- Line 1: <Dictionary>
- Line 2: S ClassName = "HMDHomeModel"
- Line 3: S ownerUserID = "homepodforensics@icloud.com" (highlighted with a red box)
- Line 4: S networkProtectionMode = 0
- Line 5: S \_y = "6.2"
- Line 6: B multiUserEnabled = True
- Line 7: B ownerPublicKey
- Line 8: S ClassName = "NSMutableData"
- Line 9: NS.data = {i:(Ü=zÜAÍÀÖ„ÄñµjKç¶çÉ.¶FO}
- Line 10: S ownerName = "0AC97E25-58DF-44CA-B6DF-2C3D3A3B1D99"
- Line 11: S ownerUUID = "A4A32D3D-59AF-4F47-981B-2D2BD1E34065"
- Line 12: S primaryResidentUUID = "DBACBD84-0916-5FA2-9943-15C93517B9EB"
- Line 13: B homeLocationData
- Line 14: S ClassName = "NSMutableData"
- Line 15: NS.data = bplist00Ô.....X\$versionY\$archiverT\$topX\$objects...† \_ .NSKeyedArchiverN..Troot€.§...3:>AU>nullÔ..... (highlighted with a red box)
- Line 16: B presenceAuthorizationStatus = 1
- Line 17: B name = "La mia abitazione" (highlighted with a red box)

**Right Editor (HMDHomeLocationData.plist):**

- Line 1: <Dictionary>
- Line 2: S ClassName = "HMDHomeLocationData"
- Line 3: B homeLocation
- Line 4: S ClassName = "CLLocation"
- Line 5: R kCLLocationCodingKeyHorizontalAccuracy = 65
- Line 6: B kCLLocationCodingKeyType = 4
- Line 7: B kCLLocationCodingKeyGroundAltitude
- Line 8: R kCLLocationCodingKeyCoordinateLongitude = 8,93557236487001 (highlighted with a red box)
- Line 9: B kCLLocationCodingKeyFloor = 2147483647
- Line 10: R kCLLocationCodingKeyCourse = -1
- Line 11: B kCLLocationCodingKeyIntegrity = 25
- Line 12: B kCLLocationCodingKeyMatchInfo
- Line 13: R kCLLocationCodingKeySpeedAccuracy = -1
- Line 14: R kCLLocationCodingKeyLifespan = 9
- Line 15: R kCLLocationCodingKeyCoordinateLatitude = 44,4061081898348 (highlighted with a red box)
- Line 16: R kCLLocationCodingKeyVerticalAccuracy = 10
- Line 17: B reserved = 1
- Line 18: R kCLLocationCodingKeyAltitude = 22,0447864532471
- Line 19: R kCLLocationCodingKeyTimestamp = 604306351,096622
- Line 20: R kCLLocationCodingKeySpeed = -1
- Line 21: R homeLocationNextUpdate = 604306653,113131

# DATASTORE.SQLITE

## HMDRoomModel / HMDAppleMediaAccessoryModel

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

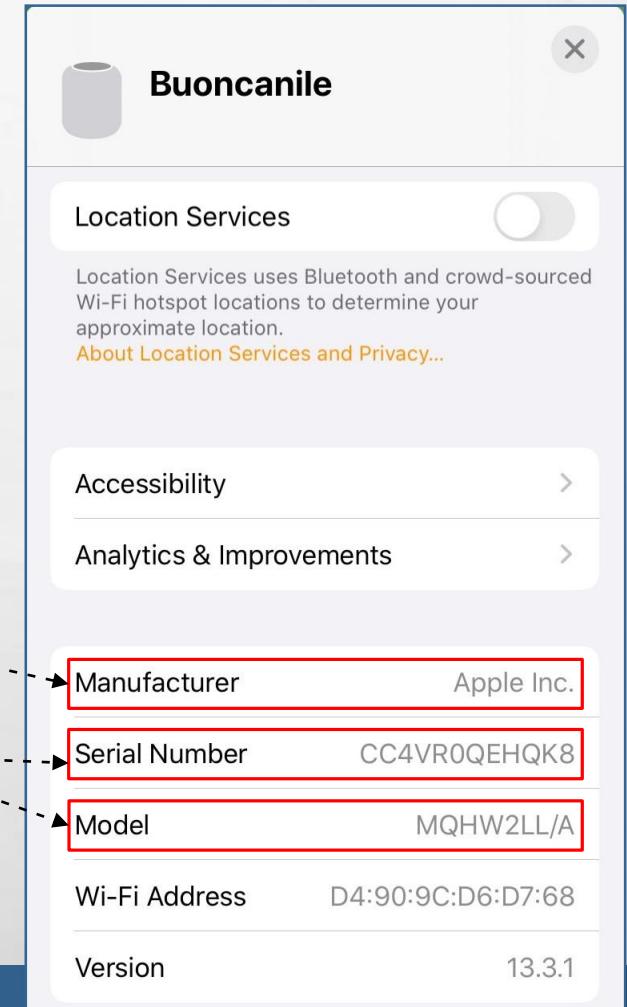
Filter in any column

	e_id	name	type	uuid	parent_uuid	encoding	record	data
		Filter	Filter	Filter	Filter	Filter	Filter	Filter
73	1	9BF59942-0654-4350-8125-4133A1850961	HMDActionSetModel	976D30EC-E24A-52DA-921B-83B9B6685934	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
74	1	B5094766-7F20-4C73-8188-EA51CD5786CC	HMDUserModel	A4A32D3D-59AF-4F47-981B-2D2BD1E34065	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
75	1	93B78C42-E385-493D-B4A9-264CE1589117	HMDActionSetModel	E1AAAE36-31B5-5433-B73C-1A82AD218D1A	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
76	1	41396CF7-DECC-414E-BC5E-8098A6ECF15D	HMDHomeNetworkRouterSettingsModel	4C439A6B-F1E4-52DB-A541-8B2FC9D745EC	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
77	1	EA9CE1F7-66E3-4BDC-B4C2-F1E16E86FBCA	HMDHomeNetworkRouterManagingDeviceSetting...	EC205060-73E2-5550-AACA-D4B09573B160	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
78	1	3A56BCA1-E636-48D7-B9A3-3F803D56013D	HMDActionSetModel	113E9DA9-9B4D-58B0-B8D5-0C5EFBE3580F	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
79	1	66F2DE08-8ED5-4BA5-AFBD-EA0C99000000	9 HMDActionSetModel	C612DD2C-E416-55BD-AD8A-2EA4C23C776C	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
80	1	5DECAC1E-C6FB-41EB-9833-2CEA80000000	HMDRoomModel	04C5D232-98E0-5732-ABEE-A6AEC0010B0C	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
81	1	6CA11486-01E1-46D5-968A-8F3D00000000	HMDRoomModel	6B76D45C-3257-4DE9-A00F-8F724CB0D4E8	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
82	1	D50296B2-138D-4245-B28F-15A0000000000	HMDRoomModel	8E714D75-8B62-50B7-9D94-3A9839F2BCE9	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
83	1	83026FA1-202C-4DD5-A8EF-A19D00000000	HMDHomeSettingsMode	3C8210A3-D3E4-5662-A9A0-ECA8464DC528	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
84	1	D563AB7A-21CC-49C3-809C-7D3B82660EE7	HMDResidentDeviceModel	DBACBD84-0916-5FA2-9943-15C93517B9EB	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
85	1	BDDA5512-7F96-4655-9D6D-776ECA3BE456	HMDRoomModel	32180983-7A6E-4C41-8EC8-0E1D348BB0D60	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
86	1	D13BB7B2-9501-475B-AA9B-9CEA534D0D08	HMDRoomModel	3886FDCB-7840-47FA-B0B8-A8DC389F31B5	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
87	1	A40327ED-116E-487F-8068-C0B846770000	HMDActionSetModel	6-B210-50C268CC6645	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
88	1	F0200FCB-61F8-41C6-9766-4F1964000000	HMDRoomModel	2-831C-C11FA06536A3	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
89	1	525B1827-0333-4B40-8E8D-DBF473000000	HMDAppleMediaAccessoryModel	1-ABF3-C8B0BDB1E256	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
90	1	38E268B0-9334-45FF-8719-40F8EFL000000	HMDAccessoryTransaction	F-BEAE-07A03DFA0D76	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
91	1	1204E7FF-407D-4699-A563-2FAB0A000000	HMDAccessoryTransaction	7-A4A3-569D81B296A4	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB

# HOMEPOD INFORMATION

## HMDAppleMediaAccessoryModel

Key	Type	Value
I accessoryCategory	Integer	25
S appleMediaAccessoryChan...	String	A06CAAF2-0049-4037-85BA-827E66C3AF62
S configurationAppIdentifier	String	com.apple.SharingViewService
S configuredName	String	Buoncanile
D device	Array	2 objects
S deviceUUID	String	DAD423DA-F06A-58A9-9205-BA4F6F838DD8
S firmwareVersion	String	13.3.1 (17D50)
S identifier	String	B40BD6EA-126C-4C38-AE0F-698CE3048132
D loggedInAccount	Array	2 objects
S manufacturer	String	Apple Inc.
S model	String	MQHW2LL/A
S name	String	Buoncanile
D pairingIdentity	Array	2 objects
S providedName	String	HomePod
S roomUUID	String	3886FDCB-7840-47FA-B0B8-A8DC389F31B5
S serialNumber	String	CC4VR0QEHQK8
D softwareVersion	Array	2 objects
D symptoms	Array	2 objects
D wifiNetworkInfo	Array	2 objects
S _P	String	8F4D7D36-91CB-43EA-8250-31FEC09DE463
S _t	String	HMDAppleMediaAccessoryModel
S _u	String	4952117C-F0B4-57A1-ABF3-C8B0BDB1E256
S _v	String	6.2

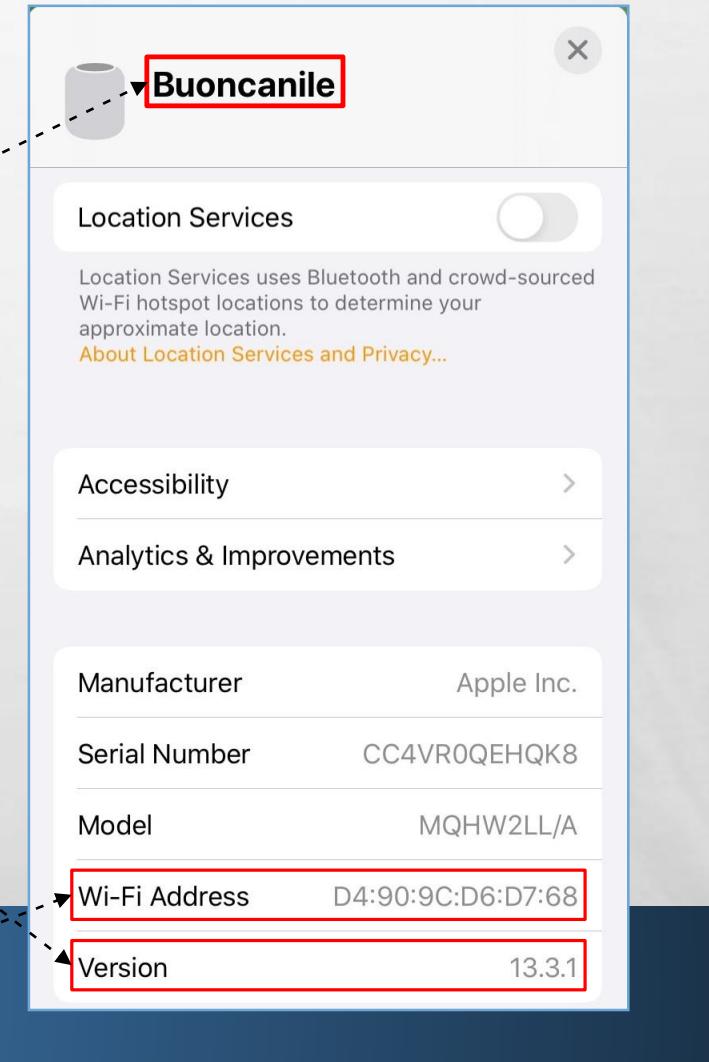


# HOMEPOD INFORMATION

## HMDAppleMediaAccessoryModel

Key	Type	Value
I accessoryCategory	Integer	25
S appleMediaAccessoryChan...	String	A06CAAF2-0049-4037-85BA-827E66C3AF62
S configurationAppIdentifier	String	com.apple.SharingViewService
S configuredName	String	Buoncanile
device	Array	2 objects
S deviceUUID	String	DAD423DA-F06A-58A9-9205-BA4F6F838DD8
S firmwareVersion	String	13.3.1 (17D50)
S identifier	String	B40BD6EA-126C-4C38-AE0F-698CE3048132
loggedInAccount	Array	2 objects
S manufacturer	String	Apple Inc.
S model	String	MQHW2LL/A
S name	String	Buoncanile
pairingIdentity	Array	2 objects
S providedName	String	HomePod
S roomUUID	String	3886FDDB-7840-47FA-B0B8-A8DC389F31B5
S serialNumber	String	CC4VR0QEHQK8
softwareVersion	Array	2 objects
symptoms	Array	2 objects
wifiNetworkInfo	Array	2 objects
S _P	String	8F4D7D36-91CB-43EA-8250-2455600B5463
S _t	String	HMDAppleMediaAccessory
S _u	String	4952117C-F0B4-57A1-AB
S _y	String	6.2

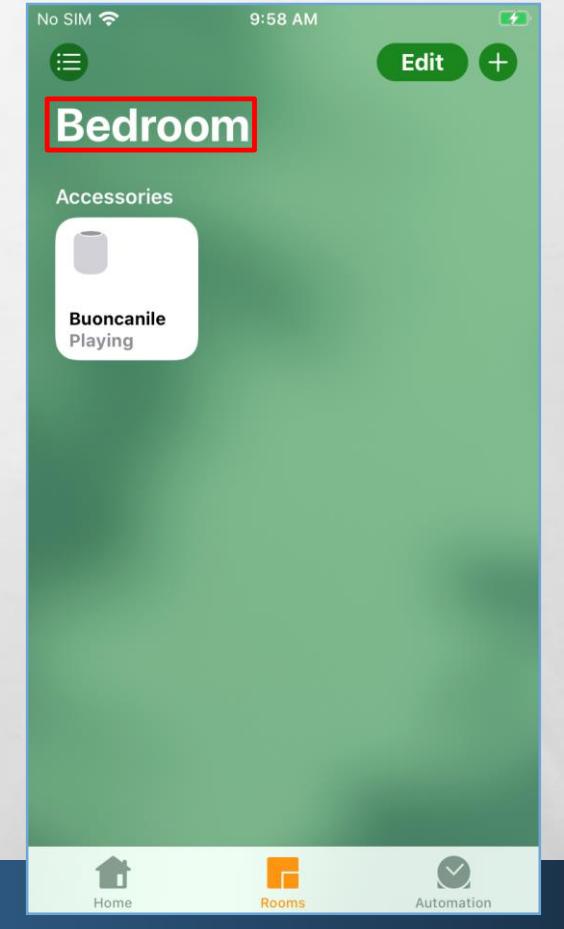
```
wifiNetworkInfo : bplist = {
    HMF.SSID : AsciiString = rmsys
    HMF.MACAddress : HMFMACAddress = {
        HMF.data : data = D4 90 9C D6 D7 68
    }
}
```



# HOMEPOD ROOM INFORMATION

## HMDAppleMediaAccessoryModel / HMDRoomModel

Key	Type	Value
I accessoryCategory	Integer	25
S appleMediaAccessoryChan...	String	A06CAAF2-0049-4037-85BA-827E66C
S configurationAppIdentifier	String	com.apple.SharingViewService
S configuredName	String	Buoncanile
D device	Array	2 objects
S deviceUUID	String	DAD423DA-F06A-58A9-9205-BA4F6F8
S firmwareVersion	String	13.3.1 (17D50)
S identifier	String	B40BD6EA-126C-4C38-AE0F-698CE30
D loggedInAccount	Array	2 objects
S manufacturer	String	Apple Inc.
S model	String	MQHW2LL/A
S name	pairingIdentity	Array
S providedName	String	HomePod
S roomUUID	String	3886FDCB-7840-47FA-B0B8-A8DC389F31B5
S serialNumber	String	CC4VR0QEHQK8
S softwareVersion	Array	2 objects
S symptoms	Array	2 objects
D wifiNetworkInfo	Array	2 objects
S _P		4952117C-F0B4-57A1-ABF3-C8B0BDB1E256
S _t		
S _u		
S _v		



# DATASTORE.SQLITE

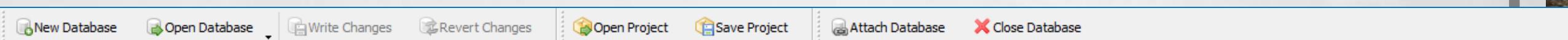
## HMDAccessorySettingGroupModel

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

Filter in any column

e_id	name	type	uuid	parent_uuid	encoding	record	data
41	1 8742C517-7B43-4553-B5DB-9CDB59AA582B	HMDAccessorySettingGroupModel	9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9	4952117C-F0B4-57A1-ABF3-C8B0BDB1E256	1	BLOB	BLOB
42	1 DEC4E145-8334-4C2D-B867-E98842CF20D4	HMDSoftwareUpdateModel	AF81A457-1F75-51ED-ABBD-D4B422C8A284	4952117C-F0B4-57A1-ABF3-C8B0BDB1E256	1	BLOB	BLOB
43	1 A8740A9B-B2A4-4295-8D64-BEDE74211728	HMDApplicationDataModel	EA43BBAE-EDD0-5D6C-9B91-15C5B20C4748	4952117C-F0B4-57A1-ABF3-C8B0BDB1E256	1	BLOB	BLOB



Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

Filter in any column

tore_id	name	type	uuid	parent_uuid	encoding	record	data
198	1 A7653A32-2C92-4111-8026-436D95367220	HMDAccessorySettingGroupModel	EA9814ED-AE03-42A6-9C29-39F84FFF5523	9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9	1	BLOB	BLOB
199	1 D6896D7D-35B9-421D-BE8C-B5B2F3EE06B9	HMDAccessorySettingGroupModel	C96B47A2-D8BB-42A3-9342-7FA5CF5CF3B1	9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9	1	BLOB	BLOB
200	1 D412F0D7-F004-445B-B816-996E952E4EFA	HMDAccessorySettingGroupModel	FC2D71B8-9D5E-4F45-AE51-F56F7FAE7919	9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9	1	BLOB	BLOB
201	1 1AF8F5DC-DDEE-4071-B58F-5958A36C75AE	HMDAccessorySettingGroupModel	DB13BB40-2ADB-4EB3-95D1-48D82E8EF25C	9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9	1	BLOB	BLOB
202	1 E3AA9E20-4DB2-4D36-B046-6F9DEA66B5E8	HMDAccessorySettingGroupModel	26710BA8-6619-4935-93A2-D98CE19523D9	9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9	1	BLOB	BLOB
203	1 4E947EDD-C231-473C-BDBA-83409CB4C2D3	HMDAccessorySettingGroupModel	515794C1-0680-4B82-93EA-C2645F5213AE	9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9	1	BLOB	BLOB

# HOMEPOD MUSIC SETTINGS

Hex Plist

```
1 1 <Dictionary>
2   S _P = "9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9"
3   S _V = "4.1.1"
4   S name = "music"
5   S _u = "26710BA8-6619-4935-93A2-D98CE19523D9"
6   S _t = "HMDAccessorySettingGroupModel"
```

Database Structure Browse Data Edit Pragmas Execute SQL

Table: record

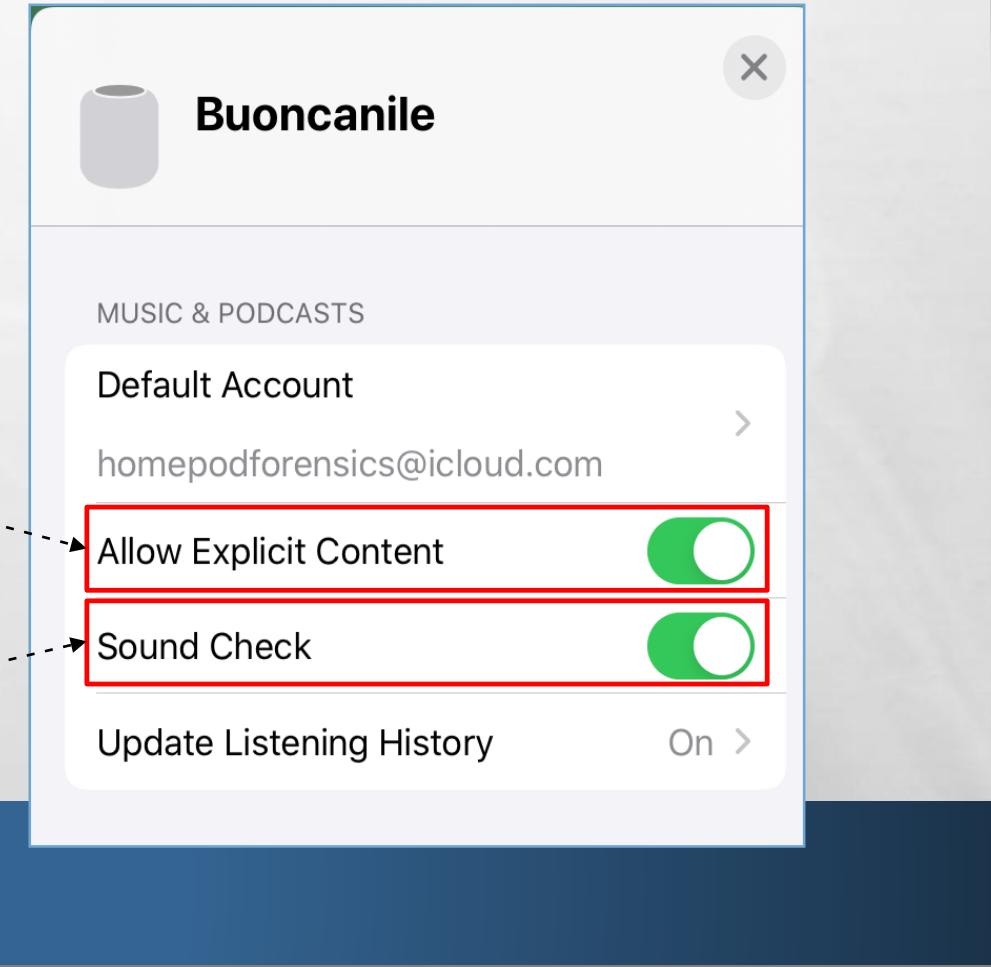
Filter in any column

	tore_id	name	type	uuid	parent_uuid <small>*1</small>	encoding	record	data
20	ter	FB8CBBB7-864D-4E91-88FB-876EC32CC44A	HMDAccessorySettingModel	67C2F3C3-B3F6-4427-A81C-C1D50B8706E8	26710BA8-6619-4935-93A2-D98CE19523D9	1	BLOB	BLOB
21		85AC45FE-F8DF-48A7-8411-667057E7EFC9	HMDAccessorySettingModel	474E6002-385F-4966-B1AA-EBAFE8E277E4	26710BA8-6619-4935-93A2-D98CE19523D9	1	BLOB	BLOB
22		C8193D50-D16E-4B04-A402-8A1D3C4C6C78	HMDAccessorySettingModel	77F45335-24B5-4322-A50F-A3B7EB4CF742	26710BA8-6619-4935-93A2-D98CE19523D9	1	BLOB	BLOB

# HOMEPOD MUSIC SETTINGS

```
◀ NSMutableDictionary = {  
    _P : AsciiString = 26710BA8-6619-4935-93A2-D98CE19523D9  
    _u : AsciiString = 474E6002-385F-4966-B1AA-EBAFE8E277E4  
    configurationVersion : integer = 6  
    _V : AsciiString = 4.1.1  
    properties : integer = 3  
    value : bplist = True  
    type : integer = 2  
    name : AsciiString = allowExplicitContent  
    _t : AsciiString = HMDAccessorySettingModel
```

```
◀ NSMutableDictionary = {  
    _P : AsciiString = 26710BA8-6619-4935-93A2-D98CE19523D9  
    _u : AsciiString = 77F45335-24B5-4322-A50F-A3B7EB4CF742  
    configurationVersion : integer = 5  
    _V : AsciiString = 4.1.1  
    properties : integer = 3  
    value : bplist = True  
    type : integer = 2  
    name : AsciiString = soundCheck  
    _t : AsciiString = HMDAccessorySettingModel
```



# HOMEPOD SIRI SETTINGS

Hex Plist

```
1  ⌂ <Dictionary>
2  S, _P = "9C3C5B09-8A6A-44CE-861F-0C3A6CF453E9"
3  S, V = "4.1.1"
4  S, name = "siri"
5  S, _u = "EA9814ED-AE03-42A6-9C29-39F84FFF5523"
6  S, _t = "HMDAccessorySettingGroupModel"
```

record

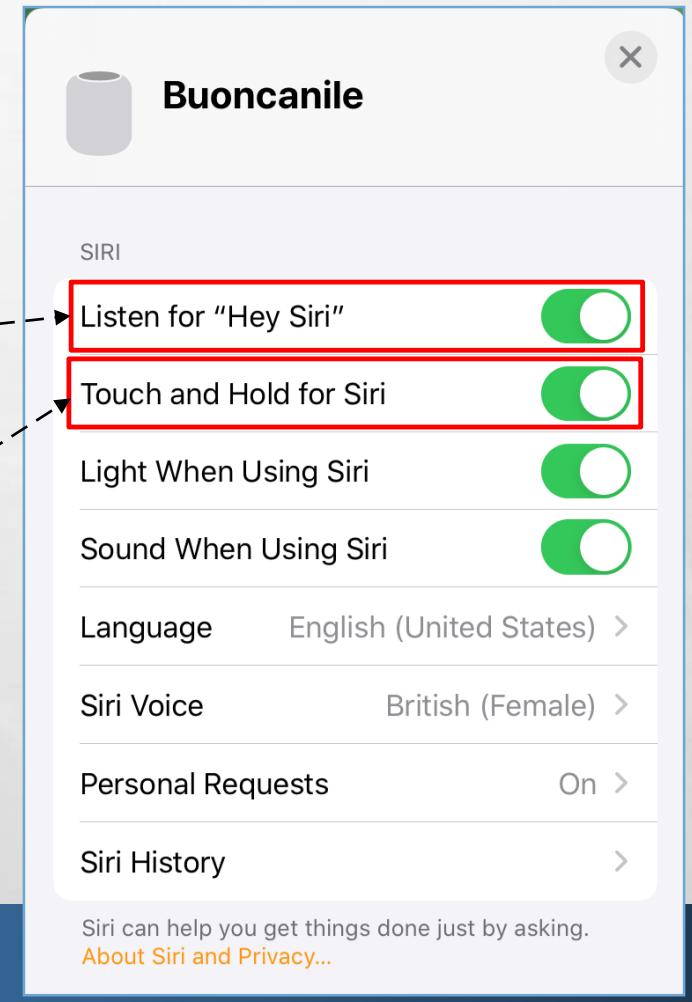
Filter in any column

store_id	name	type	uuid	parent_uuid	encoding	record	data
1	00F4D278-DCF9-471D-97D9-A0A3DE862A55	HMDAccessorySettingModel	D17AFDA6-DB46-4D4A-B7A0-3483C8E2552B	EA9814ED-AE03-42A6-9C29-39F84FFF5523	1	BLOB	BLOB
1	7EF65293-C215-4E10-B82E-84D35D77F0F0	HMDAccessorySettingModel	C2BEED0B-FF3E-413A-9B1F-3959FA265888	EA9814ED-AE03-42A6-9C29-39F84FFF5523	1	BLOB	BLOB
1	1BF08CFC-343E-431B-AFB0-44272154668F	HMDAccessorySettingModel	CAE0CEFE-EAC9-4D7A-98D9-BC9DCCA325B1	EA9814ED-AE03-42A6-9C29-39F84FFF5523	1	BLOB	BLOB
1	8C9C8BAB-FCF9-4A4D-B077-1742DE34827F	HMDAccessorySettingModel	64610117-E34B-4C32-9917-E92F562A5F8F	EA9814ED-AE03-42A6-9C29-39F84FFF5523	1	BLOB	BLOB
1	E02B6D1B-76B2-4D3D-B4A2-997629C11FB9	HMDAccessorySettingModel	9D167C58-7A94-445D-9E1C-619BA52FC4C1	EA9814ED-AE03-42A6-9C29-39F84FFF5523	1	BLOB	BLOB

# HOMEPOD SIRI SETTINGS

```
◀ NSMutableDictionary = {  
    _P : AsciiString = EA9814ED-AE03-42A6-9C29-39F84FFF5523  
    _u : AsciiString = CAE0CEFE-EAC9-4D7A-98D9-BC9DCCA325B1  
    configurationVersion : integer = 6  
    _V : AsciiString = 4.1.1  
    properties : integer = 3  
    value : bplist = True  
    type : integer = 2  
    name : AsciiString = allowHeySiri  
    _t : AsciiString = HMDAccessorySettingModel
```

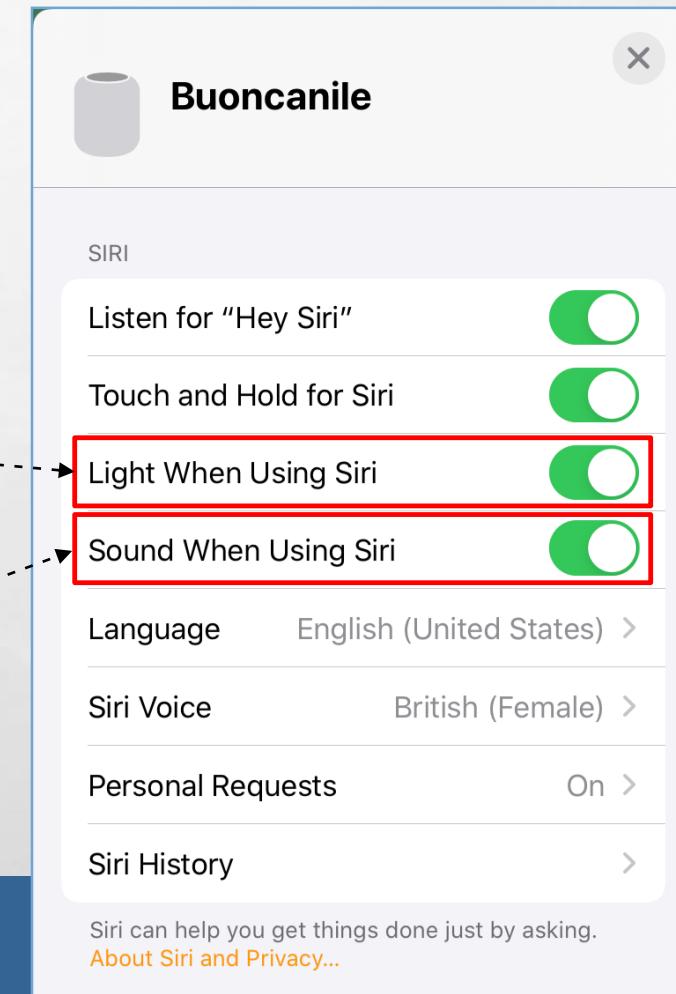
```
◀ NSMutableDictionary = {  
    _P : AsciiString = EA9814ED-AE03-42A6-9C29-39F84FFF5523  
    _u : AsciiString = C2BEED0B-FF3E-413A-9B1F-3959FA265888  
    configurationVersion : integer = 4  
    _V : AsciiString = 4.1.1  
    properties : integer = 3  
    value : bplist = True  
    type : integer = 2  
    name : AsciiString = tapToAccess  
    _t : AsciiString = HMDAccessorySettingModel
```



# HOMEPOD SIRI SETTINGS

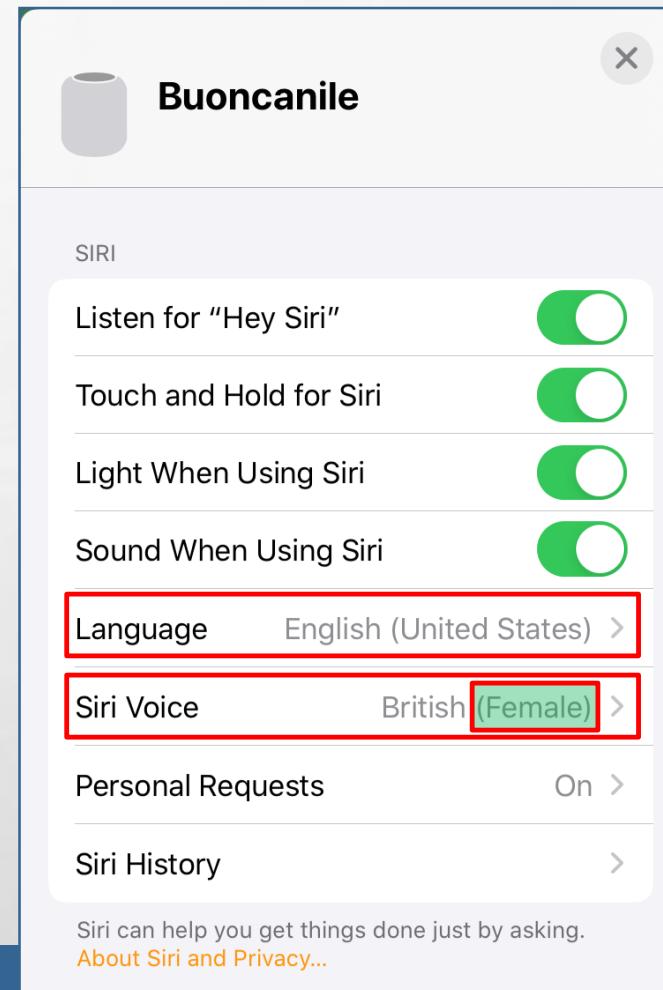
```
◀ NSMutableDictionary = {  
    _P : AsciiString = EA9814ED-AE03-42A6-9C29-39F84FFF5523  
    _u : AsciiString = 64610117-E34B-4C32-9917-E92F562A5F8F  
    configurationVersion : integer = 6  
    _V : AsciiString = 4.1.1  
    properties : integer = 3  
    value : bplist = True  
    type : integer = 2  
    name : AsciiString = lightWhenUsingSiri  
    _t : AsciiString = HMDAccessorySettingModel
```

```
◀ NSMutableDictionary = {  
    _P : AsciiString = EA9814ED-AE03-42A6-9C29-39F84FFF5523  
    _u : AsciiString = 9D167C58-7A94-445D-9E1C-619BA52FC4C1  
    configurationVersion : integer = 5  
    _V : AsciiString = 4.1.1  
    properties : integer = 3  
    value : bplist = True  
    type : integer = 2  
    name : AsciiString = soundAlert  
    _t : AsciiString = HMDAccessorySettingModel
```



# HOMEPOD SIRI SETTINGS

```
NSMutableDictionary = {  
    _P : AsciiString = EA9814ED-AE03-42A6-9C29-39F84FFF5523  
    _u : AsciiString = D17AFDA6-DB46-4D4A-B7A0-3483C8E2552B  
    configurationVersion : integer = 4  
    _V : AsciiString = 4.1.1  
    properties : integer = 3  
    value : bplist = {  
        HM.identifier : NSUUID = 67b2c439-f03a-804e-b5a5-6d4bab7edabc  
        HM.title : AsciiString = en-US|en-GB|  
        type : integer = 4  
        name : AsciiString = language  
        _t : AsciiString = HMDAccessorySettingModel}
```



# HOMEPOD INFORMATION

/private/var/mobile/Library/Caches/com.Apple.Homekit.Configurations/homeData.\*.Config

Key	Type	Value
	dict	
	dict	
	string	4952117C-F0B4-57A1-ABF3-C8B0BDB1E256
	string	Buoncanile
	string	CC4VR0QEHQK8
	string	Apple Inc.
\$class	dict	
NS.string	dict	
	string	MQHW2LL/A
	dict	
	string	13.3.1
	dict	
	string	1D8FD40E-7CAE-4AD5-9973-977D18890DE2
	string	HomePod
	dict	
	string	com.apple.SharingViewService
	dict	
	string	Bedroom
	string	3886FDCB-7840-47FA-B0B8-A8DC389F31B5
	dict	
	string	B40BD6EA-126C-4C38-AE0F-698CE3048132

string	Buoncanile
dict	
string	IRK
data	...
dict	
dict	
string	17D50
dict	
dict	
dict	
data	...
dict	
string	
dict	
Position:	0 / 5 (0%)
00000000:	D4 90 9C D6 D7 68

# HOMEPOD MUSIC PLAYBACK

/private/var/mobile/Library/com.apple.siri.inference/srdb.db

Tables	
<b>srdb.db (main)</b>	
<input checked="" type="checkbox"/>	configs(3/0)
<input checked="" type="checkbox"/>	entities(3/0)
<input checked="" type="checkbox"/>	entities_fts_config(1/0)
<input checked="" type="checkbox"/>	entities_fts_data(3/0)
<input checked="" type="checkbox"/>	entities_fts_docsizes(3/0)
<input checked="" type="checkbox"/>	entities_fts_idx(1/0)
<input checked="" type="checkbox"/>	intent_entities(12/0)
<input checked="" type="checkbox"/>	intents(6/0)
<input type="checkbox"/>	All Deleted Data

#	id	type	srid	content_tokens	created_at	modified_at
1	1	INMediaItem	mpc-item://com.apple.Music/playlistEntry?storeAdamID=...	saint cecilia zzzsong	2020-02-17T11:01:02.090Z	2020-02-25T09:14:02.833Z
2	2	INMediaItem	mpc-container://com.apple.Music/playlist?databaseID=2...	acquisti zzplaylist	2020-02-17T11:01:02.090Z	2020-02-25T09:14:02.833Z
3	3	INMediaItem	mpc-item://com.apple.Music/playlistEntry?storeAdamID=...	savior breath zzzsong	2020-02-25T09:10:00.707Z	2020-02-25T09:10:00.707Z

Tables	
<b>srdb.db (main)</b>	
<input checked="" type="checkbox"/>	configs(3/0)
<input checked="" type="checkbox"/>	entities(3/0)
<input checked="" type="checkbox"/>	entities_fts_config(1/0)
<input checked="" type="checkbox"/>	entities_fts_data(3/0)
<input checked="" type="checkbox"/>	entities_fts_docsizes(3/0)
<input checked="" type="checkbox"/>	entities_fts_idx(1/0)
<input checked="" type="checkbox"/>	intent_entities(12/0)
<input checked="" type="checkbox"/>	intents(6/0)
<input type="checkbox"/>	All Deleted Data

#	id	domain	verb	bundle_id	created_at	modified_at
1	1	Media	PlayMedia	com.apple.Music	2020-02-17T11:01:02.090Z	2020-02-17T11:01:02.090Z
2	2	Media	PlayMedia	com.apple.Music	2020-02-17T11:01:03.758Z	2020-02-17T11:01:03.758Z
3	3	Media	PlayMedia	com.apple.Music	2020-02-25T09:10:00.707Z	2020-02-25T09:10:00.707Z
4	4	Media	PlayMedia	com.apple.Music	2020-02-25T09:13:31.616Z	2020-02-25T09:13:31.616Z
5	5	Media	PlayMedia	com.apple.Music	2020-02-25T09:13:59.592Z	2020-02-25T09:13:59.592Z
6	6	Media	PlayMedia	com.apple.Music	2020-02-25T09:14:02.833Z	2020-02-25T09:14:02.833Z



# HOMEPOD MUSIC PLAYBACK

## /private/var/mobile/CoreDuet/Knowledge/knowledgeC.db

```
SELECT DATETIME(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') AS "START",
       DATETIME(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') AS "END",
       ZSTREAMNAME AS "STREAM NAME", ZVALUESTRING AS "VALUE STRING",
       Z_DKNOPLAYINGMETADATAKEY__TITLE AS "TITLE",
       Z_DKNOPLAYINGMETADATAKEY__ARTIST AS "ARTIST",
       Z_DKNOPLAYINGMETADATAKEY__ALBUM AS "ALBUM",
       Z_DKNOPLAYINGMETADATAKEY__DURATION AS "DURATION",
       Z_DKNOPLAYINGMETADATAKEY__GENRE AS "GENRE",
       Z_DKNOPLAYINGMETADATAKEY__MEDIATYPE AS "MEDIA TYPE",
       Z_DKNOPLAYINGMETADATAKEY__OUTPUTDEVICEIDS AS "OUTPUT DEVICE ID"
FROM ZSTRUCTUREDMETADATA JOIN ZOBJECT
ON ZOBJECT.ZSTRUCTUREDMETADATA = ZSTRUCTUREDMETADATA.Z_PK
ORDER BY ZOBJECT.ZSTARTDATE
```

# HOMEPOD MUSIC PLAYBACK

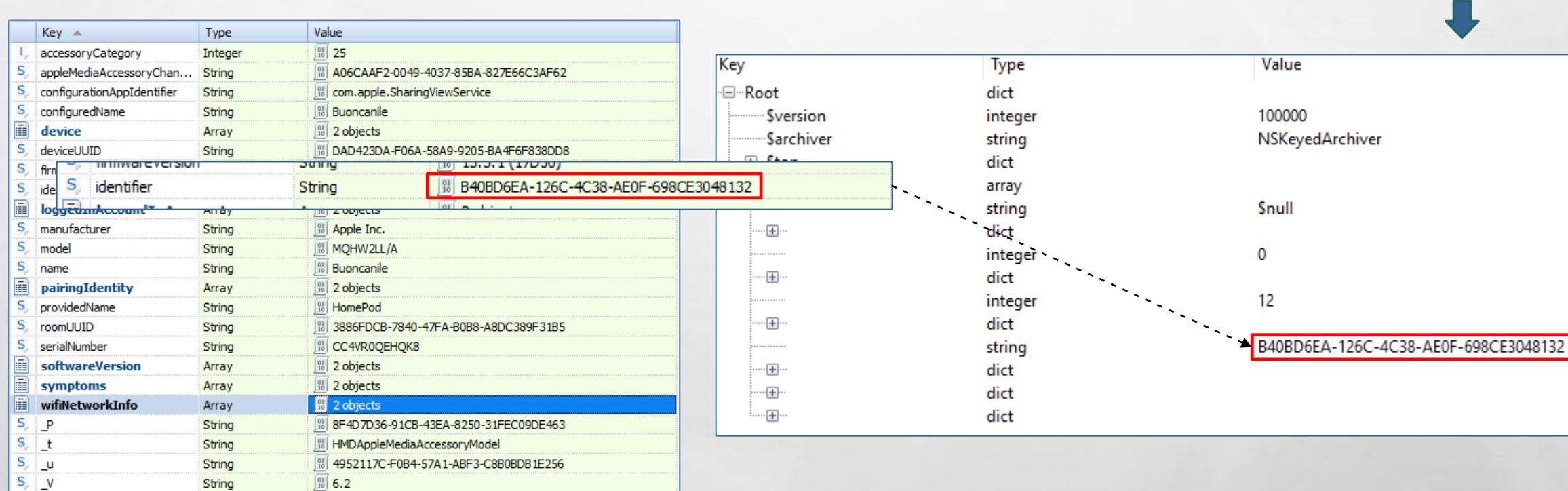
/private/var/mobile/CoreDuet/Knowledge/knowledgeC.db

#		START	END	STREAM NAME	VALUE STRING	TITLE ▾	ARTIST	ALBUM	DURATION	GENRE	MEDIA TYPE	OUTPUT DEVICE ID
1	<input checked="" type="checkbox"/>	2020-02-17 09:55:18	2020-02-17 11:01:01	/media/nowPlaying	com.apple.Music	The Neverending Sigh	Foo Fighters	Saint Cecilia - EP	285,257142857143	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
2	<input checked="" type="checkbox"/>	2020-02-17 09:55:12	2020-02-17 09:55:12	/media/nowPlaying	com.apple.Music	The Neverending Sigh	Foo Fighters	Saint Cecilia - EP	285,257142857143	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
3	<input checked="" type="checkbox"/>	2020-02-17 09:55:12	2020-02-17 09:55:12	/media/nowPlaying	com.apple.Music	The Neverending Sigh	Foo Fighters	Saint Cecilia - EP	285,257142857143	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
4	<input checked="" type="checkbox"/>	2020-02-17 09:55:12	2020-02-17 09:55:18	/media/nowPlaying	com.apple.Music	The Neverending Sigh	Foo Fighters	Saint Cecilia - EP	285,257142857143	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
5	<input checked="" type="checkbox"/>	2020-01-28 09:26:34	2020-01-28 09:26:34	/media/nowPlaying	com.apple.Music	Sean		Foo Fighters	131,401723356009	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
6	<input checked="" type="checkbox"/>	2020-01-28 09:26:34	2020-01-28 09:26:34	/media/nowPlaying	com.apple.Music	Sean		Foo Fighters	131,401723356009	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
7	<input checked="" type="checkbox"/>	2020-01-28 09:26:34	2020-01-28 09:26:34	/media/nowPlaying	com.apple.Music	Sean		Foo Fighters	131,401723356009	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
8	<input checked="" type="checkbox"/>	2020-01-28 09:26:34	2020-01-28 09:26:44	/media/nowPlaying	com.apple.Music	Sean		Foo Fighters	131,401723356009	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
9	<input checked="" type="checkbox"/>	2020-01-28 09:26:26	2020-01-28 09:26:26	/media/nowPlaying	com.apple.Music	Sean		Foo Fighters	131,333	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
10	<input checked="" type="checkbox"/>	2020-01-28 09:26:26	2020-01-28 09:26:34	/media/nowPlaying	com.apple.Music	Sean		Foo Fighters	131,401723356009	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
11	<input checked="" type="checkbox"/>	2020-02-25 09:14:02	2020-02-25 09:14:02	/media/nowPlaying	com.apple.Music	Savior Breath		Foo Fighters	191,285986394558	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
12	<input checked="" type="checkbox"/>	2020-02-25 09:11:41	2020-02-25 09:14:02	/media/nowPlaying	com.apple.Music	Savior Breath		Foo Fighters	191,285986394558	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
13	<input checked="" type="checkbox"/>	2020-02-25 09:10:00	2020-02-25 09:10:00	/media/nowPlaying	com.apple.Music	Savior Breath		Foo Fighters	191,285	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
14	<input checked="" type="checkbox"/>	2020-02-25 09:10:00	2020-02-25 09:11:41	/media/nowPlaying	com.apple.Music	Savior Breath		Foo Fighters	191,285986394558	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
15	<input checked="" type="checkbox"/>	2020-02-25 09:16:05	2020-02-25 09:22:40	/media/nowPlaying	com.apple.Music	Saint Cecilia		Foo Fighters	221,727346938775	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
16	<input checked="" type="checkbox"/>	2020-02-25 09:14:02	2020-02-25 09:14:02	/media/nowPlaying	com.apple.Music	Saint Cecilia		Foo Fighters	221,727	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
17	<input checked="" type="checkbox"/>	2020-02-25 09:14:02	2020-02-25 09:16:05	/media/nowPlaying	com.apple.Music	Saint Cecilia		Foo Fighters	221,727346938775	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
18	<input checked="" type="checkbox"/>	2020-02-17 11:01:03	2020-02-17 11:01:03	/media/nowPlaying	com.apple.Music	Saint Cecilia		Foo Fighters	221,727	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1
19	<input checked="" type="checkbox"/>	2020-02-17 11:01:03	2020-02-17 11:01:13	/media/nowPlaying	com.apple.Music	Saint Cecilia		Foo Fighters	221,727346938775	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□□X\$versionY\$archiver1

# HOMEPOD MUSIC PLAYBACK

## /private/var/mobile/CoreDuet/Knowledge/knowledgeC.db

17	<input checked="" type="checkbox"/>	2020-02-25 09:14:02	2020-02-25 09:16:05	/media/nowPlaying	com.apple.Music	Saint Cecilia	Foo Fighters	Saint Cecilia - EP	221,727346938775	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□X\$versionY\$archiverT\$tc
18	<input checked="" type="checkbox"/>	2020-02-17 11:01:03	2020-02-17 11:01:03	/media/nowPlaying	com.apple.Music	Saint Cecilia	Foo Fighters	Saint Cecilia - EP	221,727	Rock	MRMediaRemoteMediaTypeMusic	bplist00? □□□□X\$versionY\$archiverT\$tc



# DATA ANALYSIS - SYSDIAGNOSE

MATTIA EPIFANI

SANS DFIR SUMMIT

17<sup>TH</sup> JULY 2020



# HOMEPOD SYSDIAGNOSE

Nome	Ultima modifica	Tipo	Dimensione
ASPSnapshots	25/02/2020 16:59	Cartella di file	
crashes_and_spins	25/02/2020 16:59	Cartella di file	
errors	25/02/2020 16:59	Cartella di file	
ioreg	25/02/2020 16:59	Cartella di file	
logs	25/02/2020 16:59	Cartella di file	
PaxHeader	25/02/2020 16:59	Cartella di file	
Personalization	25/02/2020 16:59	Cartella di file	
Preferences	25/02/2020 16:59	Cartella di file	
RunningBoard	25/02/2020 16:59	Cartella di file	
summaries	25/02/2020 16:59	Cartella di file	
system_logs.logarchive	25/02/2020 16:59	Cartella di file	
TimezoneDB	25/02/2020 16:59	Cartella di file	
WiFi	25/02/2020 16:59	Cartella di file	

Nome	Ultima modifica	Tipo	Dimensione
apfs_stats.txt	25/02/2020 11:39	Documento di testo	14 KB
ckksctl_status.txt	25/02/2020 11:39	Documento di testo	10 KB
disks.txt	25/02/2020 11:38	Documento di testo	1 KB
error_log.txt	25/02/2020 11:38	Documento di testo	0 KB
fileproviderctl.log	25/02/2020 11:39	File LOG	0 KB
fileproviderctl_check.log	25/02/2020 11:39	File LOG	1 KB
fileproviderctl_dump.log	25/02/2020 11:39	File LOG	1 KB
hidutil.plist	25/02/2020 11:38	File PLIST	497 KB
kbdebug.txt	25/02/2020 11:38	Documento di testo	1 KB
lsaw.csstoredump	25/02/2020 11:38	File CSSTOREDUMP	3.879 KB
microstackshots	25/02/2020 11:39	File	10 KB
mount.txt	25/02/2020 11:38	Documento di testo	1 KB
night-shift.log	25/02/2020 11:39	File LOG	1 KB
oslog_archive_error.log	25/02/2020 11:39	File LOG	0 KB
otctl_status.txt	25/02/2020 11:39	Documento di testo	7 KB
pcsstatus.txt	25/02/2020 11:38	Documento di testo	21 KB
ps.txt	25/02/2020 11:38	Documento di testo	19 KB
ps_thread.txt	25/02/2020 11:38	Documento di testo	65 KB
README.txt	25/02/2020 11:38	Documento di testo	1 KB
security-syndiagnose.txt	25/02/2020 11:38	Documento di testo	269 KB
smcDiagnose.txt	25/02/2020 11:38	Documento di testo	1 KB
spindump-nosymbols.txt	25/02/2020 11:38	Documento di testo	576 KB
swutil_show.txt	25/02/2020 11:39	Documento di testo	1 KB
sysdiagnose.log	25/02/2020 11:39	File LOG	105 KB
tailspin-info.txt	25/02/2020 11:38	Documento di testo	1 KB
taskinfo.txt	25/02/2020 11:38	Documento di testo	1 KB
taskSummary.csv	25/02/2020 11:39	OpenOffice.org 1....	9 KB
vm_stat.txt	25/02/2020 11:38	Documento di testo	6 KB

# HOMEPOD INFORMATION

## /logs/Networking/preferences.plist

Key	Type	Value
Root	dict	
Sets	dict	
CurrentSet	string	/Sets/DDD76F4C-D8
NetworkServices	dict	
Model	string	B238aAP
System	dict	
Network	dict	
HostNames	dict	
LocalHostName	string	Buoncanile
System	dict	
ComputerNameEncoding	integer	134217984
ComputerName	string	Buoncanile
HostName	string	Buoncanile

# HOMEPOD BLUETOOTH ADDRESS

## /WiFi/bluetooth\_status.txt

```
# --- Bluetooth Status

Power : On
MAC Address : D4:90:9C:D6:D7:69
Discoverable : No
Connectable : No
Scanning : No
Devices : 2 (paired=2 cloud=2 connected=0)

iPhone di Homepod
Address : 317A801D-77E0-77BF-1972-96BC60D22E46
Paired : Yes
CloudPaired : Yes
Connected : No

19
Address : 6A65FCA5-AA6C-165F-3833-72A998191C3F
Paired : Yes
CloudPaired : Yes
Connected : No
```

# HOMEPOD WI-FI ADDRESS

## /WiFi/wifi\_status.txt

```
# --- Wi-Fi Status

MAC Address      : d4:90:9c:d6:d7:68
Interface Name   : en0
Power            : On [On]
Op Mode          : STA
SSID             : dfrws_rodeo_2020
BSSID            : c0:a0:bb:f1:ea:f8
RSSI             : -34 dBm
Noise            : -91 dBm
Tx Rate          : 24.0 Mbps
Security         : WPA/WPA2 Personal
PHY Mode         : 11n
MCS Index        : 15
Guard Interval   : 800
NSS               : 2
Channel          : 1 (20 MHz, Active)
Country Code     : IT
NetworkServiceID : 5395C805-DB65-44B1-B8AC-C2C2BD3CCF05
IPv4 Config Method : DHCP
IPv4 Address     : 10.7.7.13
```

# HOMEPOD WI-FI ADDRESS

## /WiFi/com.apple.wifi.plist

...+ RATES	array	
...CARPLAY_NETWORK	boolean	false
...+ BEACON_PROBE_INFO_PER_BSSID_LIST	array	
...networkKnownBSSListKey	array	
...+ RSN_IE	dict	
...SCAN_RESULT_FROM_PROBE_RSP	boolean	false
...SSID	data	...
...SSID_STR	string	dfrws_rodeo_2020
...Strength	real	0.949410
...80211W_ENABLED	boolean	true
...INSTANT_HOTSPOT_ASSOC	boolean	false
...CAPABILITIES	integer	1041
...BEACON_INT	integer	100
...AGE		
...WiFiNetworkAttributelsMoving		
...SNR		
...WiFiAutoInstantHotspotJoining		
...ScaledRSSI		
...addedAt		
...lastUpdated		
+ WPS_PROB_RESP_IE	dict	
...IE_KEY_WPS_UUID_E	data	
...IE_KEY_WPS_MANUFACTURER	string	D-Link Corporation
...IE_KEY_WPS_RESP_TYPE	integer	3
...IE_KEY_WPS_SERIAL_NUM	string	123456789012347
+ IE_KEY_WPS_PRIMARY_DEV_TYPE	dict	
...IE_KEY_WPS_MODEL_NAME	string	DAP-1360
...IE_KEY_WPS_MODEL_NUM	string	C1
...IE_KEY_WPS_DEV_NAME	string	DAP-1360
...IE_KEY_WPS_CFG_METHODS	integer	130
...IE_KEY_WPS_SC_STATE	integer	2
...FT_ENABLED		
...NOISE		
...ORIG_AGE		
+ WPA_IE	dict	
...RSSI	integer	-34
...BLW_MODE	integer	16

# HOMEPOD WI-FI ADDRESS

/WiFi/com.apple.wifi.plist

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

```
Running sysdiagnose-wifi-plist.py v2019-10-24 Version 1.0
```

```
=====
SSID_STR = dfrws_rodeo_2020
BSSID = c0:a0:bb:f1:ea:f8
IE_KEY_WPS_MANUFACTURER = D-Link Corporation
IE_KEY_WPS_SERIAL_NUM = 123456789012347
IE_KEY_WPS_MODEL_NAME = DAP-1360
IE_KEY_WPS_DEV_NAME = DAP-1360
enabled = True
=====
```

[https://github.com/cheeky4n6monkey/iOS\\_sysdiagnose\\_forensic\\_scripts/sysdiagnose-wifi-plist.py](https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts/sysdiagnose-wifi-plist.py)

# HOMEPOD MOBILE ACTIVATION LOGS

## /logs/MobileActivation/mobileactivationd.log.\*

```
Command Prompt  
28 Jan 2020 18:42:38 Mobile Activation Build Version = 17C54  
28 Jan 2020 18:42:39 Mobile Activation Hardware Model = B238aAP  
28 Jan 2020 18:42:39 Mobile Activation Product Type = AudioAccessory1,1  
28 Jan 2020 18:42:39 Mobile Activation Device Class = AudioAccessory  
  
28 Jan 2020 18:42:39 Upgraded from 15D61 to 17C54 [line 414]  
  
29 Jan 2020 02:01:59 Mobile Activation Startup [line 417]  
29 Jan 2020 02:01:59 Mobile Activation Build Version = 17D50  
29 Jan 2020 02:01:59 Mobile Activation Hardware Model = B238aAP  
29 Jan 2020 02:01:59 Mobile Activation Product Type = AudioAccessory1,1  
29 Jan 2020 02:01:59 Mobile Activation Device Class = AudioAccessory  
  
29 Jan 2020 02:01:59 Upgraded from 17C54 to 17D50 [line 431]  
  
29 Jan 2020 10:57:40 Mobile Activation Startup [line 433]  
29 Jan 2020 10:57:40 Mobile Activation Build Version = 17D50  
29 Jan 2020 10:57:40 Mobile Activation Hardware Model = B238aAP  
29 Jan 2020 10:57:40 Mobile Activation Product Type = AudioAccessory1,1  
29 Jan 2020 10:57:40 Mobile Activation Device Class = AudioAccessory  
  
17 Feb 2020 09:46:18 Mobile Activation Startup [line 448]  
17 Feb 2020 09:46:18 Mobile Activation Build Version = 17D50  
17 Feb 2020 09:46:18 Mobile Activation Hardware Model = B238aAP  
17 Feb 2020 09:46:18 Mobile Activation Product Type = AudioAccessory1,1  
17 Feb 2020 09:46:18 Mobile Activation Device Class = AudioAccessory  
  
17 Feb 2020 10:55:28 Mobile Activation Startup [line 463]  
17 Feb 2020 10:55:28 Mobile Activation Build Version = 17D50
```

# HOMEPOD POWERLOGS

## /logs/PowerLogs

Key	Activity	Output
Filtro	Filtro	Filtro
2020-02-25 09:23:20	Application Info	[TIMESTAMP: 2020-02-25 09:23:20] [APP NAME: AirMusic] [APP EXECUTABLE NAME: AirMusic] [BUNDLE ID: com.apple.Music] [APP
2020-02-25 09:23:20	Application Info	[TIMESTAMP: 2020-02-25 09:23:20] [APP NAME: AirPodcasts] [APP EXECUTABLE NAME: AirPodcasts] [BUNDLE ID: com.apple.podca
2020-02-25 09:23:20	Device Status	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:20] [DEVICE CONNECTABLE: NO] [DEVICE CONNECTED: NO] [DEVICE DISCOVERABLE:
2020-02-25 09:23:21	Application Info	[TIMESTAMP: 2020-02-25 09:23:21] [APP NAME: DiagnosticsService] [APP EXECUTABLE NAME: DiagnosticsService] [BUNDLE ID: co
2020-02-25 09:23:21	Application Info	[TIMESTAMP: 2020-02-25 09:23:21] [APP NAME: Ambient Sounds] [APP EXECUTABLE NAME: SoundScapes] [BUNDLE ID: com.apple
2020-02-25 09:23:21	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:21] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Au
2020-02-25 09:23:21	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:21] [VOLUME PERCENTAGE: 12.580643594264984] [MUTED: NO] [ORIGINAL_VOLUME_
2020-02-25 09:23:21	Network Usage	[TIMESTAMP: 2020-02-25 09:23:21] [INTERFACE: en0] [DOWN BYTES: 389068] [UP BYTES: 562936] [PLNETWORKAGENT_EVENTB
2020-02-25 09:35:49	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:35:49] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHONES CONNECTED: 0] [ORIGIN
2020-02-25 09:35:49	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:35:49] [VOLUME PERCENTAGE: 12.580643594264984] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 2020-02-25 09:35:49] [OFFSET_TIMESTAMP: 2020-02-25 09:3
2020-02-25 09:35:49	Network Usage	[TIMESTAMP: 2020-02-25 09:35:49] [INTERFACE: en0] [DOWN BYTES: 332329] [UP BYTES: 461652] [PLNETWORKAGENT_EVENTBACKWARD_CUMULATIVENETWORKUSAGE TABLE ID: 3]
2020-02-25 09:35:49	Network Usage	[TIMESTAMP: 2020-02-25 09:35:49] [INTERFACE: awdl0] [DOWN BYTES: 0] [UP BYTES: 260] [PLNETWORKAGENT_EVENTBACKWARD_CUMULATIVENETWORKUSAGE TABLE ID: 4]
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: amsaccounts] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 4156] [WIFI OUT: 983] [PL
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: timed] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 625] [WIFI OUT: 524] [PLPROCESS

<https://github.com/mac4n6/APOLLO>



# HOMEPOD POWERLOGS

## /logs/PowerLogs

Key	Activity	Output
Filtro	Filtro	Filtro
2020-02-25 09:23:20	Application Info	[TIMESTAMP: 2020-02-25 09:23:20] [APP NAME: AirMusic] [APP EXECUTABLE NAME: AirMusic] [BUNDLE ID: com.apple.Music] [APP BUILD VERSION: 1.0] [APP BUNDLE VERSION: 3.1] [APP TYPE: 3] [APP DELE
2020-02-25 09:23:20	Application Info	[TIMESTAMP: 2020-02-25 09:23:20] [APP NAME: AirPodcasts] [APP EXECUTABLE NAME: AirPodcasts] [BUNDLE ID: com.apple.podcasts] [APP BUILD VERSION: 1425.5] [APP BUNDLE VERSION: 3.9] [APP TYPE: 3] [APP DELE
2020-02-25 09:23:20	Device Status	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:20] [DEVICE CONNECTABLE: NO] [DEVICE CONNECTED: NO] [DEVICE DISCOVERABLE: NO] [DEVICE POWERED: YES] [ORIGINAL_BLUETOOTHSTATE_TIMESTAMP: 2020-02-25 09:23:20]
2020-02-25 09:23:21	Application Info	[TIMESTAMP: 2020-02-25 09:23:21] [APP NAME: DiagnosticsService] [APP EXECUTABLE NAME: DiagnosticsService] [BUNDLE ID: com.apple.DiagnosticsService] [APP BUILD VERSION: 11] [APP BUNDLE VERSION: 11]
2020-02-25 09:23:21	Device Status	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:21] [TIME ZONE NAME: Europe/Rome] [COUNTRY CODE: IT] [LOCALE ID: en_IT] [SECONDS FROM G
2020-02-25 09:23:21	Device State	[TIMESTAMP: 2020-02-25 09:23:21] [Volume: 12.580643594264984] [MUTED: NO] [PLAUDIOAGENT_EVENTFORWARD_OUTPUT TABLE ID: 1]
2020-02-25 09:23:21	Network Usage	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:21] [CURRENTSSID: BF25650C1124E918BB43E5E5273DE398] [CURRENTCHANNEL: 9] [OFFSET_TIMESTAMP: 2020-02-25 09:23:21]
2020-02-25 09:23:21	Network Usage	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:21] [CURRENTSSID: BF25650C1124E918BB43E5E5273DE398] [CURRENTCHANNEL: 9] [OFFSET_TIMESTAMP: 2020-02-25 09:23:21]
2020-02-25 09:35:49	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:35:49] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HE
2020-02-25 09:35:49	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:35:49] [VOLUME PERCENTAGE: 12.580643594264984] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 2020-02-25 09:35:49]
2020-02-25 09:35:49	Network Usage	[TIMESTAMP: 2020-02-25 09:35:49] [INTERFACE: en0] [DOWN BYTES: 332329] [UP BYTES: 461652] [PLNETWORKAGENT_EVENTBACKWARD_CU
2020-02-25 09:35:49	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:35:49] [VOLUME PERCENTAGE: 12.580643594264984] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 2020-02-25 09:35:49] [OFFSET_TIMESTAMP: 2020-02-25 09:35:49]
2020-02-25 09:35:49	Network Usage	[TIMESTAMP: 2020-02-25 09:35:49] [INTERFACE: en0] [DOWN BYTES: 332329] [UP BYTES: 461652] [PLNETWORKAGENT_EVENTBACKWARD_CUMULATIVENETWORKUSAGE TABLE ID: 3]
2020-02-25 09:35:49	Network Usage	[TIMESTAMP: 2020-02-25 09:35:49] [INTERFACE: awdl0] [DOWN BYTES: 0] [UP BYTES: 260] [PLNETWORKAGENT_EVENTBACKWARD_CUMULATIVENETWORKUSAGE TABLE ID: 4]
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: amsaccounts] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 4156] [WIFI OUT: 983] [PL

<https://github.com/mac4n6/APOLLO>



# HOMEPOD POWERLOGS

## /logs/PowerLogs

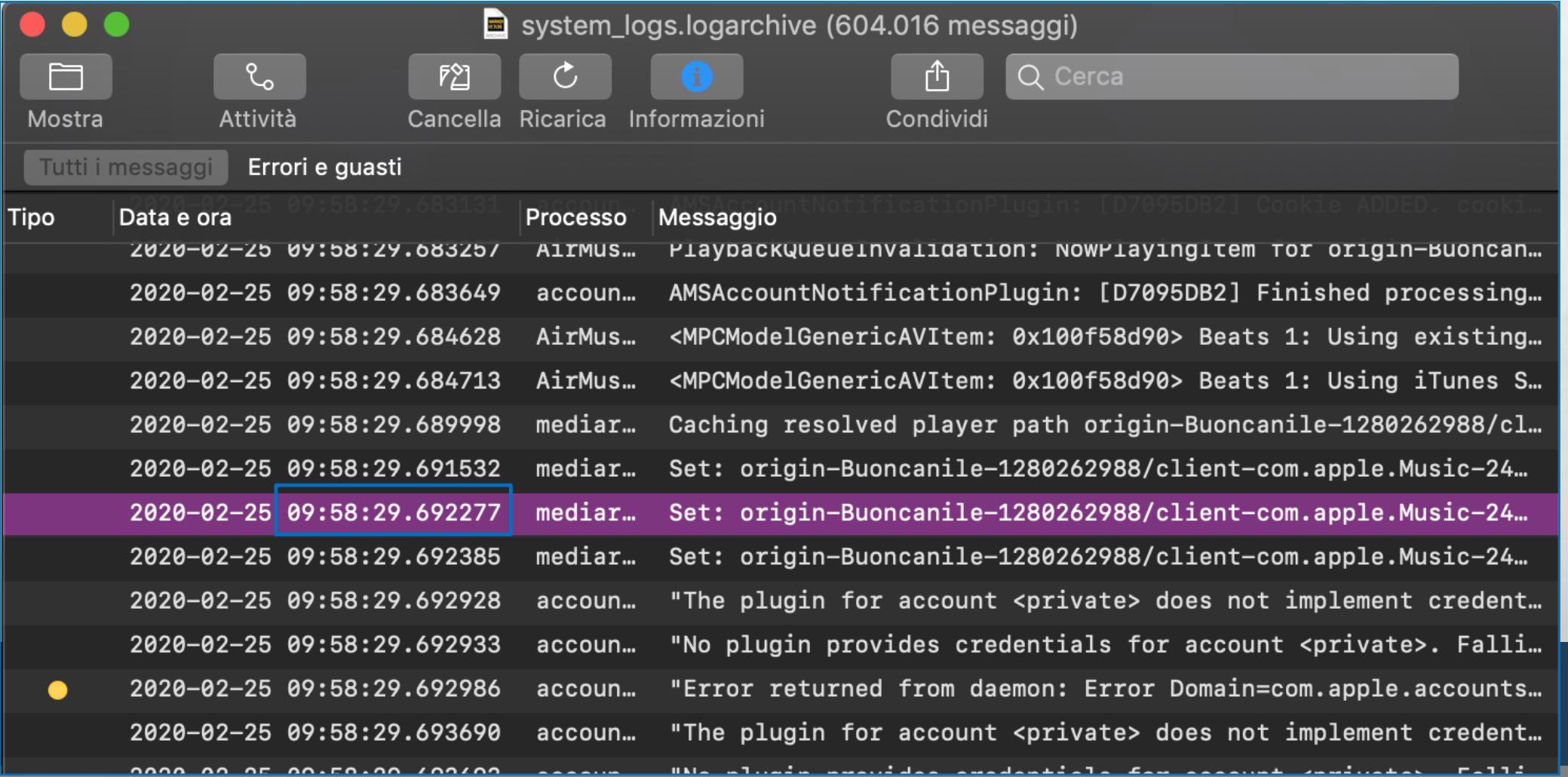
Key	Activity	Output
Filtro	Filtro	Filtro
2020-02-25 09:23:20	Application Info	[TIMESTAMP: 2020-02-25 09:23:20] [APP NAME: AirMusic] [APP EXECUTABLE NAME: AirMusic] [BUNDLE ID: com.apple.Music] [APP BUILD VERSION: 1.0] [APP BUNDLE VERSION: 3.1] [APP TYPE: 3] [APP DELE
2020-02-25 09:23:20	Application Info	[TIMESTAMP: 2020-02-25 09:23:20] [APP NAME: AirPodcasts] [APP EXECUTABLE NAME: AirPodcasts] [BUNDLE ID: com.apple.podcasts] [APP BUILD VERSION: 1425.5] [APP BUNDLE VERSION: 3.9] [APP TYPE:
2020-02-25 09:23:20	Device Status	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:20] [DEVICE CONNECTABLE: NO] [DEVICE CONNECTED: NO] [DEVICE DISCOVERABLE: NO] [DEVICE POWERED: YES] [ORIGINAL_BLUETOOTHSTATE_TIMESTAMP: 2
2020-02-25 09:23:21	Application Info	[TIMESTAMP: 2020-02-25 09:23:21] [APP NAME: DiagnosticsService] [APP EXECUTABLE NAME: DiagnosticsService] [BUNDLE ID: com.apple.DiagnosticsService] [APP BUILD VERSION: 1] [APP BUNDLE VERSION
2020-02-25 09:23:21	Application Info	[TIMESTAMP: 2020-02-25 09:23:21] [APP NAME: Ambient Sounds] [APP EXECUTABLE NAME: SoundScapes] [BUNDLE ID: com.apple.SoundScapes] [APP BUILD VERSION: 1] [APP BUNDLE VERSION: 1.0] [APP T
2020-02-25 09:23:21	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:21] [ACTIVEROUTE: Speaker] [ACTIVE: NO] [ACTIVE PID: 0] [OUTPUT CATEGORY: Audio/Video] [HEADSET HAS INPUT: 0] [HEADPHONES CONNECTED: 0] [ORIGIN
2020-02-25 09:23:21	Device State	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:21] [VOLUME PERCENTAGE: 12.580643594264984] [MUTED: NO] [ORIGINAL_VOLUME_TIMESTAMP: 2020-02-25 09:23:21] [OFFSET_TIMESTAMP: 2020-02-25 09:3
2020-02-25 09:23:21	Network Usage	[TIMESTAMP: 2020-02-25 09:23:21] [INTERFACE: en0] [DOWN BYTES: 389068] [UP BYTES: 562936] [PLNETWORKAGENT_EVENTBACKWARD_CUMULATIVENETWORKUSAGE TABLE ID: 1]
2020-02-25 09:23:21	Network Usage	[TIMESTAMP: 2020-02-25 09:23:21] [INTERFACE: awdl0] [DOWN BYTES: 0] [UP BYTES: 260] [PLNETWORKAGENT_EVENTBACKWARD_CUMULATIVENETWORKUSAGE TABLE ID: 2]
2020-02-25 09:23:21	Device Status	[ADJUSTED_TIMESTAMP: 2020-02-25 09:23:21] [TIMEZONE NAME: Europe/Rome] [COUNTRY CODE: IT] [LOCALE ID: it_IT] [SECONDS FROM CMT: 11] [TIMEZONE IN DST: 0] [TRIGGERED_BY_POWERDOWN] [OFFSET
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: amsaccounts] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 0] [WIFI OUT: 0] [BT IN: 0] [BT OUT: 0] [ETHERNET IN: 0] [ETHERNET OUT: 0] [USB IN: 0] [USB OUT: 0] [POWER IN: 0] [POWER OUT: 0] [CPU IN: 0] [CPU OUT: 0] [GPU IN: 0] [GPU OUT: 0] [HDD IN: 0] [HDD OUT: 0] [SSD IN: 0] [SSD OUT: 0] [FIR
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: timed] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 6] [WIFI OUT: 0] [BT IN: 0] [BT OUT: 0] [ETHERNET IN: 0] [ETHERNET OUT: 0] [USB IN: 0] [USB OUT: 0] [POWER IN: 0] [POWER OUT: 0] [CPU IN: 0] [CPU OUT: 0] [GPU IN: 0] [GPU OUT: 0] [HDD IN: 0] [HDD OUT: 0] [SSD IN: 0] [SSD OUT: 0] [FIR
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: rtreportingd] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 0] [WIFI OUT: 0] [BT IN: 0] [BT OUT: 0] [ETHERNET IN: 0] [ETHERNET OUT: 0] [USB IN: 0] [USB OUT: 0] [POWER IN: 0] [POWER OUT: 0] [CPU IN: 0] [CPU OUT: 0] [GPU IN: 0] [GPU OUT: 0] [HDD IN: 0] [HDD OUT: 0] [SSD IN: 0] [SSD OUT: 0] [FIR
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: fmfd] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 16] [WIFI OUT: 0] [BT IN: 0] [BT OUT: 0] [ETHERNET IN: 0] [ETHERNET OUT: 0] [USB IN: 0] [USB OUT: 0] [POWER IN: 0] [POWER OUT: 0] [CPU IN: 0] [CPU OUT: 0] [GPU IN: 0] [GPU OUT: 0] [HDD IN: 0] [HDD OUT: 0] [SSD IN: 0] [SSD OUT: 0] [FIR
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: ind] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 276] [WIFI OUT: 0] [BT IN: 0] [BT OUT: 0] [ETHERNET IN: 0] [ETHERNET OUT: 0] [USB IN: 0] [USB OUT: 0] [POWER IN: 0] [POWER OUT: 0] [CPU IN: 0] [CPU OUT: 0] [GPU IN: 0] [GPU OUT: 0] [HDD IN: 0] [HDD OUT: 0] [SSD IN: 0] [SSD OUT: 0] [FIR
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: IMRemoteURLConne] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 0] [WIFI OUT: 0] [BT IN: 0] [BT OUT: 0] [ETHERNET IN: 0] [ETHERNET OUT: 0] [USB IN: 0] [USB OUT: 0] [POWER IN: 0] [POWER OUT: 0] [CPU IN: 0] [CPU OUT: 0] [GPU IN: 0] [GPU OUT: 0] [HDD IN: 0] [HDD OUT: 0] [SSD IN: 0] [SSD OUT: 0] [FIR
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: locationd] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 0] [WIFI OUT: 0] [BT IN: 0] [BT OUT: 0] [ETHERNET IN: 0] [ETHERNET OUT: 0] [USB IN: 0] [USB OUT: 0] [POWER IN: 0] [POWER OUT: 0] [CPU IN: 0] [CPU OUT: 0] [GPU IN: 0] [GPU OUT: 0] [HDD IN: 0] [HDD OUT: 0] [SSD IN: 0] [SSD OUT: 0] [FIR
2020-02-25 09:35:49	Device State	[TIMESTAMP: 2020-02-25 09:35:49] [TIMESTAMP END: 2020-02-25 10:05:47] [BUNDLE ID: None] [PROCESS NAME: rapportd] [CELLULAR IN: 0] [CELLULAR OUT: 0] [WIFI IN: 0] [WIFI OUT: 0] [BT IN: 0] [BT OUT: 0] [ETHERNET IN: 0] [ETHERNET OUT: 0] [USB IN: 0] [USB OUT: 0] [POWER IN: 0] [POWER OUT: 0] [CPU IN: 0] [CPU OUT: 0] [GPU IN: 0] [GPU OUT: 0] [HDD IN: 0] [HDD OUT: 0] [SSD IN: 0] [SSD OUT: 0] [FIR

<https://github.com/mac4n6/APOLLO>



# HOMEPOD SYSLOG ARCHIVE – BEATS 1 RADIO

## /system\_logs.logarchive/



The screenshot shows the macOS Activity Monitor application window for the log file "system\_logs.logarchive". The window title bar indicates there are 604,016 messages. The toolbar includes standard Mac OS X icons for Show, Activity, Cancel, Refresh, Information, and Share, along with a search field. Below the toolbar, two tabs are visible: "Tutti i messaggi" (All messages) and "Errori e guasti" (Errors and faults), with "Tutti i messaggi" being the active tab. The main pane displays a table of log entries with columns for Type, Date and Time, Process, and Message. The "Message" column contains detailed log entries from the HomePod, such as playback queue invalidation logs and account plugin errors related to Beats 1 Radio. One specific entry for a media player process is highlighted with a purple background and a blue border around its timestamp.

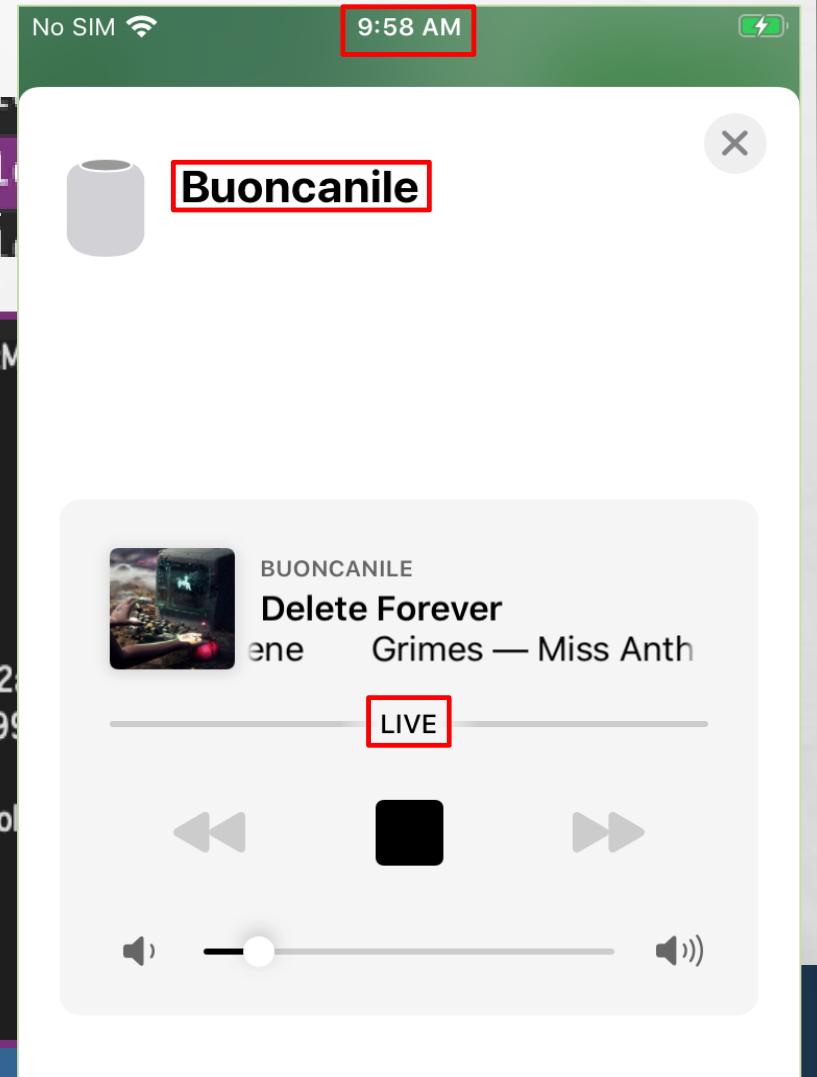
Tipologia	Data e ora	Processo	Messaggio
	2020-02-25 09:58:29.683131	AIRMUS...	PlaybackQueueInvalidation: NowPlayingItem for origin-Buoncan...
	2020-02-25 09:58:29.683257	AIJMUS...	PlaybackQueueInvalidation: NowPlayingItem for origin-Buoncan...
	2020-02-25 09:58:29.683649	account...	AMSAccountNotificationPlugin: [D7095DB2] Finished processing...
	2020-02-25 09:58:29.684628	AirMus...	<MPCModelGenericAVItem: 0x100f58d90> Beats 1: Using existing...
	2020-02-25 09:58:29.684713	AirMus...	<MPCModelGenericAVItem: 0x100f58d90> Beats 1: Using iTunes S...
	2020-02-25 09:58:29.689998	mediar...	Caching resolved player path origin-Buoncanile-1280262988/cl...
	2020-02-25 09:58:29.691532	mediar...	Set: origin-Buoncanile-1280262988/client-com.apple.Music-24...
	2020-02-25 09:58:29.692277	mediar...	Set: origin-Buoncanile-1280262988/client-com.apple.Music-24...
	2020-02-25 09:58:29.692385	mediar...	Set: origin-Buoncanile-1280262988/client-com.apple.Music-24...
	2020-02-25 09:58:29.692928	account...	"The plugin for account <private> does not implement credential...
	2020-02-25 09:58:29.692933	account...	"No plugin provides credentials for account <private>. Falli...
●	2020-02-25 09:58:29.692986	account...	"Error returned from daemon: Error Domain=com.apple.accounts...
	2020-02-25 09:58:29.693690	account...	"The plugin for account <private> does not implement credential...
	2020-02-25 09:58:29.694022	account...	"No plugin provides credentials for account <private>. Falli...

# HOMEPOD SYSLOG ARCHIVE – BEATS 1 RADIO

## /system\_logs.logarchive/

```
2020-02-25 09:58:29.692277 mediare... Set: origin-Buoncanile
2020-02-25 09:58:29.692385 mediare... Set: origin-Buoncanile
```

```
Set: origin-Buoncanile-1280262988/client-com.apple.Music-24 (AirMusic)/player-Music setting nowPlayingItem to <>M
identifier = "Bxjf9fsBR0eouHZZXDTcA\U22060t9lwLDRTFObwijEelaQAQ";
metadata = {
    "__playbackRate" = 0;
    "__title" = "Beats 1";
    albumYear = 0;
    artworkAvailable = 1;
    artworkIdentifier = "https://is1-ssl.mzstatic.com/image/thumb/Features113/v4/10/e7/de/10e7deff-d674-e2a5-99
artworkURL = "https://is1-ssl.mzstatic.com/image/thumb/Features113/v4/10/e7/de/10e7deff-d674-e2a5-99
collectionInfo = {
    kMRMediaRemoteNowPlayingCollectionInfoKeyType = kMRMediaRemoteNowPlayingCollectionInfoCol
    kMRMediaRemoteNowPlayingCollectionInfoKeyIdentifiers = {
        kMRMediaRemoteNowPlayingInfoRadioStationHash = CgkIBRoFlaS40gMQBA;
        kMRMediaRemoteNowPlayin>
```



# HOMEPOD SYSLOG ARCHIVE – MUSIC PLAYBACK

## /system\_logs.logarchive/

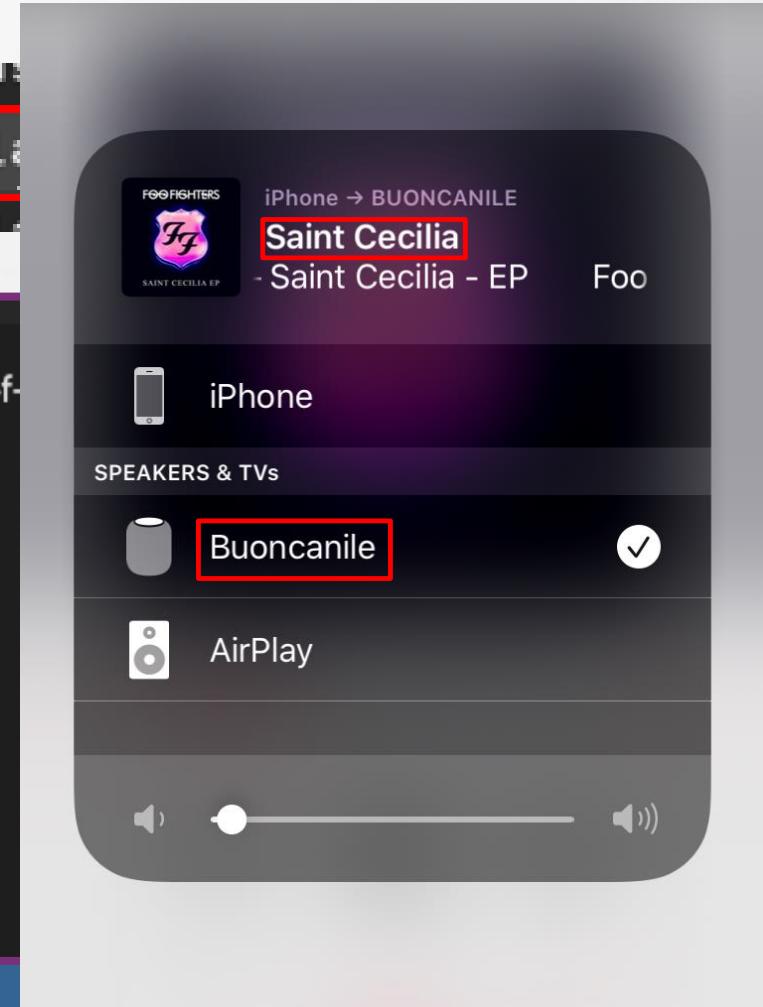
The screenshot shows a macOS System Log window titled "system\_logs.logarchive (604.016 messaggi)". The window includes standard OS X controls like close, minimize, and maximize buttons, and a toolbar with icons for Show, Activity, Delete, Refresh, Information, and Share. A search bar is present at the top right. Below the toolbar, there are two tabs: "Tutti i messaggi" (selected) and "Errori e guasti". The main area displays a table of log entries with columns for Type, Date and Time, Process, and Message. The "Message" column contains detailed log entries, such as network requests, homed process activity, and AirPlay receiver commands. One specific entry from 2020-02-25 at 10:14:03.748323 is highlighted with a red border.

Tipo	Data e ora	Processo	Messaggio
	2020-02-25 10:14:03.738281	airtun...	Request start: CID 0x2D8600D8, Peer NULL, TimeoutSecs 30
	2020-02-25 10:14:03.738333	airtun...	Request written: CID 0x2D8600D9, Header 128 bytes, Body 1759...
	2020-02-25 10:14:03.738512	airtun...	[HTTPRequest (053EE9F1-8B35-4BE8-8C1B-A6169A722336)] Started
	2020-02-25 10:14:03.742845	homed	[APReceiverRequestProcessorAirPlay] Received command: 'updat...
	2020-02-25 10:14:03.747326	airtun...	[APReceiverRequestProcessorAirPlay] [0x68DF] Update MR Now P...
	2020-02-25 10:14:03.747360	airtun...	Response received: CID 0x2D8600D9, Header 75 bytes, Body 0 b...
	2020-02-25 10:14:03.747605	airtun...	Response received: CID 0x2D8600D9, Header 75 bytes, Body 0 b...
	2020-02-25 10:14:03.748323	airtun...	[NowPlayingInfo] Setting nowPlayingInfo with mergePolicy Upd...
	2020-02-25 10:14:03.748403	airtun...	[NowPlayingInfo] Setting nowPlayingInfo artwork: MRNowPlayin...
	2020-02-25 10:14:03.749603	airtun...	Not sending contentItemChange for path origin-Buoncanile-128...
	2020-02-25 10:14:03.750738	homed	[C79 27A501AF-8082-44E6-9D70-F69005E50D3A IPv4#1e64d294:4999...
	2020-02-25 10:14:03.751024	airtun...	Sending contentItemChange for path origin-Buoncanile-1280262...
	2020-02-25 10:14:03.751509	homed	nw_connection_report_state_with_handler_on_nw_queue [C79] re...

# HOMEPOD SYSLOG ARCHIVE – MUSIC PLAYBACK

## /system\_logs.logarchive/

```
2020-02-25 10:14:03.748000 airtun... : Response  
2020-02-25 10:14:03.748323 airtun... : [NowPl...  
2020-02-25 10:14:03.748402 airtun... : [NowPl...  
  
[NowPlayingInfo] Setting nowPlayingInfo with mergePolicy Update: <NSCFDictionary 0x10130e9c0 {  
    kMRMediaRemoteNowPlayingInfoArtworkIdentifier = Music69/v4/d8/58/f8/d858f83f-ac7c-aa4f-  
    kMRMediaRemoteNowPlayingInfoTrackNumber = 1  
    kMRMediaRemoteNowPlayingInfoDuration = 221.7273469387755  
    kMRMediaRemoteNowPlayingInfoTitle = Saint Cecilia  
    kMRMediaRemoteNowPlayingInfoPlaybackRate = 1  
    kMRMediaRemoteNowPlayingInfoAlbum = Saint Cecilia - EP  
    kMRMediaRemoteNowPlayingInfoUserInfo = {  
        libEligible = 1;  
        rdwn = 1;  
        sfid = "143441-1,29";  
    }  
    kMRMediaRemoteNowPlayingInfoTotalQueueCount = 5  
    kMRMediaRemoteNowPlayingInfoActualMMEType = image/jpeg
```



# DATA ANALYSIS – EVE DOOR SENSOR

MATTIA EPIFANI

SANS DFIR SUMMIT

17<sup>TH</sup> JULY 2020



# DATASTORE.SQLITE

## HMDAccessoryTransaction

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

Filter in any column

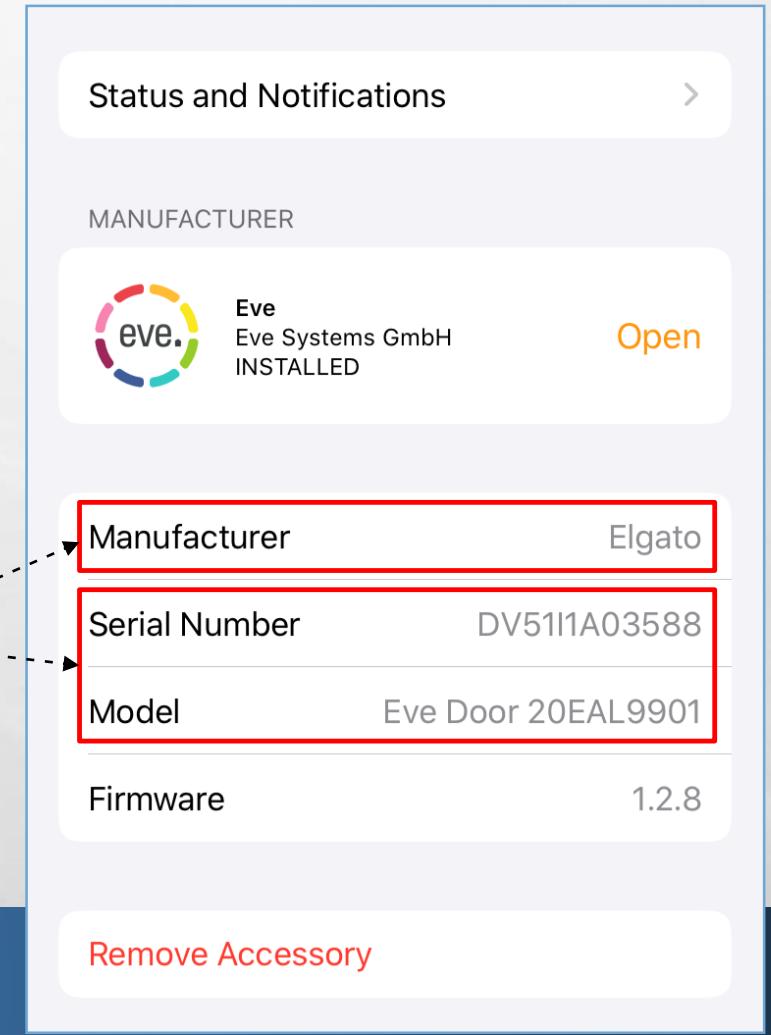
a_id	name	type	uuid	parent_uuid	encoding	record	data
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
73	1 9BF59942-0654-4350-8125-4133A1850961	HMDActionSetModel	976D30EC-E24A-52DA-921B-83B9B6685934	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
74	1 B5094766-7F20-4C73-8188-EA51CD5786CC	HMDUserModel	A4A32D3D-59AF-4F47-981B-2D2BD1E34065	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
75	1 93B78C42-E385-493D-B4A9-264CE1589117	HMDActionSetModel	E1AAAE36-31B5-5433-B73C-1A82AD218D1A	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
76	1 41396CF7-DECC-414E-BC5E-8098A6ECF15D	HMDHomeNetworkRouterSettingsModel	4C439A6B-F1E4-52DB-A541-8B2FC9D745EC	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
77	1 EA9CE1F7-66E3-4BDC-B4C2-F1E16E86FBCA	HMDHomeNetworkRouterManagingDeviceSetting...	EC205060-73E2-5550-AACA-D4B09573B160	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
78	1 3A56BCA1-E636-48D7-B9A3-3F803D56013D	HMDActionSetModel	113E9DA9-9B4D-58B0-B8D5-0C5EFBE3580F	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
79	1 66F2DE08-8ED5-4BA5-AFBD-EA07F4AB34ED	HMDHomeMediaSettingsModel	C612DD2C-E416-55BD-AD8A-2EA4C23C776C	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
80	1 5DECAF1E-C6FB-41EB-9833-2CEC4383ACA9	HMDActionSetModel	04C5D232-88F9-5733-ABFF-A6AFC9919B9C	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
81	1 6CA11486-01E1-46D5-968A-8F3F3ABFB633	HMDRoomModel	6B76D45C-3257-4DE9-A00F-8F724CB0D4E8	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
82	1 D50296B2-138D-4245-B28F-15A538EDE728	HMDHomeSettingsModel	8E714D75-8B62-50B7-9D94-3A9839F2BCE9	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
83	1 83026FA1-202C-4DD5-A8EF-A19E346620BC	HMDApplicationDataModel	3C8210A3-D3E4-5662-A9A0-ECA8464DC528	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
84	1 D563AB7A-21CC-49C3-809C-7D3B82660EE7	HMDResidentDeviceModel	DBACBD84-0916-5FA2-9943-15C93517B9EB	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
85	1 BDAA5512-7F96-4655-9D6D-776ECA3BE456	HMDRoomModel	32180983-7A6E-4C41-8EC8-0E1D348BB60	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
86	1 D13BB7B2-9501-475B-AA9B-9CEA534D0D08	HMDRoomModel	3886FDCB-7840-47FA-B0B8-A8DC389F31B5	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
87	1 A40327ED-116E-487F-8068-C0B8463E2239	HMDEventTriggerModel	3348B48B-D825-4306-B210-50C268CC6645	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
88	1 F0200FCB-61F8-41C6-9766-4F196485CAF7	HMDActionSetModel	80A4CB44-046F-40F2-831C-C11FA06536A3	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
89	1 525B1827-0333-4B40-8E8D-DBF47399FF60	HMDAppleMediaAccessoryModel	4952117C-F0B4-57A1-ABF3-C8B0BDB1E256	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
90	1 38E268B0-9334-45FF-8719-40F8EFD52178	HMDAccessoryTransaction	84E4B706-55F7-429F-BEAE-07A03DFA0D76	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB
91	1 1204E7FF-407D-4699-A563-2FAB0AD578A9	HMDHomeConfigurationModel	5D160B75-D05B-58A7-A4A3-569D81B296A4	8F4D7D36-91CB-43EA-8250-31FEC09DE463	1	BLOB	BLOB

# EVE DOOR SENSOR INFORMATION

## HMDAccessoryTransaction

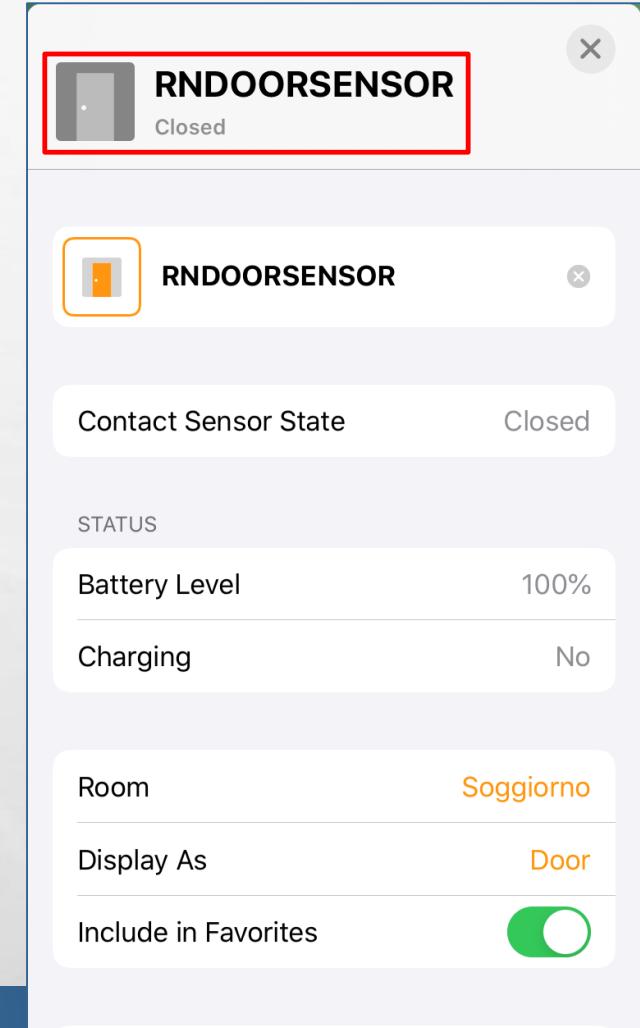
Hex Plist

```
1 1 <Dictionary>
2 2   S_v = "6.2"
3 3   transportInformation
4 4     <Dictionary>
5 5       S_HM.serverIdentifier = "39:46:7A:6E:03:FD"
6 6       HM.instanceID = 1
7 7       linkType = 2
8 8       S_pairingUsername = "39:46:7A:6E:03:FD"
9 9       networkClientLAN = 1
10 10      S_t = "HMDAccessoryTransaction"
11 11      S_u = "84E4B706-55F7-429F-BEAE-07A03DFA0D76"
12 12      WiFiCredentialType = 0
13 13      S_initialModel = "Eve Door 20EAL9901" [Red Box]
14 14      certificationStatus = 2
15 15      S_serialNumber = "DV51I1A03588"
16 16      S_roomUUID = "6B76D45C-3257-4DE9-A00F-8F724CB0D4E8"
17 17      firmwareVersion = "1.2.8"
18 18      initialCategoryIdentifier = 10
19 19      S_uniqueIdentifier = "39:46:7A:6E:03:FD+1"
20 20      S_configurationAppIdentifier = "com.apple.Home.HomeUIService"
21 21      S_configuredName = "Eve Door 93F5"
22 22      S_name = "Eve Door 93F5"
23 23      S_model = "Eve Door 20EAL9901"
24 24      S_manufacturer = "Elgato" [Red Box]
25 25      S_providedName = "Eve Door 93F5"
26 26      S_initialManufacturer = "Elgato"
27 27      S_identifier = "39:46:7A:6E:03:FD"
```



# EVE DOOR SENSOR NAME HMDServiceTransaction

Key	Type	Value
	integer	22
	string	E863F119-079E-48FF-8F27-
	dict	
	dict	
	integer	23
	string	E863F11A-079E-48FF-8F27
	dict	
	dict	
	string	6.2
	string	Eve Door
	string	00000081-0000-1000-8000-
	integer	17
	string	00000080-0000-1000-8000-
	boolean	true
	string	HMDServiceTransaction
	string	RNDOORSENSOR
	string	84E4B706-55F7-429F-BEAE



# EVE DOOR SENSOR ROOM

## HMDAccessoryTransaction / HMDRoom

Key	Type	Value
	string	HM.instanceID
	string	linkType
	string	39:46:7A:6E:03:FD
	integer	1
	integer	2
	dict	
	dict	
	string	39:46:7A:6E:03:FD
	string	HMDAccessoryTransaction
	string	84E4B706-55F7-429F-BEAE-07A03DFA0D76
	integer	0
	string	Eve Door 20EAL9901
	string	DV51I1A03588
	string	6B76D45C-3257-4DE9-A00F-8F724CB0D4E8
	string	1.2.8
	integer	10
	string	39:46:7A:6E:03:FD+1
	string	com.apple.Home.HomeUIService
	string	Eve Door 93F5
	string	Eve Door 20EAL9901
	string	Elgato
	string	Eve Door 93F5
	dict	
	dict	
	string	8F4D7D36-91CB-43EA-8250-31FEC09DE463
	integer	209
	data	...
	data	...
	dict	

The screenshot shows the Home app interface on an iPhone. At the top, it displays the room name "Soggiorno". Below this, under the "Accessories" section, there is a card for a device named "RNDOORSEN SOR Closed". The status of the door is shown as "Closed".

Below the card, a detailed view of the accessory's properties is displayed in a table:

Key	Type	Value
Root	dict	
\$version	integer	100000
\$archiver	string	NSKeyedArchiver
Stop	dict	
Sobjects	array	
	string	\$null
	dict	
	string	_P
	string	_V
	string	name
	string	_u
	string	t
	string	8F4D7D36-91CB-43EA-8250-31FEC09DE463
	string	6.2
	string	Soggiorno
	string	6B76D45C-3257-4DE9-A00F-8F724CB0D4E8
	string	HMDRoomModel

The table includes several redacted values (indicated by red boxes) and some specific values highlighted in red boxes: "8F4D7D36-91CB-43EA-8250-31FEC09DE463", "6.2", and "Soggiorno".

# EVE DOOR SENSOR INFORMATION

/private/var/mobile/Library/Caches/com.apple.HomeKit.configurations/homeData.\*.config

Key	Type	Value
.....	dict	
.....	dict	
.....	dict	
.....	string	84E4B706-55F7-429F-BEAE-07A03DFA0D76
.....	string	Eve Door 93F5
.....	string	DV51I1A03588
.....	string	Elgato
.....	string	Eve Door 20EAL9901
.....	string	1.2.8
.....	dict	
.....	dict	
.....	string	772AFB8E-8D2F-455E-90E5-9852E6C4DD31
.....	string	Sensor
.....	string	com.apple.Home.HomeUIService
.....	string	39FA322E-5145-548C-BB94-E621393D6CA7
.....	dict	
.....	string	Soggiorno
.....	string	6B76D45C-3257-4DE9-A00F-8F724CB0D4E8
.....	string	com.elgato.eve
.....	string	917695792
.....	string	39:46:7A:6E:03:FD

# EVE DOOR SENSOR INFORMATION – EVE APP

com.elgato.plist

Key	Type	Value
CloudClientFeatureSwitch.eve	boolean	false
ELGFluidVolumeUnit	string	ELGFluidVolumeUnit_GallonUS
ELGPrimaryHomeUseSameAsC	boolean	true
RRMSessionsCountSinceUpdate	integer	2
SessionIdHistory	data	...
identifierKey:1FAD21D8-DD28	string	Elgato##Eve Door 20EAL9901##DV51I1A03588
RRMLastDidEnterBackground	string	2/25/20, 10:08:17 AM
UserIdHistory	data	...
ELGThermoSchedulesToken	data	...
serialNumberKey:1FAD21D8-D	string	DV51I1A03588
ELGPressureUnit	string	ELGPressureUnit_Hg
ELGEveLastPositionPrior2_9_5	boolean	true
ELGEve2_5VersionWasInstalled	boolean	true
ELGSystemInfoLastTime	real	604314152.175106
ELGAltitudeUnit	string	ELGAltitudeUnit_Feet
RRMLastBuildNumber	string	4793



# EVE DOOR SENSOR INFORMATION – EVE APP

Elgato##Eve Door 20EAL9901##DV51I1A03588.sql

UTC					
1	<input checked="" type="checkbox"/>	4107	17/02/2020 11:42:23	0	
2	<input checked="" type="checkbox"/>	4108	17/02/2020 11:43:40	1	
3	<input checked="" type="checkbox"/>	4109	17/02/2020 11:43:41	0	
4	<input checked="" type="checkbox"/>	4110	17/02/2020 11:43:44	1	
5	<input checked="" type="checkbox"/>	4111	17/02/2020 11:43:44	0	
6	<input checked="" type="checkbox"/>	4112	17/02/2020 11:43:46	1	
7	<input checked="" type="checkbox"/>	4113	17/02/2020 11:43:48	0	
8	<input checked="" type="checkbox"/>	4114	17/02/2020 11:43:50	1	
9	<input checked="" type="checkbox"/>	4115	17/02/2020 11:43:51	0	
10	<input checked="" type="checkbox"/>	4116	17/02/2020 11:47:03	1	
11	<input checked="" type="checkbox"/>	4117	17/02/2020 11:47:03	0	
12	<input checked="" type="checkbox"/>	4118	17/02/2020 11:47:06	1	
13	<input checked="" type="checkbox"/>	4119	17/02/2020 11:47:09	0	
14	<input checked="" type="checkbox"/>	4120	17/02/2020 11:47:10	1	
15	<input checked="" type="checkbox"/>	4121	17/02/2020 11:47:12	0	
16	<input checked="" type="checkbox"/>	4122	17/02/2020 11:47:50	1	
17	<input checked="" type="checkbox"/>	4123	17/02/2020 11:47:51	0	
18	<input checked="" type="checkbox"/>	4124	17/02/2020 11:49:19	1	
19	<input checked="" type="checkbox"/>	4125	17/02/2020 11:49:29	0	
20	<input checked="" type="checkbox"/>	4126	17/02/2020 11:49:31	1	
21	<input checked="" type="checkbox"/>	4127	17/02/2020 11:49:39	0	
22	<input checked="" type="checkbox"/>	4128	17/02/2020 11:49:42	1	
23	<input checked="" type="checkbox"/>	4129	17/02/2020 11:49:50	0	
24	<input checked="" type="checkbox"/>	4130	17/02/2020 11:50:01	1	
25	<input checked="" type="checkbox"/>	4131	17/02/2020 11:50:01	0	
26	<input checked="" type="checkbox"/>	4132	17/02/2020 11:50:02	1	
27	<input checked="" type="checkbox"/>	4133	17/02/2020 11:50:04	0	
28	<input checked="" type="checkbox"/>	4134	17/02/2020 11:50:06	1	

GMT+1	<a href="#">Back</a>	<a href="#">Open Events</a>	<a href="#">Edit</a>
		12:49 PM	00:11
		12:49 PM	00:03
		12:49 PM	00:02
		12:47 PM–12:49 PM	01:28
		12:47 PM	00:38
		12:47 PM	00:01
		12:47 PM	00:03
		12:43 PM–12:47 PM	03:12
		12:43 PM	00:02
		12:43 PM	00:02
		12:43 PM	00:03
		12:42 PM–12:43 PM	01:17

La mia abitazione

Rooms

Automation

Settings

# FINDINGS AND VALIDATION

MATTIA EPIFANI

SANS DFIR SUMMIT

17<sup>TH</sup> JULY 2020

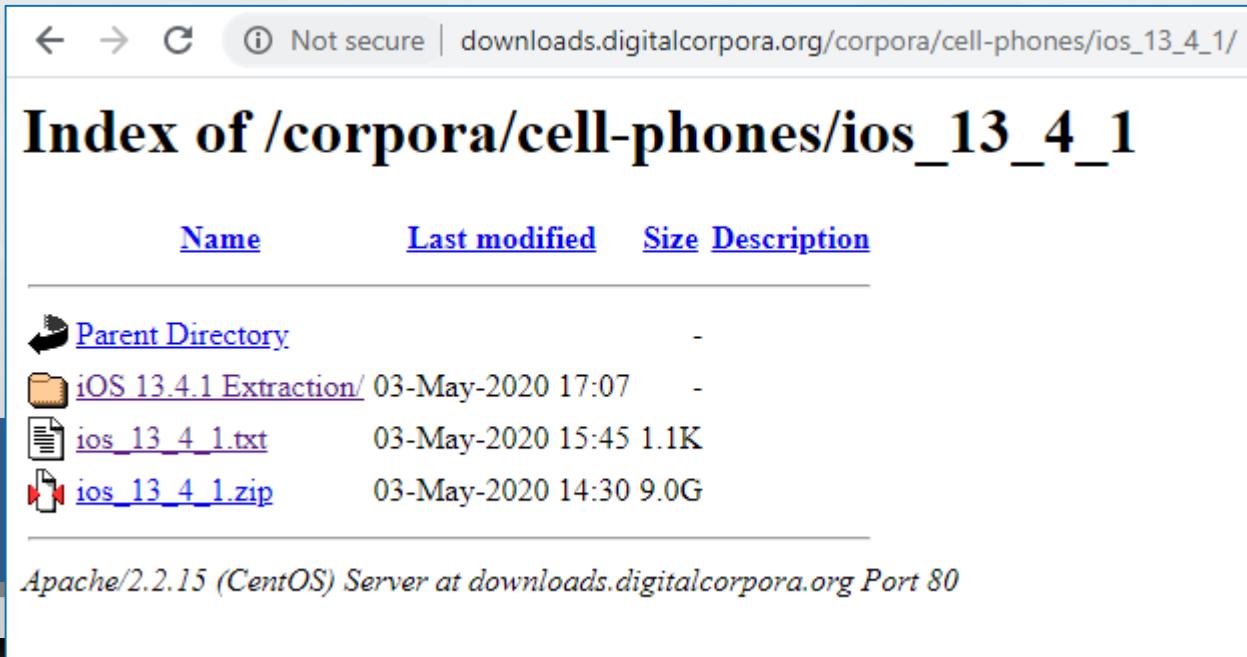


# FINDINGS

- Apple HomeKit is an unexplored field in IoT/Mobile Forensics
- The analysis of an iPhone connected to an Apple Home can reveal
  - Home location
  - Home organization (rooms)
  - Installed HomeKit devices
  - Interactions (Music, Sensors)
- The analysis of an HomePod connected to an Apple Home can reveal
  - HomePod Settings
  - HomePod network connections
  - HomePod usage (Powelog, Syslog)

# VALIDATION

- We tested our findings on the Joshua Hickman iOS 13.4.1 image
- <https://digitalcorpora.org/archives/1496>



The screenshot shows a web browser window with the URL [https://downloads.digitalcorpora.org/corpora/cell-phones/ios\\_13\\_4\\_1/](https://downloads.digitalcorpora.org/corpora/cell-phones/ios_13_4_1/). The page title is "Index of /corpora/cell-phones/ios\_13\_4\_1". Below the title is a table with three columns: "Name", "Last modified", and "Size Description". The table contains four rows: a parent directory link, an extraction archive folder, a plain text file, and a large zip archive. At the bottom of the page is the Apache server information: "Apache/2.2.15 (CentOS) Server at downloads.digitalcorpora.org Port 80".

Name	Last modified	Size Description
<a href="#">Parent Directory</a>		-
<a href="#">iOS 13.4.1 Extraction/</a>	03-May-2020 17:07	-
<a href="#">ios_13_4_1.txt</a>	03-May-2020 15:45	1.1K
<a href="#">ios_13_4_1.zip</a>	03-May-2020 14:30	9.0G

Apache/2.2.15 (CentOS) Server at downloads.digitalcorpora.org Port 80

# DATASTORE.SQLITE

## HMDHomeManagerModel / HMDHomeModel

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

	group_id	share_id	store_id	name	type	uuid	parent_uuid	encoding	record	data
1	4	0	1	55C72C52-0304-4E13-90B1-5D0A5EF53E94	HMDHomeManagerModel	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	NULL	1	BLOB	BLOB
2	2	0	1	9C3BF4D1-C7CF-4217-BCD2-0F7E96D5B300	HMDCloudLegacyModelObject	457C009B-1DA4-4B71-BD09-93D344A81A8B	NULL	1	BLOB	BLOB

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

	group_id	share_id	store_id	name	type	uuid	parent_uuid	encoding	record	data
12	4	0	1	84C5BA82-0D4E-4541-B68B-9F0BBE93A4DC	HMDApplicationDataModel	D162EAEF-8138-5E87-9A01-29F8B9A950A7	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB
13	4	0	1	A4100B50-0A29-41DF-88B4-D30A997ACD91	HMDAccountModel	464C253A-E17D-5881-A8BE-C53773BF98DA	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB
14	4	0	1	9754E933-4AD3-4581-84F9-E4C5FC5F5C08	HMDCloudZoneInformationModel	C04E1CE7-FE08-5F1D-B82E-5C8F39EE63F3	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB
15	4	0	1	A6BBA3B0-78E6-4BE3-82DB-A3872E643D0D	HMDHAPMetadataModel	9C7B07AE-AB5E-58F8-99B8-22ED7732C292	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB
16	5	1	1	68FDD0E1-E60D-4639-9C9E-C2DA19733A98	HMDHomeModel	A7FA5B35-F540-4226-AA03-0126B5B928EF	1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938	1	BLOB	BLOB

# HOME NAME, HOME GEOLOCATION AND USER ID

## HMDHomeModel

Hex Plist

```
1 1 <Dictionary>
2 S _u = "A7FA5B35-F540-4226-AA03-0126B5B928EF"
3 S homeLocationData
4 S ClassName = "NSMutableData"
5 S NS.data = bplist000.....X$versionY$archiverT$topX$objects...+_.NSKeyedArchiverN..TrootE...E...U>nullO.....
6 S ownerUserID = "thisisdfir@gmail.com"
7 S defaultRoomUUID = C02D3608-63CF-4B75-B413-B41668E0BC55"
8 S networkProtectionMode = 0
9 S _V = "6.2"
10 B multiUserEnabled = True
11 S ownerPublicKey = "tLu.GbÆlµ..`@Ô•YD¢b²mÓ!.^ç/àš
12 S ownerName = "7AB2FF69-E391-4AB2-980B-A8191E8A840A"
13 S ownerUUID = "FDFDF0DB-58DD-45FA-BF21-F84CF640A05A"
14 S _t = "HMDHomeModel"
15 S presenceAuthorizationStatus = 1
16 S primaryResidentUUID = "E9903C6B-CC33-578E-A3E0-2876D3C71B43"
17 S name = "My Home"
18 S _P = "1CAEDC10-E3E5-41A4-BB17-A9EEBA14A938"
```

Hex Plist

```
1 1 <Dictionary>
2 S ClassName = "HMDHomeLocationData"
3 S homeLocation
4 S homeLocationNextUpdate
```

# DATASTORE.SQLITE

## HMDRoomModel / HMDAppleMediaAccessoryModel

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

	group_id	share_id	store_id	name	type	uuid	parent_uuid	encoding	record	data
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
54	5	1	1	F4F9800F-AC09-4A40-8789-B1C7A08C5728	HMDHomeSettingsModel	55D6B260-3BB2-5EE6-9BBC-5C87E9960F15	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
55	5	1	1	A45FF377-BF59-4221-9864-735B391F0883	HMDActionSetModel	1CD12ADD-D479-525E-BC76-59EAA394E939	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
56	5	1	1	23173970-AFCA-4D37-BEFF-7ABDB0996FB3	HMDHomeNetworkRouterManagingDeviceSetting...	CE495F7C-7E34-5F10-B823-E93DDA264E5C	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
57	5	1	1	C802C768-6ACE-4A40-A3C2-24E98FF41654	HMDActionSetModel	13F3CC57-35DD-5A26-B4DD-10E1C433F337	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
58	5	1	1	BB7DDAA1-4262-4F9B-8557-0A805F8E3698	HMDActionSetModel	4AC04E92-74E4-5D6B-A4D0-E87419D440DE	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
59	5	1	1	4531A7B8-963E-4F0A-A4EC-C138BE2B690C	HMDApplicationDataModel	556EF00C-89F0-5BC8-8E83-EB4F6B611C54	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
60	5	1	1	97733E44-727A-455F-8772-C400251D8B77	HMDUserModel	FDFDF0DB-58DD-45FA-BF21-F84CF640A05A	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
61	5	1	1	14C2EFE1-E6DA-4663-8B98-89C8545AAA3B	HMDActionSetModel	B914A4D2-66FE-5E59-B2D3-1EB269C6ACD6	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
62	5	1	1	258A2A5D-EE34-40C1-A950-AD9EB754B40B	HMDHomeNetworkRouterSettingsModel	94116D5A-D19C-564A-9E61-A278BE32533E	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
63	5	1	1	BBFCEFD8-F006-4157-A6D1-A124587687E7	HMDRoomModel	34147518-5CB4-4A4E-B139-E0E3E37A7001	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
64	5	1	1	50DA2986-6452-4CC8-9CA0-7E9A3C16CC94	HMDResidentDeviceModel	E9903C6B-CC33-578E-A3E0-2876D3C71B43	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
65	5	1	1	65ED7919-839B-4DAE-A703-D095DB42AEB9	HMDHomeMediaSettingsModel	144BFB15-C934-5335-AE19-FAC2A64237C1	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
66	5	1	1	975A902D-E42E-4DAE-9B73-DEBA76D5824D	HMDHomeConfigurationModel	62FCB50D-8D55-5877-8581-24380CB4A1F7	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB
67	5	1	1	C0FC6DFE-3E9A-4F90-9323-3AB9ADAC6C21	HMDAppleMediaAccessoryModel	8EB90DD5-0F47-5027-BA90-5274B123D579	A7FA5B35-F540-4226-AA03-0126B5B928EF	1	BLOB	BLOB

# HOMEPOD INFORMATION

## HMDAppleMediaAccessoryModel

### HMDRoomModel

```
Hex Plist
1 <Dictionary>
2   S _P = "A7FA5B35-F540-4226-AA03-0126B5B928EF"
3   S V = "6.2"
4   S name = "Office"
5   S u = "34147518-5CB4-4A4E-B139-E0E3E37A7001"
6   S t = "HMDRoomModel"
```

```
Hex Plist
1 <Dictionary>
2   S configuredName
3     S ClassName = "NSNull"
4   S accessoryCategory = 25
5   S roomUUID = "34147518-5CB4-4A4E-B139-E0E3E37A7001"
6   S pairingIdentity
7     S ClassName = "NSMutableData"
8       NS.data = bplist00Ô.....X$versionY$archiverT$topX$objects...+ ...NSKeyedArchiverÑ..Troot€.§.....U$nullÔ.....
9     S _t = "HMDAppleMediaAccessoryModel"
10    S _u = "8EB90DD5-0F47-5027-BA90-5274B123D579"
11    S deviceUUID = "0B40F101-4268-5AA0-9A35-2CBC35398429"
12   S wifiNetworkInfo
13     S ClassName = "NSMutableData"
14       NS.data = bplist00Ô.....X$versionY$archiverT$topX$objects...+ ...NSKeyedArchiverÑ..Troot€.§....!U$nullÔ.....
15     S _V = "6.2"
16     S firmwareVersion = "13.4 (17L256)"
17   S name
18     S ClassName = "NSNull"
19     S manufacturer = "Apple Inc."
20     S providedName = "HomePod"
21     S identifier = "A85EA0EB-E871-4875-8A3A-889A11288A35"
22     S configurationAppIdentifier = "com.apple.SharingViewService"
23     S serialNumber = "DLXW2G7KHQK8"
24     S _P = "A7FA5B35-F540-4226-AA03-0126B5B928EF"
25     S model = "NQHW2LL/A"
26   S softwareVersion
27     S ClassName = "NSMutableData"
28       NS.data = bplist00Ô.....X$versionY$archiverT$topX$objects...+ ...NSKeyedArchiverÑ..Troot€.¤....U$nullÔ.....
29   S device
30     S ClassName = "NSMutableData"
31       NS.data = bplist00Ô.....X$versionY$archiverT$topX$objects...+ ...NSKeyedArchiverÑ..Troot€.¬.*..-17=AHIOSTW\...
32   S loggedInAccount
33     S ClassName = "NSMutableData"
34       NS.data = bplist00Ô.....X$versionY$archiverT$topX$objects...+ ...NSKeyedArchiverÑ....Troot€.¬.¼.....
```

# DATASTORE.SQLITE

## HMDAccessorySettingGroupModel

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

group_id	share_id	store_id	name	type	uuid	parent_uuid	encoding	record	data
76	5	1	1 7DB7AF54-F1DD-474D-B5D1-20D4731D8BBF	HMDAccessorySettingGroupModel	CDA42BD0-73DF-488F-9142-0BA954C6C5DE	8EB90DD5-0F47-5027-BA90-5274B123D579	1	BLOB	BLOB
77	5	1	1 D2D2E130-0AAA-43F2-AE27-A24E72C5EC69	HMDAccessorySettingGroupModel	BAA48C94-F995-5CB4-A21C-A929B1FD0853	8EB90DD5-0F47-5027-BA90-5274B123D579	1	BLOB	BLOB

Database Structure   Browse Data   Edit Pragmas   Execute SQL

Table: record

group_id	share_id	store_id	name	type	uuid	parent_uuid	encoding	record	data
21	5	1	1 F9C9E7E4-E490-4CCC-9077-E14F3C521E01	HMDAccessorySettingGroupModel	20A07D20-00C6-4ED5-9C83-31924CA08538	CDA42BD0-73DF-488F-9142-0BA954C6C5DE	1	BLOB	BLOB
22	5	1	1 66893FAA-C503-4CFA-B3DA-25FA0FDDF26E	HMDAccessorySettingGroupModel	7688AE36-3441-44D0-9740-9BF30B6435D2	CDA42BD0-73DF-488F-9142-0BA954C6C5DE	1	BLOB	BLOB
23	5	1	1 1D755A59-2834-46D9-9A78-50BA804B6C74	HMDAccessorySettingGroupModel	3AA98B51-2739-4225-80E2-60453A314A97	CDA42BD0-73DF-488F-9142-0BA954C6C5DE	1	BLOB	BLOB
24	5	1	1 A4E95495-BA8C-4342-B351-5D5E26C378A2	HMDAccessorySettingGroupModel	459A650B-D8AE-48B5-8781-80FE5F47C022	CDA42BD0-73DF-488F-9142-0BA954C6C5DE	1	BLOB	BLOB
25	5	1	1 E8BCC7A4-72D2-4E4E-B535-B033308524A2	HMDAccessorySettingGroupModel	B75CCD62-221B-4D4D-A5A2-37947D890E01	CDA42BD0-73DF-488F-9142-0BA954C6C5DE	1	BLOB	BLOB
26	5	1	1 BC7F20DD-DE83-4CE5-9D26-1DA8ADA17C0E	HMDAccessorySettingGroupModel	55A6631B-FBDF-46E0-9E60-F8E6865B7CBC	CDA42BD0-73DF-488F-9142-0BA954C6C5DE	1	BLOB	BLOB

# HOMEPOD SIRI SETTINGS

```
Hex Plist
1 | 1 <Dictionary>
2 |   S, _P = "CDA42BD0-73DF-488F-9142-0BA954C6C5DE"
3 |   S, _V = "6.2"
4 |   S, name = "siri"
5 |   S, _u = "7688AE36-3441-44D0-9740-9BF30B6435D2"
6 |   S, _t = "HMDAccessorySettingGroupModel"
```

Database Structure Browse Data Edit Pragmas Execute SQL

Table: record

group_id	share_id	store_id	name	type	uuid	parent_uuid ↗ <sup>1</sup>	encoding	record	data
152	5	1	1 24F0FDEC-73C5-4E6E-9AF9-1A979DC05BCF	HMDAccessorySettingModel	DE0B6401-11CD-465E-997B-448F1F85845A	7688AE36-3441-44D0-9740-9BF30B6435D2	1 BLOB	BLOB	
153	5	1	1 8E7EC072-0081-4ECD-808D-F4CC57AED240	HMDAccessorySettingModel	2E72B831-3D72-4449-8E61-FDB3C6DDA16D	7688AE36-3441-44D0-9740-9BF30B6435D2	1 BLOB	BLOB	
154	5	1	1 82DF6B4E-43B2-414A-8641-2A71235D2FF5	HMDAccessorySettingModel	10B5CF35-B041-4171-8D15-4CE1CBA9983E	7688AE36-3441-44D0-9740-9BF30B6435D2	1 BLOB	BLOB	
155	5	1	1 F888B19F-614E-490C-BEC4-079E01C73CE1	HMDAccessorySettingModel	657632FB-44BC-462F-A069-9C33C4F1047C	7688AE36-3441-44D0-9740-9BF30B6435D2	1 BLOB	BLOB	
156	5	1	1 21158DD2-AF06-4C2B-8787-EE7A7A6676C9	HMDAccessorySettingModel	1E049B6F-4DE1-437E-BABF-87E61968EABB	7688AE36-3441-44D0-9740-9BF30B6435D2	1 BLOB	BLOB	

# HOMEPOD SIRI LANGUAGE SETTINGS

Hex Plist

```
1 <Dictionary>
2   S _P = "7688AE36-3441-44D0-9740-9BF30B6435D2"
3   S _U = "2E72B831-3D72-4449-8E61-FDB3C6DDA16D"
4   configurationVersion = 1
5   S _V = "6.2"
6   properties = 3
7   value
8     S ClassName = "NSMutableData"
9     NS.data = bplist00Ó.....X$versionY$archiverT$topX$objects...+_.NSKeyedArchiverÑ.Troot€.!.....U>nullÓ.....
10    type = 4
11    S name = "language"
12    S _t = HMAccessorySettingModel
```

Hex Plist

```
1 <Dictionary>
2   S ClassName = "HMAccessorySelectionSettingItem"
3   HM.identifier
4     S ClassName = "NSUUID"
5     NS.uuidbytes = .ÓÝ.Í.M±.Âg.ú"Í
6     S HM.title = [en-US|en-US].t.d
```

# HOMEPOD INFORMATION

/private/var/mobile/Library/Caches/com.Apple.Homekit.Configurations/homeData.\*.Config

users

- <Dictionary>
  - S ClassName = "HMUser"
  - B HM.isCurrentUser = True
  - S userID = "thisisdfir@gmail.com"
- HMS.settings.shared
- HMS.settings.private
- B isAdminUser = True
- S userUUID = "FDFDF0DB-58DD-45FA-BF21-F84CF640A05A"
- HM.u.mu.accessories
- B HM.isOwnerUser = True
- HM.camerasAccessLevelKey = 2
- S userDisplayName = "thisisdfir@gmail.com"

accessories

- <Dictionary>
  - S ClassName = "HMAccessory"
  - HM.accessoryProfiles
  - HM.accessoryCategory
    - S ClassName = "HMAccessoryCategory"
    - S HM.accessoryCategoryType = "1D8FD40F-7CAE-4AD5-9973-977D18890DE2"
    - S HM.accessoryCategoryName = "HomePod"  - HMA.targetNetworkProtectionMode = 0
  - HM.softwareUpdate
  - S accessoryUUID = "8EB90DD5-0F47-5027-BA90-5274B123D579"
  - HM.appData
  - B HMA.supportsNetworkProtection = False
  - HM.symptomsHandler
  - S HM.firmwareVersion = "13.4"

HM.settings

- B HM.supportsIdentify = False
- S HM.model = "NQHW2LL/A"
- B HMA.supportsMediaAccessControl = True
- HM.reachability = 0
- HM.wifiNetworkInfo
- B isPrimary = True
- HMA.currentNetworkProtectionMode = 4
- accessoryConfiguredName
- HM.storeID
- HM.remoteLoginHandler
- B HMA.supportsMultiUser = True
- HM.bundleID
- B HMCT.supportsTargetControl = False
- S configurationAppID = "com.apple.SharingViewService"
- S accessoryName = "Office"
- S HM.serialNumber = "DLXW2G7KHQK8"

accessoryRoom

- <Dictionary>
  - S ClassName = "HMRoom"
  - home
  - S roomName = "Office"
  - S roomUUID = "34147518-5CB4-4A4E-B139-E0E3E37A7001"

# HOMEPOD MUSIC PLAYBACK

## /private/var/mobile/CoreDuet/Knowledge/knowledgeC.db

```
SELECT DATETIME(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') AS "START",
       DATETIME(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') AS "END",
       ZSTREAMNAME AS "STREAM NAME", ZVALUESTRING AS "VALUE STRING",
       Z_DKNOPLAYINGMETADATAKEY__TITLE AS "TITLE",
       Z_DKNOPLAYINGMETADATAKEY__ARTIST AS "ARTIST",
       Z_DKNOPLAYINGMETADATAKEY__ALBUM AS "ALBUM",
       Z_DKNOPLAYINGMETADATAKEY__DURATION AS "DURATION",
       Z_DKNOPLAYINGMETADATAKEY__GENRE AS "GENRE",
       Z_DKNOPLAYINGMETADATAKEY__MEDIATYPE AS "MEDIA TYPE",
       Z_DKNOPLAYINGMETADATAKEY__OUTPUTDEVICEIDS AS "OUTPUT DEVICE ID"
FROM ZSTRUCTUREDMETADATA JOIN ZOBJECT
ON ZOBJECT.ZSTRUCTUREDMETADATA = ZSTRUCTUREDMETADATA.Z_PK
ORDER BY ZOBJECT.ZSTARTDATE
```

DB Browser for SQLite - D:\knowledgeC.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL

SQL 1

```

1 SELECT DATETIME(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') AS "START",
2       DATETIME(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') AS "END",
3       ZSTREAMNAME AS "STREAM NAME", ZVALUESTRING AS "VALUE STRING",
4       Z_DKNOPLAYINGMETADATATEKEY__TITLE AS "TITLE",
5       Z_DKNOPLAYINGMETADATATEKEY_ARTIST AS "ARTIST",
6

```

	START	END	STREAM NAME	VALUE STRING	TITLE	ARTIST	ALBUM	DURATION	GENRE	MEDIA TYPE	OUTPUT DEV
7537	2020-04-06 14:18:07	2020-04-06 14:18:11	/media/nowPlaying	com.apple.podcasts	Month In 4n6 – ...	This Week In 4n6 » Podcasts	Marc...	1074.7588208...	NULL	MRMediaRemoteMediaTypePodcast	BLOB
7538	2020-04-06 14:18:11	2020-04-06 14:19:10	/media/nowPlaying	com.apple.podcasts	Month In 4n6 – ...	This Week In 4n6 » Podcasts	Marc...	1074.7588208...	NULL	MRMediaRemoteMediaTypePodcast	BLOB
7539	2020-04-06 14:19:10	2020-04-06 14:26:41	/media/nowPlaying	com.apple.podcasts	Month In 4n6 – ...	This Week In 4n6 » Podcasts	Marc...	1074.7588208...	NULL	MRMediaRemoteMediaTypePodcast	BLOB
7540	2020-04-06 14:26:41	2020-04-06 14:26:43	/media/nowPlaying	com.apple.podcasts	Month In 4n6 – ...	This Week In 4n6 » Podcasts	Marc...	1074.7588208...	NULL	MRMediaRemoteMediaTypePodcast	BLOB
7541	2020-04-06 14:26:43	2020-04-06 14:38:08	/media/nowPlaying	com.apple.podcasts	Month In 4n6 – ...	This Week In 4n6 » Podcasts	Marc...	1074.7588208...	NULL	MRMediaRemoteMediaTypePodcast	BLOB
7542	2020-04-06 14:38:08	2020-04-06 14:38:08	/media/nowPlaying	com.apple.podcasts	Month In 4n6 – ...	This Week In 4n6 » Podcasts	Marc...	1074.7588208...	NULL	MRMediaRemoteMediaTypePodcast	BLOB
7543	2020-04-04 22:17:42	2020-04-04 22:20:32	/media/nowPlaying	com.apple.Music	Move Your Feet	Junior Senior	D-D...	180.97632653...	Pop	MRMediaRemoteMediaTypeMusic	BLOB
7544	2020-04-04 22:20:32	2020-04-04 22:20:35	/media/nowPlaying	com.apple.Music	Move Your Feet	Junior Senior	D-D...	180.97632653...	Pop	MRMediaRemoteMediaTypeMusic	BLOB
7545	2020-04-04 22:20:35	2020-04-05 06:03:15	/media/nowPlaying	com.apple.Music	Move Your Feet	Junior Senior	D-D...	180.97632653...	Pop	MRMediaRemoteMediaTypeMusic	BLOB
7546	2020-04-01 18:09:39	2020-04-01 18:12:33	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7547	2020-04-01 18:12:33	2020-04-01 18:12:45	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7548	2020-04-01 18:12:45	2020-04-02 17:26:35	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7549	2020-04-02 17:26:35	2020-04-02 17:27:55	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7550	2020-04-02 17:27:55	2020-04-02 17:28:20	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7551	2020-04-02 17:28:20	2020-04-02 17:28:30	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7552	2020-04-02 17:28:30	2020-04-02 17:32:06	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7553	2020-04-02 17:32:06	2020-04-02 17:33:01	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7554	2020-04-02 17:33:01	2020-04-02 18:06:12	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7555	2020-04-02 18:06:12	2020-04-02 18:09:16	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7556	2020-04-02 18:09:16	2020-04-03 16:32:01	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7557	2020-04-03 16:32:01	2020-04-03 16:32:17	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB
7558	2020-04-03 16:32:17	2020-04-03 18:54:42	/media/nowPlaying	com.apple.Music	Name of the Game	The Crystal Method	Twee...	255.16408163...	Elect...	MRMediaRemoteMediaTypeMusic	BLOB

Execution finished without errors.  
Result: 7600 rows returned in 135ms  
At line 1:  
SELECT DATETIME(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') AS "START",
 DATETIME(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') AS "END",
 ZSTREAMNAME AS "STREAM NAME", ZVALUESTRING AS "VALUE STRING",
 Z\_DKNOPLAYINGMETADATATEKEY\_\_TITLE AS "TITLE",
 Z\_DKNOPLAYINGMETADATATEKEY\_ARTIST AS "ARTIST",

Edit Database Cell

Mode: Binary

bplist00.....  
X\$versionY\$archiverT\$topX\$objec...  
ts..... NSKeyedArchiver...Troo...  
t.....!"-USnull.....WNSS.class.....  
.....SA85EA0EB-E871-4875-8A3A-889All288A35.%\$%Z\$cla...  
ssnameX\$classes^NSMutableArray.%  
'(WNSArrayListX\$Obj v

Type of data currently in cell: Binary  
453 byte(s)

Remote

Identity Public

Name	Commit	Last modified	Size

SQL Log Plot DB Schema Remote

# REFERENCES AND PUBLIC DATASET

MATTIA EPIFANI

SANS DFIR SUMMIT

17<sup>TH</sup> JULY 2020



# REFERENCES

- **HomePod Teardown Reveals Hidden 14-Pin Connector, 16GB Storage, and Very Low Repairability**  
<https://www.macrumors.com/2018/02/12/homepod-teardown-ifixit/>, ultima visita: marzo 2020.
- **HomePod - iFixit**  
<https://it.ifixit.com/Guida/Smontaggio+HomePod/103133>
- **Pogo pin – Wikipedia**  
[https://en.wikipedia.org/wiki/Pogo\\_pin](https://en.wikipedia.org/wiki/Pogo_pin)
- **Profiles and Logs - Bug Reporting - Apple Developer**  
<https://developer.apple.com/bug-reporting/profiles-and-logs/>
- **HomePod Logging Instructions - Apple Developer**  
[https://developer.apple.com/services-account/download?path=/iOS/iOS\\_Logs/HomePodLogging\\_Instructions.pdf](https://developer.apple.com/services-account/download?path=/iOS/iOS_Logs/HomePodLogging_Instructions.pdf)
- **Epifani Mattia, Leong Adrian and Mahalik Heather. Using Apple “Bug Reporting” for forensic purposes. OSDFCON, 2019.**
- **GitHub - RealityNet/ios\_bfu\_triage**  
[https://github.com/RealityNet/ios\\_bfu\\_triage](https://github.com/RealityNet/ios_bfu_triage)
- **GitHub - cheeky4n6monkey/iOS\_sysdiagnose\_forensic\_scripts**  
[https://github.com/cheeky4n6monkey/iOS\\_sysdiagnose\\_forensic\\_scripts](https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts)
- **GitHub - mac4n6/APOLLO: Apple Pattern Of Lazy Output'er**  
<https://github.com/mac4n6/APOLLO>

# PUBLIC DATASET DFRWS 2020 EU RODEO – DATASET AND QUESTIONS

[http://bit.do/dfrws\\_rodeo\\_2020](http://bit.do/dfrws_rodeo_2020)

File > DFRWS_2020					
	Nome	Data/ora modifica	Modificato da	Dimensioni file	Condivisione
	Apple_Homepod_Forensics_DFRWS_2020.pdf	4 giugno	Mattia Epifani	4,69 MB	Condiviso
	DEVICE.zip	27 maggio	Mattia Epifani	409 MB	Condiviso
	DFRWS_2020_Rodeo_Presentation.pdf	3 giugno	Mattia Epifani	1,78 MB	Condiviso
	hashes.txt	29 maggio	Mattia Epifani	214 byte	Condiviso
	password.txt	3 giugno	Mattia Epifani	24 byte	Condiviso
	questions.txt	3 giugno	Mattia Epifani	865 byte	Condiviso
	useful_tools.txt	2 giugno	Mattia Epifani	116 byte	Condiviso

# **ACKNOWLEDGEMENTS**

- **Francesca Maestri**
- **Silvia Spallarossa**
- **Claudia Meda**

# 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](mailto:mattia.epifani@realitynet.it)



[@mattiaepl](https://twitter.com/mattiaepl)



<http://www.linkedin.com/in/mattiaeplfani>



<http://www.realitynet.it>



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