



5e Rendez-vous 4n6s

27 Sept 2020

Jean-Philippe Noat Senior Director of Intl training chez Cellebrite

[illegible]

- Votre rendez-vous d'échange
- Proposer les sujets qui vous intéressent
- Poser des questions techniques, si toutes ne peuvent être répondues elles le seront lors du prochain rendez-vous.
- Faites vous plaisir et échangez
- Mettre l'humain au coeur de la technique
- N'hésitez pas à présenter un sujet si vous le souhaitez

Que faire en cas de pépin ?

En cas de perturbation technique :

mon portable +33 6 08 98 08 94

Pour toute question sur le thème (et les thèmes à venir)

jean-philippe.noat@cellebrite.com

INVESTIGATION SUR LE BLUETOOTH

Intérêt de l'investigation sur Bluetooth

- Investigation sur accident
- Proximité avec un contact
- Prouver si un conducteur a été distrait avant la survenue d'un accident mortel
- Étaient-ils vraiment connectés à Bluetooth ?
- Comment peut-on en être sûr ?
- Qu'en est-il d'un appareil Bluetooth «vu»?

Ou télécharger les images

- Le but est que vous puissiez faire vos propres recherches
- <https://thebinaryhick.blog/2020/02/15/android-10-image-now-available/>
- http://downloads.digitalcorpora.org/corpora/cell-phones/ios_13_4_1/
- Approche originale : on connaît ce qui est fait au téléphone et à nous de retrouver cela dans l'analyse.

Liste des bases de données / fichiers intéressants

- DarArchive/root/private/var/containers/Shared/SystemGroup/<GUID>/Library/Database/com.apple.MobileBluetooth.ledevices.other.db
- DarArchive/root/private/var/containers/Shared/SystemGroup/<GUID>/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db
- DarArchive/root/private/var/containers/Shared/SystemGroup/<GUID>/Library/Preferences/com.apple.MobileBluetooth.devices.plist
- Note: les fichiers WAL doivent bien sur être investigués

Liste des bases de données / fichiers intéressants

- com.apple.MobileBluetooth.ledevices.other.db: Cette base de données garde trace des périphériques « basses énergies » que l'iOS détecte à proximité. Cela inclut en particulier les périphériques qui restent en mode hibernation sauf quand ils sont connectés. Ils opèrent à une fréquence différente du Bluetooth normal. Ceux-ci incluent souvent des appareils d'exercice physique, des écouteurs et plus encore.
- com.apple.MobileBluetooth.ledevices.paired.db: Cette base de données garde trace des périphériques basse énergie qui sont appairés avec le périphérique sous iOS (iPhone / iPad)
- com.apple.MobileBluetooth.devices.plist: Ce plist suit les appareils appairés et les dates et heures des dernières détections. **C'est l'un des fichiers les plus importants nécessitant une attention particulière pour tout ce qui est information d'appairage !**

Dans les données du téléphone

```

  containers (51662 files, 3,606,063 KB)
  > Bundle (51086 files, 3,532,499 KB)
  > Data (44 files, 8,184 KB)
  > Shared (532 files, 65,379 KB)
  > SystemGroup (532 files, 65,379 KB)
    > 1CC899CC-CD20-4F7B-A70E-638F6CAAADA (1 file, 1 KB)
    > 7BBDD07-A637-4628-8A28-3E1E7F47B623 (1 file, 1 KB)
    > 8D1FDDF8-CC9C-4645-AE40-88A242D3A91A (2 files, 1 KB)
    > 26EC873E-9B6D-4340-9E0C-7437382F2E6A (2 files, 443 KB)
    > 57EAE28C-99D9-4AF6-9167-83A8F7E84DA8 (1 file, 1 KB)
    > 774A13CA-9379-4875-86DD-89B22A1B0FE0 (2 files, 1 KB)
    > 994DFF21-BD24-4EAE-BE23-C9138AD8A9E1 (2 files, 1 KB)
    > 5367B37E-F77D-4359-AAE2-C15D8CA2D329 (1 file, 1 KB)
  > 9140AD4D-45D5-49D5-8AA8-1CD264CF295D (8 files, 2,424 KB)
    > Library (7 files, 2,424 KB)
      > Caches (0 files, 0 KB)
      > Database (6 files, 2,417 KB)
        com.apple.MobileBluetooth.ledevices.other.db
        com.apple.MobileBluetooth.ledevices.other.db-shm
        com.apple.MobileBluetooth.ledevices.other.db-wal
        com.apple.MobileBluetooth.ledevices.paired.db
        com.apple.MobileBluetooth.ledevices.paired.db-shm
        com.apple.MobileBluetooth.ledevices.paired.db-wal

```

```

7.....:4~...).ce7M2v...
.....:4~...).s...../.....
...K.....d.....}.....I.....b.....
{.....~.1....}.Q...8.j.....8....
.....0.....6.T...0.....
.....
.....U.5.U#.E1DF27E2-DA99-
A6D7-78F8-5CAEFB839F03[TV] Spanky
Public 64:1C:B0:AE:6C:B3.\WJ...U.
.=.....00ECDB81-308C-AEAD-FDCB-E
1E26035DFE7Public FC:F1:36:20:22:
76.[.a.*.U;.=.....7A272D6E-9BA9-
057F-8105-74AA4CF9A137This Is...s
AirPods ProPublic 38:EC:0D:E2:49
:CF.ZzJ.'.U..=.....C9C3EBC4-632C
-C716-BEC9-CEB370144E9DPublic F0:
18:98:86:3F:52.I~J...U..=.....42
004563-1678-4B78-98FD-EBCBED0E1DB
5Public D0:03:4B:35:34:64.^J.F.U
..=.....1F1C7282-DEB9-E5D7-B209-
5177E1B3B61EPublic AC:BC:32:75:4D
:1A.0.J.E.U..=.....1E8741B3-D89B
-DB06-B93E-9016BB751217Public D0:
03:4B:04:A7:1D.0iJ.@.U..=.....E5
D0E147-763B-F89E-D82B-8353B027F1C
4Public 50:DE:06:6D:02:F0.^J.A.U
..=.....D7BAB041-93BC-B651-3E24-
90B895AF9E67Public BC:54:36:C9:51
:2F.^J.,.U..=.....B24CB2A1-BC79
-8AB8-87DA-03DFEE02F736Public 70:
48:0F:E5:8F:3F.ZeJ.-.U..=.....A3
E6C910-CBC2-3834-2381-9425EA34946
1Random FD:A0:F6:AE:8B:50.Z.J.;.U

```

Dans Physical Analyzer

Josh's AirPods	Headset	30/03/2020 09:14
AirPods Pro	Headset	13/04/2020 12:28
	Unknown	

Connectivity nature ▼
Detected
Detected
Detected
Detected

Dans Physical Analyzer

Hue Lamp	Unknown		Paired
Hue Lamp	Unknown		Paired
Office	Unknown		Paired
This Is's Apple Watch	Unknown		Paired
Charge 3	Unknown		Paired
	Unknown		Paired
	Unknown		Detected
Josh's AirPods	Headset		Paired
AirPods Pro	Headset		Paired
Apple Watch	Unknown		Paired
Apple Watch	Unknown		Detected

Dans PA en triant par appareil

104				Josh's AirPods	Unknown		Bluetooth	Address Public 7C:04:D0:89:89
105				Josh's AirPods	Headset		Bluetooth	Address 7C:04:D0:89:89:A0
106				Josh's AirPods	Headset	30/03/2020 09:14	Bluetooth	Address 7C:04:D0:89:89:A0

Un périphérique peut être détecté et plus tard appairé à votre appareil sous iOS.

Ici on voit que les airpods de Josh ont été appairés (Line 105) et la dernière détection date du 30 mars 2020 à 9h14 (TZ ?)

Cette information est importante car elle indique l'heure de déconnexion du périphérique (quand l'appairage se termine).

PA montre 2 enregistrements 1 sur l'appairage, 1 sur la date de dernière détection

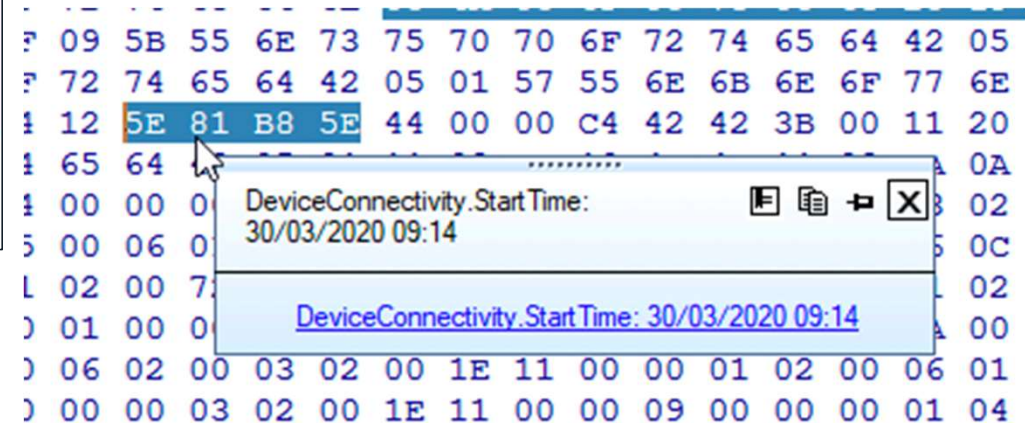
Dans PA en triant par appareil



com.apple.MobileBluetooth.devices.plist trace tous les appairages Bluetooth pas seulement les “basses” énergies. C’est là où la recherche avec des véhicules entre en jeu.

Si vous voulez prouver que le conducteur était en main libre quand un appel ou un SMS arrive, ce fichier est important.

Cependant Apple stocke les dates / heure en UTC mais pas là....



Attention au Timezone

» Device Connectivity Translate Go to

Device Name:

Hank's AirPods

Device type:

Headset

Timestamp:

3/16/2018 06:22

Connectivity method:

Bluetooth

Connectivity nature:

Detected

Artifact Family:

Source Repository Path:

Source:

Source file:

[Heather Mahalik's iPhone/containers/Shared/SystemGroup/systemgroup.com.apple.bluetooth/Library/Preferences/com.apple.MobileBluetooth.devices.plist:0x22D \(Size: 3022 bytes\)](#)

Device Identifiers

Address

7C:04:D0:A6:EE:82

La valeur “LastSeenTime” est stockée en UTC avec le timezone ajusté pour America/New York – correspondant au TZ de Heather (UTC-4:00). **Toute l’investigation peut devenir fausse si on ne prend pas en compte ce paramètre.**

ServiceNetSharingUser : AsciiString = Unsupported

SdpCacheSize : integer = 2250

LastSeenTime : integer = 1521181350

DeviceClass : data = 18 04 24 00

Name : UnicodeString = Hank's AirPods

🕒 Unix Seconds (UTC)	2018-03-16 06:22:30.0000000 Z
→ 🕒 Unix Seconds	2018-03-16 02:22:30.0000000 -04:00
🕒 Unix Milliseconds (Java Time) (UTC)	1970-01-18 14:33:01.3500000 Z

Retour à la voiture

```
▲ A0:56:B2:4C:B3:73 : dict = {  
  DefaultName : AsciiString = Handsfree  
  LastHandsfreeVersion : data = 06 01  
  ServiceA2DP : AsciiString = Unknown  
  PhonebookSyncSettings : integer = 31  
  LastAVRCPControllerSupportedFeatures : data = 41 00  
  ServiceAACPP : AsciiString = Unknown  
  ServiceRemote : AsciiString = Unknown  
  ServiceNetSharingUser : AsciiString = Unknown  
  ServiceBraille : AsciiString = Unsupported  
  LastSeenTime : integer = 1582224378  
  Name : AsciiString = Subaru BT
```

Fin de connexion à la SUBARU le 20 février 2020 à 18h46. Cela correspond à un changement de véhicule. Le 18h46 correspond à une heure locale et pas du tout à de l'UTC et le lastseentime correspond à la déconnexion du véhicule.

Original	date	format
1582224378	2/20/2020 6:46:18 PM	Unix seconds

Carplay

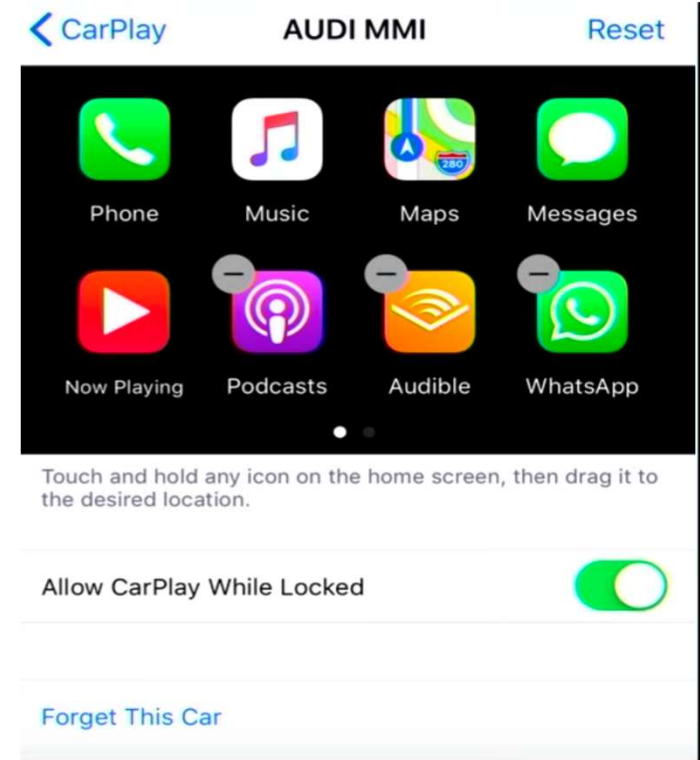
/mobile/Library/Preferences/com.apple.carplay.plist

▼ Root	Dictionary	(2 items)
▼ AppBlacklist	Array	(2 items)
Item 0	String	com.apple.carplay.blacklisted
Item 1	String	com.apple.carplay.blacklisted-nav
▼ pairings	Dictionary	(3 items)
▼ C2BF6EB1-751D-4C82-864C-BD845ABC1619	Dictionary	(2 items)
name	String	Volkswagen
▼ carPlayProtocols	Array	(1 item)
Item 0	String	com.vwag.infotainment.carplay.exlap
▼ 4BE58249-F22D-4096-B8D4-1CA81D1DFF1D	Dictionary	(2 items)
name	String	AUDI MMI
▼ carPlayProtocols	Array	(0 items)
▼ 58CC10AB-96A1-4CA4-A2E2-34A5A18F9FCF	Dictionary	(2 items)
name	String	Honda Display Audio
▼ carPlayProtocols	Array	(5 items)
Item 0	String	com.honda.cp.background
Item 1	String	com.honda.hondalink.hlc
Item 2	String	com.honda.cp.pet.honda
Item 3	String	com.honda.cp.allhonda
Item 4	String	com.honda.cp.honda

Carplay : configuration des icônes

/mobile/Library/Springboard/<GUID>-CarDisplay.... IconState.plist

▼ Root	Dictionary	(3 items)
▼ metadata	Dictionary	(6 items)
OEMIconLabel	String	Audi MMI
maxIconColumnCount	Number	4
▼ hiddenIcons	Array	(0 items)
screenBounds	String	{{0, 0}, {400, 240}}
maxIconRowCount	Number	2
displaysOEMIcon	Boolean	YES
▼ iconLists	Array	(2 items)
▼ Item 0	Array	(8 items)
Item 0	String	com.apple.mobilephone
Item 1	String	com.apple.Music
Item 2	String	com.apple.Maps
Item 3	String	com.apple.MobileSMS
Item 4	String	com.apple.cardisplay.nowplaying
Item 5	String	com.apple.podcasts
Item 6	String	com.audible.iphone
Item 7	String	net.whatsapp.WhatsApp
▼ Item 1	Array	(7 items)
Item 0	String	com.amazon.mp3.AmazonCloudPlayer
Item 1	String	com.pandora
Item 2	String	com.spotify.client
Item 3	String	com.apple.iBooks
Item 4	String	com.apple.cardisplay.OEM
Item 5	String	com.google.Maps
Item 6	String	com.waze.iphone
▼ buttonBar	Array	(0 items)



Carplay : Connection

knowledgeC.db

	Local Time	Activity	Output
1	2019-07-18 06:46:24	Device Plug In Status	[IS PLUGGED IN: UNPLUGGED] [USAGE IN SECONDS: 8328] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 06:46:24]
2	2019-07-18 09:05:12	Device Plug In Status	[IS PLUGGED IN: PLUGGED IN] [USAGE IN SECONDS: 316] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 09:05:12]
3	2019-07-18 09:07:12	CarPlay Connected	[CARPLAY CONNECTED: CONNECTED] [USAGE IN SECONDS: 4] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 09:07:12]
4	2019-07-18 09:10:27	CarPlay Connected	[CARPLAY CONNECTED: DISCONNECTED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 09:10:27]
5	2019-07-18 09:10:28	Device Plug In Status	[IS PLUGGED IN: UNPLUGGED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 09:10:28]
6	2019-07-18 09:10:28	Device Plug In Status	[IS PLUGGED IN: PLUGGED IN] [USAGE IN SECONDS: 1480] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 09:10:28]
7	2019-07-18 09:10:33	CarPlay Connected	[CARPLAY CONNECTED: CONNECTED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 09:10:33]
8	2019-07-18 09:35:08	Device Plug In Status	[IS PLUGGED IN: UNPLUGGED] [USAGE IN SECONDS: 14092] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 09:35:08]
9	2019-07-18 09:35:10	CarPlay Connected	[CARPLAY CONNECTED: DISCONNECTED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 09:35:10]
10	2019-07-18 13:30:00	Device Plug In Status	[IS PLUGGED IN: PLUGGED IN] [USAGE IN SECONDS: 128] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 13:30:00]
11	2019-07-18 13:32:08	Device Plug In Status	[IS PLUGGED IN: UNPLUGGED] [USAGE IN SECONDS: 15720] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 13:32:08]
12	2019-07-18 17:54:08	Device Plug In Status	[IS PLUGGED IN: PLUGGED IN] [USAGE IN SECONDS: 2020] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 17:54:08]
13	2019-07-18 17:54:13	CarPlay Connected	[CARPLAY CONNECTED: CONNECTED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 17:54:13]
14	2019-07-18 18:27:48	Device Plug In Status	[IS PLUGGED IN: UNPLUGGED] [USAGE IN SECONDS: 1152] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 18:27:48]
15	2019-07-18 18:27:50	CarPlay Connected	[CARPLAY CONNECTED: DISCONNECTED] [USAGE IN SECONDS: 4] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 18:27:50]

Carplay : Messages avec Siri

knowledgeC.db

	Local Time	Activity	Output
1	2019-07-18 09:07:26	Siri Usage	[APP NAME: com.apple.siri.ui.begin] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18
2	2019-07-18 09:07:51	Siri Usage	[APP NAME: com.apple.siri.ui.end] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 13
3	2019-07-18 09:08:21	Siri Usage	[APP NAME: com.apple.siri.ui.begin] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18
4	2019-07-18 09:08:55	Siri Usage	[APP NAME: com.apple.siri.ui.end] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 13
5	2019-07-18 09:08:58	Siri Usage	[APP NAME: com.apple.siri.ui.begin] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18
6	2019-07-18 09:09:15	Siri Usage	[APP NAME: com.apple.siri.ui.end] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 13
7	2019-07-18 09:27:05	Siri Usage	[APP NAME: com.apple.siri.ui.begin] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18
8	2019-07-18 09:27:32	Siri Usage	[APP NAME: com.apple.siri.ui.end] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 13

Carplay : Messages (global)

knowledgeC.db, InteractionsC.db, sms.db

	Local Time	Activity	Output
70	2019-07-18 09:07:10	SMS Chat - Message Read	[MESSAGE DATE: 2019-07-18 13:06:27] [DATE DELIVERED: N/A] [DATE READ: 2019-07-18 13:07:10] [MESSAGE: Bring bacon.] [CONTACT ID: +] [SERVICE: iMess.
71	2019-07-18 09:07:12	CarPlay Connected	[CARPLAY CONNECTED: CONNECTED] [USAGE IN SECONDS: 4] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 13:07:08] [END: 2019-07-18 13:07:12] [EN
72	2019-07-18 09:07:15	Audio Output	[AUDIO IDENTIFIER: Speaker] [AUDIO PORT NAME: Speaker] [AUDIO PORT TYPE: Speaker] [USAGE IN SECONDS: 51396] [DAY OF WEEK: Wednesday] [GMT OFFSET: -4] [STA
73	2019-07-18 09:07:15	Now Playing	[BUNDLE ID: com.apple.Music] [NOW PLAYING ALBUM: All Your Fault: Pt. 1 - EP] [NOW PLAYING ARTIST: Bebe Rexha] [NOW PLAYING GENRE: Pop] [NOW PLAYING TITLE: I G
74	2019-07-18 09:07:15	Now Playing	[BUNDLE ID: com.apple.Music] [NOW PLAYING ALBUM: All Your Fault: Pt. 1 - EP] [NOW PLAYING ARTIST: Bebe Rexha] [NOW PLAYING GENRE: Pop] [NOW PLAYING TITLE: I G
75	2019-07-18 09:07:17	App Usage	[ZBUNDLEID: com.apple.MobileSMS] [ZDISPLAYNAME: None] [ZIDENTIFIER: None] [ZPERSONID: None] [ZDIRECTION: 3] [ZISRESPONSE: 0] [ZMECHANISM: 4] [ZRECIPIENTC.
76	2019-07-18 09:07:18	SMS Chat	[MESSAGE DATE: 2019-07-18 13:07:18] [DATE DELIVERED: 2019-07-18 13:07:19] [DATE READ: N/A] [MESSAGE: 😊] [CONTACT ID: +1] [SERVICE: iMessage] [ACC
77	2019-07-18 09:07:18	Application Intents	[BUNDLE ID: com.apple.MobileSMS] [APP NAME: Messages] [INTENT CLASS: INSendMessageIntent] [INTENT VERB: SendMessage] [USAGE IN SECONDS: 0] [SERIALIZED INTE
78	2019-07-18 09:07:19	SMS Chat - Message Delivered	[MESSAGE DATE: 2019-07-18 13:07:18] [DATE DELIVERED: 2019-07-18 13:07:19] [DATE READ: N/A] [MESSAGE: 😊] [CONTACT ID: +1] [SERVICE: iMessage] [ACC
79	2019-07-18 09:07:26	Now Playing	[BUNDLE ID: com.apple.Music] [NOW PLAYING ALBUM: All Your Fault: Pt. 1 - EP] [NOW PLAYING ARTIST: Bebe Rexha] [NOW PLAYING GENRE: Pop] [NOW PLAYING TITLE: I G
80	2019-07-18 09:07:29	Audio Input	[AUDIO IDENTIFIER: Built-In Microphone] [AUDIO PORT NAME: iPhone Microphone] [AUDIO PORT TYPE: MicrophoneBuiltIn] [USAGE IN SECONDS: 16] [DAY OF WEEK: Thursda
81	2019-07-18 09:07:46	SMS Chat	[MESSAGE DATE: 2019-07-18 13:07:46] [DATE DELIVERED: 2019-07-18 13:07:47] [DATE READ: N/A] [MESSAGE: Last time I asked if you want to bacon you didn't so no bacon]
82	2019-07-18 09:07:46	App Usage	[ZBUNDLEID: com.apple.MobileSMS] [ZDISPLAYNAME: None] [ZIDENTIFIER: None] [ZPERSONID: None] [ZDIRECTION: 1] [ZISRESPONSE: 0] [ZMECHANISM: 4] [ZRECIPIENTCC
83	2019-07-18 09:07:46	App Usage	[ZBUNDLEID: com.apple.MobileSMS] [ZDISPLAYNAME: None] [ZIDENTIFIER: None] [ZPERSONID: None] [ZDIRECTION: 3] [ZISRESPONSE: 0] [ZMECHANISM: 4] [ZRECIPIENTC.
84	2019-07-18 09:07:47	SMS Chat - Message Delivered	[MESSAGE DATE: 2019-07-18 13:07:46] [DATE DELIVERED: 2019-07-18 13:07:47] [DATE READ: N/A] [MESSAGE: Last time I asked if you want to bacon you didn't so no bacon]
85	2019-07-18 09:07:47	Application Intents	[BUNDLE ID: com.apple.MobileSMS] [APP NAME: Messages] [INTENT CLASS: INSendMessageIntent] [INTENT VERB: SendMessage] [USAGE IN SECONDS: 0] [SERIALIZED INTE
86	2019-07-18 09:07:49	Audio Input	[AUDIO IDENTIFIER: 74:6F:F7:20:6D:77-Audio-AudioMain-103462616097708] [AUDIO PORT NAME: CarPlay] [AUDIO PORT TYPE: CarAudio] [USAGE IN SECONDS: 20] [DAY O.
87	2019-07-18 09:07:49	Now Playing	[BUNDLE ID: com.apple.Music] [NOW PLAYING ALBUM: All Your Fault: Pt. 1 - EP] [NOW PLAYING ARTIST: Bebe Rexha] [NOW PLAYING GENRE: Pop] [NOW PLAYING TITLE: I G

Utilisation d'une appli dans le véhicule

knowledgeC.db, cache_encryptedC.db

2019-07-18 18:17:07	Motion	[START TIME: 2019-07-18 22:17:07] [TIMESTAMP: 119538.986257] [TYPE: 4096] [CONFIDENCE: 3] [MOUNTED: 1] [MOUNTED CONFIDENCE: 2] [TURN: 0] [IS VEHICULAR: 1] [IS MOVING: 1] [VEHICLE
2019-07-18 18:18:14	Application In Focus	[BUNDLE ID: com.apple.podcasts] [USAGE IN SECONDS: 1] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 22:18:14] [END: 2019-07-18 22:18:15] [ENTRY CREATION: 2019-07-18
2019-07-18 18:18:16	Application In Focus	[BUNDLE ID: org.whispersystems.signal] [USAGE IN SECONDS: 1] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 22:18:16] [END: 2019-07-18 22:18:17] [ENTRY CREATION: 2019-
2019-07-18 18:18:17	Application In Focus	[BUNDLE ID: com.apple.CoreAuthUI] [USAGE IN SECONDS: 2] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 22:18:17] [END: 2019-07-18 22:18:19] [ENTRY CREATION: 2019-07-
2019-07-18 18:18:19	Application In Focus	[BUNDLE ID: org.whispersystems.signal] [USAGE IN SECONDS: 8] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 22:18:19] [END: 2019-07-18 22:18:27] [ENTRY CREATION: 2019-
2019-07-18 18:18:35	Motion	[START TIME: 2019-07-18 22:18:35] [TIMESTAMP: 119626.575791] [TYPE: 256] [CONFIDENCE: 3] [MOUNTED: 1] [MOUNTED CONFIDENCE: 2] [TURN: 0] [IS VEHICULAR: 1] [IS MOVING: 0] [VEHICLE

Vitesse et utilisation d'une appli

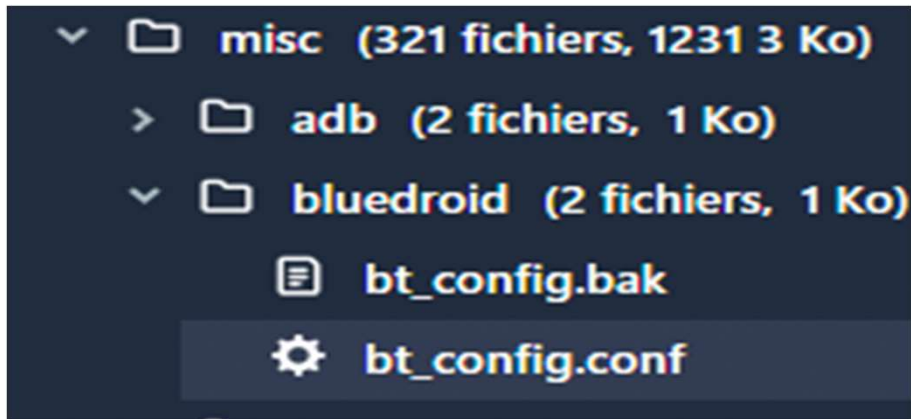
knowledgeC.db, Location DBS

2019-07-18 18:18:10	Location	[TIMESTAMP: 2019-07-18 22:18:10] [COORDINATES: 38.8608163284047, -77.0919290286513] [ALTITUDE: 71.3] [COURSE: 354.73147583] [SPEED (M/S): 0.720222222222] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:10	Location	[TIMESTAMP: 2019-07-18 22:18:10] [COORDINATES: 38.8608163284047, -77.0919290286513] [ALTITUDE: 71.3] [COURSE: 354.73147583] [SPEED (M/S): 0.720222222222] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:11	Location	[TIMESTAMP: 2019-07-18 22:18:11] [COORDINATES: 38.8608197452118, -77.0919294161854] [ALTITUDE: 71.6] [COURSE: 354.73147583] [SPEED (M/S): 0.205777777778] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:11	Location	[TIMESTAMP: 2019-07-18 22:18:11] [COORDINATES: 38.8608197452118, -77.0919294161854] [ALTITUDE: 71.6] [COURSE: 354.73147583] [SPEED (M/S): 0.205777777778] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:12	Location	[TIMESTAMP: 2019-07-18 22:18:12] [COORDINATES: 38.8608192813259, -77.0919293614724] [ALTITUDE: 71.7] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:12	Location	[TIMESTAMP: 2019-07-18 22:18:12] [COORDINATES: 38.8608192813259, -77.0919293614724] [ALTITUDE: 71.7] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:13	Location	[TIMESTAMP: 2019-07-18 22:18:13] [COORDINATES: 38.8608198121316, -77.0919294240802] [ALTITUDE: 71.7] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:13	Location	[TIMESTAMP: 2019-07-18 22:18:13] [COORDINATES: 38.8608198121316, -77.0919294240802] [ALTITUDE: 71.7] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:14	Location	[TIMESTAMP: 2019-07-18 22:18:14] [COORDINATES: 38.8608203424164, -77.0919294866206] [ALTITUDE: 71.8] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:14	Location	[TIMESTAMP: 2019-07-18 22:18:14] [COORDINATES: 38.8608203424164, -77.0919294866206] [ALTITUDE: 71.8] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:14	Application In Focus	[BUNDLE ID: com.apple.podcasts] [USAGE IN SECONDS: 1] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 22:18:14] [END: 2019-07-18 22:18:15] [ENTRY CREATION: 2019-07-18 22:18:14]
2019-07-18 18:18:15	Location	[TIMESTAMP: 2019-07-18 22:18:15] [COORDINATES: 38.8608187196236, -77.0919292952259] [ALTITUDE: 71.8] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:15	Location	[TIMESTAMP: 2019-07-18 22:18:15] [COORDINATES: 38.8608187196236, -77.0919292952259] [ALTITUDE: 71.8] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:16	Location	[TIMESTAMP: 2019-07-18 22:18:16] [COORDINATES: 38.8608192510033, -77.0919293578986] [ALTITUDE: 71.8] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:16	Location	[TIMESTAMP: 2019-07-18 22:18:16] [COORDINATES: 38.8608192510033, -77.0919293578986] [ALTITUDE: 71.8] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:16	Application In Focus	[BUNDLE ID: org.whispersystems.signal] [USAGE IN SECONDS: 1] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 22:18:16] [END: 2019-07-18 22:18:17] [ENTRY CREATION: 2019-07-18 22:18:16]
2019-07-18 18:18:17	Location	[TIMESTAMP: 2019-07-18 22:18:17] [COORDINATES: 38.8608195111715, -77.0919293885824] [ALTITUDE: 71.8] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:17	Location	[TIMESTAMP: 2019-07-18 22:18:17] [COORDINATES: 38.8608195111715, -77.0919293885824] [ALTITUDE: 71.8] [COURSE: 354.73147583] [SPEED (M/S): 0.0] [HORIZONTAL ACCURACY: 10.0]
2019-07-18 18:18:17	Application In Focus	[BUNDLE ID: com.apple.CoreAuthUI] [USAGE IN SECONDS: 2] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019-07-18 22:18:17] [END: 2019-07-18 22:18:19] [ENTRY CREATION: 2019-07-18 22:18:17]

Liste des bases de données / fichiers intéressants

ANDROID

- data/com.android.connectivity.metrics/databases/events.db (n'existe plus).



Liste des bases de données / fichiers intéressants

ANDROID

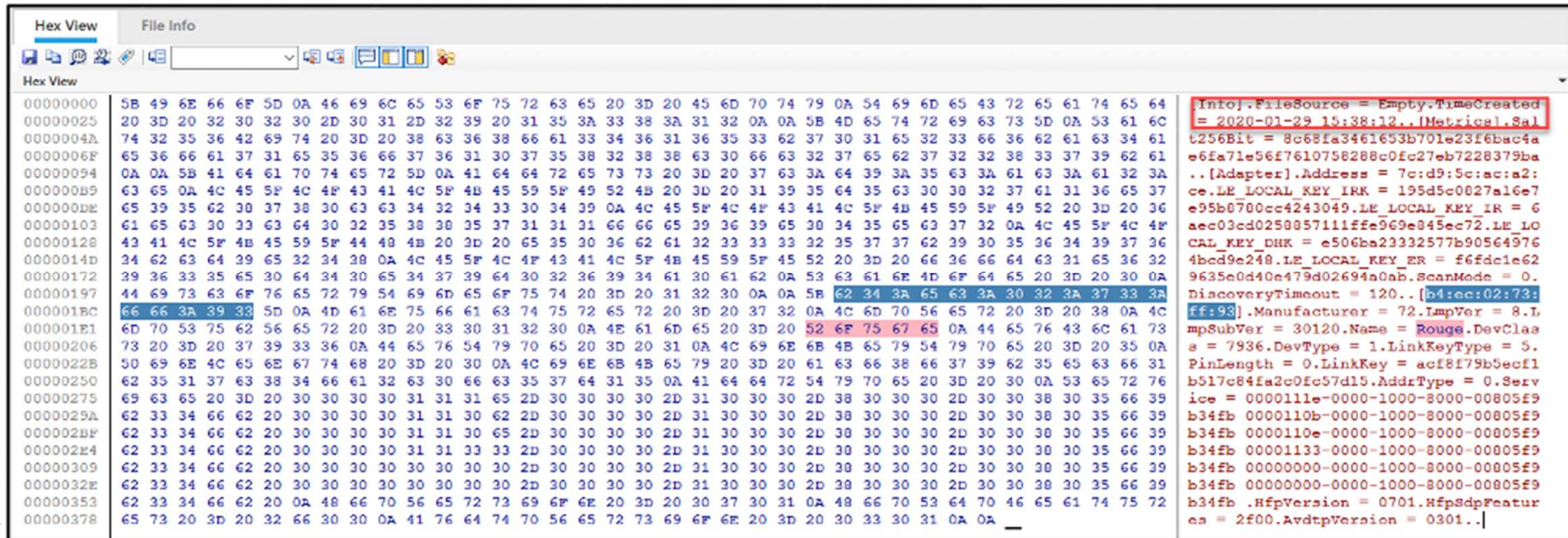
- /data/misc/bluedroid/bt_config.conf
- /data/data/com.google.android.gms/shared_prefs/coffee_preferences.xml
- /data/data/com.google.android.projection.gearhead/shared_prefs/app_state_shared_preferences.xml – dernière exécution du bluetooth
- /data/data/com.google.android.projection.gearhead/shared_prefs/com.google.android.gms.analytics.prefs.xml - Enregistre la 1^{ère} exécution et la date / heure exécution
- /data/data/com.google.android.projection.gearhead/shared_prefs/common_user_settings.xml – Utiliser pour connaître les adresses mac des véhicules
- /data/data/com.google.android.gms/shared_prefs/bluetooth_addresses_prefs.xml – Vérification des adresses mac des véhicules

Liste des bases de données / fichiers intéressants

ANDROID

- /data/user_de/0/com.android.bluetooth/shared_prefs/bluetooth_volume_map.xml – adresses mac appairées
- /data/user_de/0/com.android.bluetooth/shared_prefs/phonebook_access_permission.xml – adresses mac appairées et peut être associé à la bdd peoplelog.db qui met à jour les contacts vers le véhicule quand le périphérique est connecté en USB/Bluetooth.
- /data/data/com.google.android.gms/databases/carservicedata.db – Véhicules autorisés
- /data/data/com.google.android.googlequicksearchbox/app_shared_prefs/SearchSettings.bin – Comptes google associés avec l'adresse mac du véhicule
- /data/user_de/0/com.android.bluetooth/databases/bluetooth_db – La table métadatas montre les adresses Mac appairées.

Android et le Bluetooth

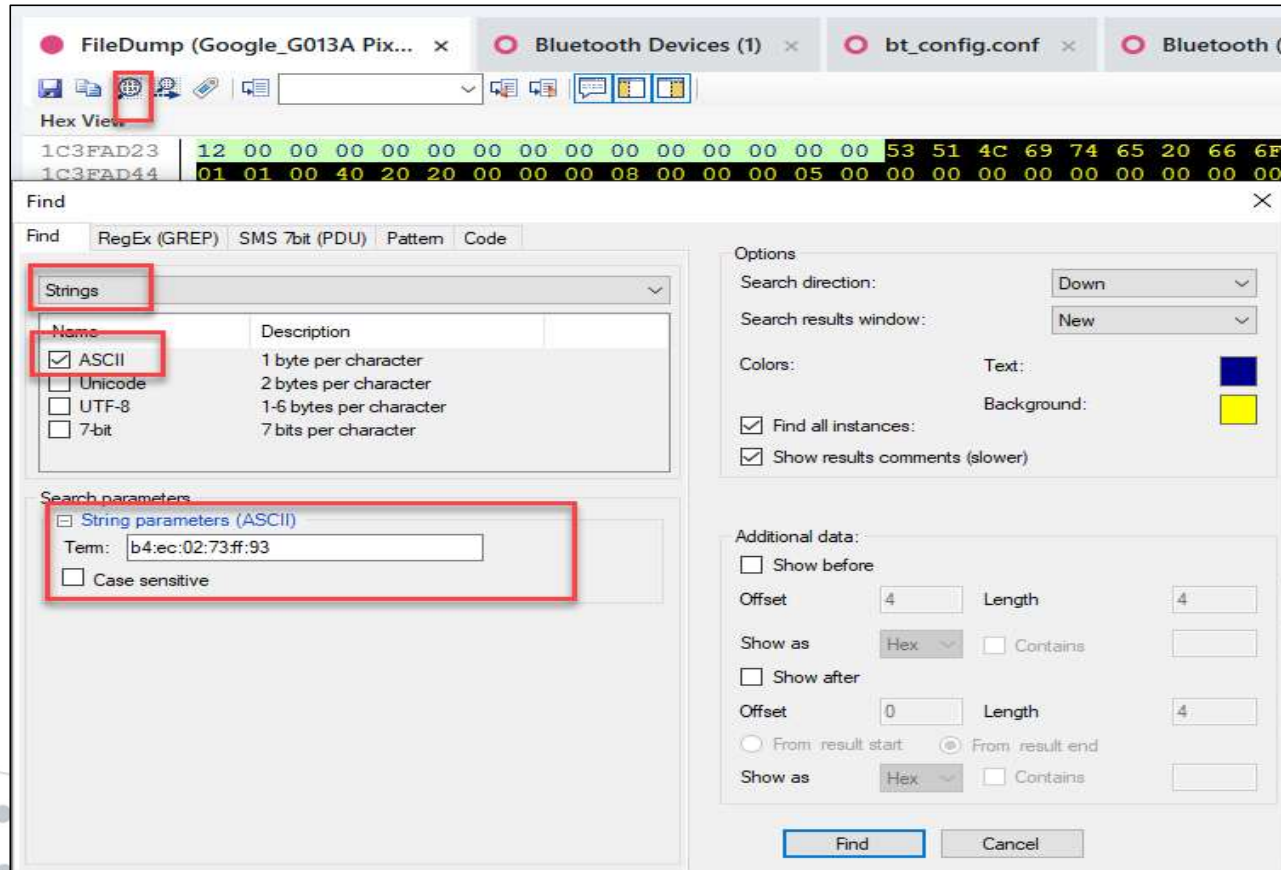


Hex View File Info

Hex View

Info: FileSource = Empty, TimeCreated = 2020-01-29 15:38:12, Metrics1.Sal t256Bit = 8c68fa3461653b701e23f6bac4a e6fa71e56f7610758288c0fc27eb7228379ba ..[Adapter].Address = 7c:d9:5c:ac:a2: ce.LE_LOCAL_KEY_IRK = 195d5c0827a16e7 e95b8780cc4243049.LE_LOCAL_KEY_IR = 6 aec03cd0258857111ffe969e845ec72.LE LO CAL_KEY_DHAK = e506ba23332577b90564976 4bcd9e248.LE_LOCAL_KEY_ER = f6fdc1e62 9635e0d40e479d02694a0ab.ScanMode = 0. DiscoveryTimeout = 120..[b4:ec:02:73: ff:93].Manufacturer = 72.LmpVer = 8.L mpSubVer = 30120.Name = Rouge.DevClas s = 7936.DevType = 1.LinkKeyType = 5. PinLength = 0.LinkKey = acf8f79b5ecf1 b517c84fa2c0fc57d15.AddrType = 0.Serv ice = 0000111e-0000-1000-8000-00805f9 b34fb 0000110b-0000-1000-8000-00805f9 b34fb 0000110e-0000-1000-8000-00805f9 b34fb 00001133-0000-1000-8000-00805f9 b34fb 00000000-0000-1000-8000-00805f9 b34fb 00000000-0000-1000-8000-00805f9 b34fb .HfpVersion = 0701.HfpSdpFeatur es = 2f00.AvdtpVersion = 0301..]

Investigations basées sur l'adresse mac



Résultat de la recherche (triée par source)

Search [106 results]

#	Offset	Length	Value	Source	More
5	0x3A3848AF	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.gms/databases/carservicedata.db	
9	0x3A3FAC79	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.gms/shared_prefs/bluetooth_addresses_prefs.xml	
6	0x3A3F3A1A	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.gms/shared_prefs/coffee_preferences.xml	
7	0x3A3F3AC1	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.gms/shared_prefs/coffee_preferences.xml	
8	0x3A3F3C4D	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.gms/shared_prefs/coffee_preferences.xml	
3	0x1E0F7D1D	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.googlequicksearchbox/app_shared_prefs/SearchSettings.bin	
4	0x1E0F8AD2	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.googlequicksearchbox/app_shared_prefs/SearchSettings.bin	
10	0x5C4500B4	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.projection.gearhead/shared_prefs/common_user_settings.xml	
11	0x5C450131	0x11	B4:EC:02:73:FF:93	/data/data/com.google.android.projection.gearhead/shared_prefs/common_user_settings.xml	
1	0x1A9CCCC1	0x11	b4:ec:02:73:ff:93	/data/misc/bluedroid/bt_config.bak	
2	0x1A9CD058	0x11	b4:ec:02:73:ff:93	/data/misc/bluedroid/bt_config.conf	RecognizedDevice.Key
34	0xE122671C	0x11	B4:EC:02:73:FF:93	/data/user_de/0/com.android.bluetooth/databases/bluetooth_db-wal	
35	0xE122776E	0x11	B4:EC:02:73:FF:93	/data/user_de/0/com.android.bluetooth/databases/bluetooth_db-wal	
36	0xE122874A	0x11	B4:EC:02:73:FF:93	/data/user_de/0/com.android.bluetooth/databases/bluetooth_db-wal	
37	0xE122979E	0x11	B4:EC:02:73:FF:93	/data/user_de/0/com.android.bluetooth/databases/bluetooth_db-wal	
38	0xE122A77A	0x11	B4:EC:02:73:FF:93	/data/user_de/0/com.android.bluetooth/databases/bluetooth_db-wal	
39	0xE122B7CE	0x11	B4:EC:02:73:FF:93	/data/user_de/0/com.android.bluetooth/databases/bluetooth_db-wal	
40	0xE122C7AC	0x11	B4:EC:02:73:FF:93	/data/user_de/0/com.android.bluetooth/databases/bluetooth_db-wal	
41	0xE122D7FE	0x11	B4:EC:02:73:FF:93	/data/user_de/0/com.android.bluetooth/databases/bluetooth_db-wal	

Carservicedata.db

SQLite wizard

Double-click or drag the database tables to the work area and link database fields.

Query builder DB viewer

main

- allowedcars
- android_metadata
- rejectedcars

allowedcars (main)


- ☐ *
- ☒ id integer
- ☒ manufacturer text
- ☒ model text
- ☒ modelyear text
- ☒ vehicleid text
- ☐ vehicleidclient text

Visible	Expression	Column Name	Sort Type	Sort Order	Aggregate	<input type="checkbox"/> Grouping	Criteria
<input checked="" type="checkbox"/>	allowedcars.id					<input type="checkbox"/>	
<input checked="" type="checkbox"/>	allowedcars.manu					<input type="checkbox"/>	
<input checked="" type="checkbox"/>	allowedcars.mode					<input type="checkbox"/>	
<input checked="" type="checkbox"/>	DateTime(allowedcars.connectiontime / 1000, 'unixepoch', 'localtime')	connection time				<input type="checkbox"/>	
<input checked="" type="checkbox"/>	allowedcars.mode					<input type="checkbox"/>	

```
Select allowedcars.id,  
allowedcars.manufacturer,  
allowedcars.model,  
DateTime(allowedcars.connectiontime / 1000, 'unixepoch', 'localtime') As  
"connection time",
```

Carservicedata.db

id ▾	manufacturer ▾	model ▾	modelyear ▾	vehicleid ▾	vehicleidclient ▾
1	Nissan	Nissan_Bosch_SUV	18 MY	137931164SunJan11379050x3001	f760dfa1380d9e4e

bluetoothConnectionAllowed ▾	 connectiontime ▾	nickname ▾	bluetoothaddress ▾	wifissid ▾	wifibssid ▾	wifipassword ▾	wifisecurity ▾
1	09/02/2020 19:09		B4:EC:02:73:FF:93				-1

02/09/2020	13:44	Connect to car
	13:46	“Give me directions to Sir Walter Coffee in Holly Springs, North Carolina.”
	13:47	Started “NPR Up First” podcast
	13:49	Got directions to Sir Walter Coffee in Holly Springs, NC
	13:51	Started “Digital Forensics Survival Podcast.”
	13:59	Disconnect from car
	14:09	Connect to car
		Continued “Digital Forensics Survival Podcast.”
	14:16	Disconnect from car

coffee_preferences.xml

coffee_preferences.xml x FileDump (Google_G013A Pix... x common_user_settings.xml x com.go

Text View Hex View File format viewer File Info

Search Clear

```

map = {
  auth_trust_agent_pref_trusted_place_home_work_account : string = thisisdfr@gmail.com
  auth_trust_agent_pref_trusted_bluetooth_titleB4:EC:02:73:FF:93 : string = Rouge
  auth_unlock_attempt_count_Voiceunlock : int = 0
  auth_trust_agent_pref_trusted_bluetooth_addressB4:EC:02:73:FF:93 : boolean = True
  auth_trust_agent_pref_trustlet_enabled_VoiceUnlockTrustletChimeraService : boolean = False
  coffee_last_known_is_keyguard_secure : boolean = True
  coffee_last_is_keyguard_secure_set_timestamp_seconds : long = 1580312558
  auth_trust_agent_pref_bluetooth_device_needs_security_approval_key_B4:EC:02:73:FF:93 : boolean = False
  promotion_status_for_1 : int = 1
  auth_trust_agent_pref_first_notification_shown_ : boolean = True
  onbody_lure_unlock_time_1581717493381 : int = 2
  auth_trust_agent_pref_trusted_place_home_work_address_last_fetch_thisisdfr@gmail.com : lon
  onbody_lure_unlock_time_1581706455755 : int = 1
  last_notification_time_2 : long = 1580392600733
  coffee_last_is_keyguard_secure_set_timestamp_confirmed : boolean = False
  onbody_lure_unlock_time_1581723659183 : int = 1
  coffee_last_log_trustlet_configuration_key : long = 1581717493408

```

2020-01-30 13:56:40.7330000 Z

2020-01-30 08:56:40.7330000 -05:00

Date	Time	Action
01/30/2020	08:56	Connect to car & setup app
	08:58	Started "NPR Up First" podcast

VS Code v1.48

File Tools Theme Help

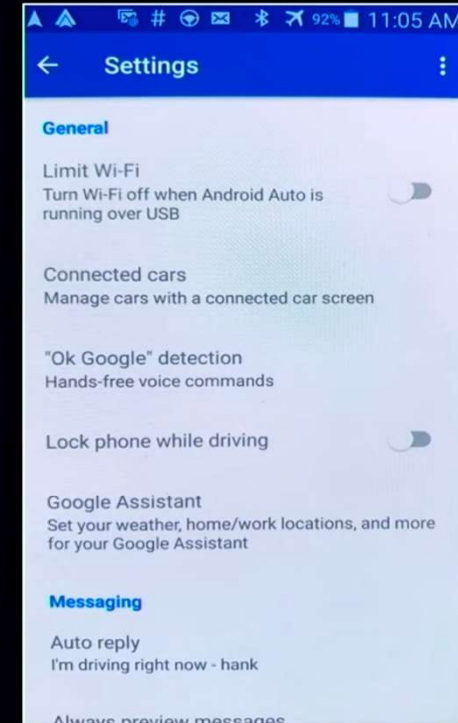
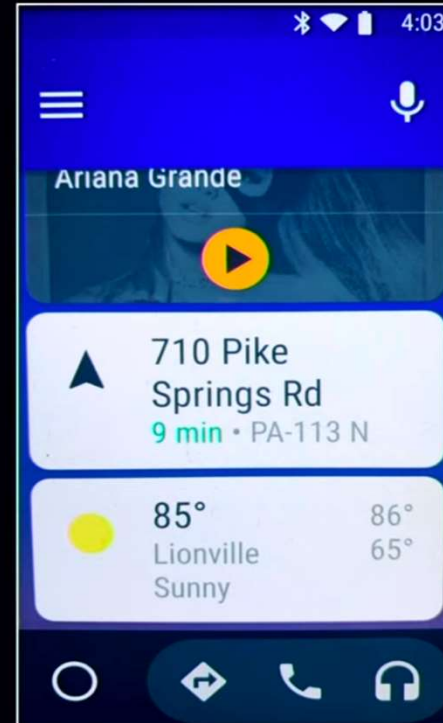
Time Decoding Time Encoding

Name	Timestamp
Apple Absolute Time (nq) (UTC)	2001-01-01 00:00:00.0000000 Z
Apple Absolute Time (nq)	2000-12-31 19:26:20.3526007 -05:00
Apple Chrome (UTC)	1601-01-19 06:59:52.6007330 Z
Google Chrome	1601-01-19 01:59:52.6007330 -05:00
Microsoft Time	0001-01-02 19:53:59.2600733
Unix Milliseconds (Java Time)	2020-01-30 13:56:40.7330000 Z
Unix Milliseconds (Java Time)	2020-01-30 08:56:40.7330000 -05:00

Configuration Android Auto

- `com.google.android.projection.gearhead/shared_prefs/`
 - `com.google.android.gms.analytics.prefs.xml`
 - Installed and Last Used Dates
 - `auto_launch_manager_shared_preferences.xml`
 - Bluetooth Connections
 - `app_state_shared_preferences.xml`
 - Last Usage Date
 - `common_user_settings.xml`
 - Bluetooth Settings
 - Caution – Last Accessed Date Incorrect

```
map = {  
    key_settings_autolaunch_enable : boolean = True  
    bt_autolaunch/GMC+IntelliLink/9C:8D:7C:18:8A:F8 : boolean = True
```



Connections Android Auto

- Syncing - /com.google.android.gms/databases/peoplelog.db

```
1  SELECT
2  account_name AS "Account",
3  datetime(timestamp/1000,"UNIXEPOCH") AS "Timestamp",
4  message
5  FROM
6  logs
7  order by "Timestamp" DESC
```

	Account	Timestamp	message
1	goodbyefelicia11@gmail.com	2019-07-06 15:40:28	***Sync start***: feed=null cannotHavePeople=true mode=0 contactOnly=false pageOnly=false skipMain=false
2	goodbyefelicia11@gmail.com	2019-07-06 15:40:28	Data still fresh; skip periodic sync.
3	goodbyefelicia11@gmail.com	2019-07-06 15:40:01	Stats=alri@2463f5b5
4	goodbyefelicia11@gmail.com	2019-07-06 15:40:01	***Sync finished***, duration: 4037
5	goodbyefelicia11@gmail.com	2019-07-06 15:39:57	***Sync start***: feed=null cannotHavePeople=true mode=2 contactOnly=false pageOnly=false skipMain=false
6	NULL	2019-06-27 05:18:29	Index version changed from 4
7	NULL	2019-06-27 05:18:29	Rebuilding index...
8	NULL	2019-06-27 05:18:29	Rebuilding index done.
9	goodbyefelicia11@gmail.com	2019-06-26 15:40:14	Stats=alri@18fff12b
10	goodbyefelicia11@gmail.com	2019-06-26 15:40:14	***Sync finished***, duration: 2749
11	goodbyefelicia11@gmail.com	2019-06-26 15:40:11	***Sync start***: feed=null cannotHavePeople=true mode=0 contactOnly=false pageOnly=false skipMain=false
12	NULL	2019-06-25 20:50:35	Index version changed from 3
13	NULL	2019-06-25 20:50:35	Rebuilding index...
14	NULL	2019-06-25 20:50:35	Rebuilding index done.

Connections Android Auto

- Bluetooth/USB - /system/powerManager
- Bluetooth - /com.android.settings/databases/search_index.db

```

1  SELECT
2  c2data_title,
3  c4data_summary_on,
4  c1data_rank,
5  c10screen_title,
6  c11class_name
7  FROM
8  prefs_index_content

```

	c2data_title	c4data_summary_on	c1data_rank	c10screen_title	c11class_name
19	Pointer speed		15	Language and input	com.android.settings.inputmethod.InputMethodAndLanguageSettings
20	Google voice typing	Automatic	15	Language and input	com.android.settings.inputmethod.InputMethodAndLanguageSettings
21	MY SENTRA		2	Bluetooth	com.android.settings.bluetooth.BluetoothSettings
22	GMC IntelliLink		2	Bluetooth	com.android.settings.bluetooth.BluetoothSettings
23	Smart card credential		14	Security	com.android.settings.SecuritySettings
24	Usage access	View which applications can access your device's usage history.	14	Security	com.android.settings.SecuritySettings
25	Bluetooth		2	Bluetooth	com.android.settings.bluetooth.BluetoothSettings
26	Samsung keyboard	Samsung keyboard	15	Language and input	com.android.settings.inputmethod.InputMethodAndLanguageSettings
27	Make passwords visible	Show password characters briefly as you type them.	14	Security	com.android.settings.SecuritySettings
28	Install from device storage	Install certificates from storage.	14	Security	com.android.settings.SecuritySettings
29	Voice input		15	Language and input	com.android.settings.inputmethod.InputMethodAndLanguageSettings
30	Owner information	Show the device owner's information on the lock screen.	14	Security	com.android.settings.SecuritySettings
31	Security update service		14	Security	com.android.settings.SecuritySettings
32	Encryption		14	Encryption	com.android.settings.SecuritySettings

De quelle voiture parle-t-on ?

- Bluetooth Connections - /misc/bluedroid/bt_config.xml

```
▼ <N188 Tag="bc:75:36:75:8c:63">
  <N1 Tag="Timestamp" Type="int">1563280749</N1>
  <N2 Tag="Name" Type="string">MY SENTRA</N2>
  <N3 Tag="DevClass" Type="int">3408904</N3>
  <N4 Tag="DevType" Type="int">1</N4>
  <N5 Tag="AddrType" Type="int">0</N5>
  <N6 Tag="Manufacturer" Type="int">72</N6>
  <N7 Tag="LmpVer" Type="int">8</N7>
  <N8 Tag="LmpSubVer" Type="int">30120</N8>
  <N9 Tag="LinkKeyType" Type="int">5</N9>
  <N10 Tag="PinLength" Type="int">0</N10>
  <N11 Tag="LinkKey" Type="binary">5f860261b8678b0ae4fd54dffe70673b</N11>
  ▼ <N12 Tag="Service" Type="string">
```

```
▼ <N142 Tag="9c:8d:7c:18:8a:f8">
  <N1 Tag="Timestamp" Type="int">1561590989</N1>
  <N2 Tag="Name" Type="string">GMC IntelliLink</N2>
  <N3 Tag="DevClass" Type="int">3539976</N3>
  <N4 Tag="DevType" Type="int">1</N4>
  <N5 Tag="AddrType" Type="int">0</N5>
  <N6 Tag="Manufacturer" Type="int">10</N6>
  <N7 Tag="LmpVer" Type="int">5</N7>
  <N8 Tag="LmpSubVer" Type="int">8241</N8>
  <N9 Tag="LinkKeyType" Type="int">5</N9>
  <N10 Tag="PinLength" Type="int">0</N10>
  <N11 Tag="LinkKey" Type="binary">02b82d658060f4b5c6673cf383b0e1fb</N11>
  ▼ <N12 Tag="Service" Type="string">
```

GMT : Tuesday, July 16, 2019 12:39:09 PM
Your time zone : Tuesday, July 16, 2019 8:39:09 AM GMT-04:00 DST

GMT : Wednesday, June 26, 2019 11:16:29 PM
Your time zone : Wednesday, June 26, 2019 7:16:29 PM GMT-04:00 DST

- Where was the device connected?
 - /com.google.android.projection.gearhead/db/CloudCards.db – Local weather where connection initiated (BLOB)

Messages

- Google Voice
- MMSSMS.db
- Other Evidence:
 - Third Party Apps
 - Logs.db

SMS Mes...	7/16/2019 1:29:34 PM(UTC+0)	To: +170...	I'm doing this hands-free.	mmssms.db-wal : 0xC
SMS Mes...	7/16/2019 1:34:37 PM(UTC+0)	To: +170...	Stupid assistant can't do much so i'm texting while driving	mmssms.db-wal : 0x8
SMS Mes...	7/16/2019 1:34:40 PM(UTC+0)	To: +170...	Stupid assistant can't do much so i'm texting while driving	mmssms.db-wal : 0xC
SMS Mes...	7/16/2019 1:35:37 PM(UTC+0)	To: +170...	👊	mmssms.db-wal : 0xC
Call Log	7/16/2019 1:41:44 PM(UTC+0)	To: +170...	00:00:26	logs.db : 0x475FD
SMS Mes...	7/16/2019 1:53:56 PM(UTC+0)	To: +170...	Are you sending this through WhatsApp?	mmssms.db-wal : 0xC
Instant...	7/16/2019 1:54:39 PM(UTC+0)	From: 15... To: 1703...	I set this up distracted while driving, but now I can text you...	msgstore.db-wal : 0x5 com.whatsapp_prefer msgstore.db : 0xAF66 wa.db-wal : 0x25333

```

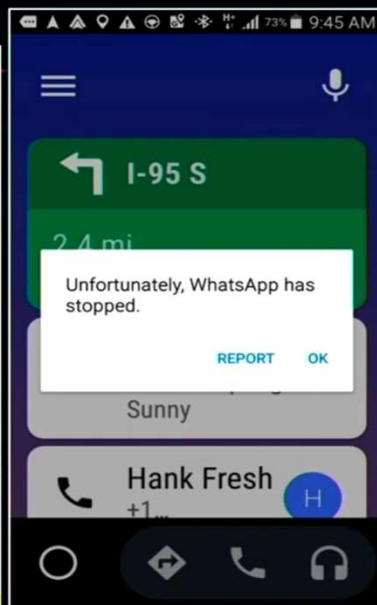
.....+1703...k...h..S
tupid assistant can't do much so i'm text
ing while driving.~T'...%.....A....[.
.....+17034...k...I'm
doing this hands-free...com.google.andro
id.googlequicksearchboxUS'...%.....%.
.....+17034%...k..2.
.k....Great...+14054720057..R(..%.....
.....+17034241981
.k.u...I left android auto to text yih d
ef distracted driving now...k.u..Q'...%.
.....E....Y.....+170342
...k.thy..I'm driving right now - hank
..com.google.android.projection.gearheadm
P'...%.....M%.....+
1703...k.tW[.k.t/..Did you read this
whole driving?+1405...bo(.....
F%
456 k N v

```


Distrait ou pas ?

- /com.google.android.googlequicksearchbox/app_session/00000034237932240452.binarypb

```
xt Hank. gearhead" h...W.h.i.c.h. .H.
a.n.k.?.....
a.....Q...fff?.w...Which
Hank?..There're two people with that
name: Hank Fresh or Hank Freshmen. Wh
ich one do you want to text?".en-USH.
H.z....J...w..hank fresh
.i.F.B.@933b06863f5233fba3e46d5d57dbb
c83e5a3be2e6fff0d9427bf1992d37f104f..
hank freshmen..G.B.@933b06863f5233fb
a3e46d5d57dbbc83e5a3be2e6fff0d9427bf1
992d37f104f.....
"...hank fresh..."hank freshmen..2.
en-US@.H.....R.X..x.P.Z.....
0.8.@.b.Which Hank?.....|.z...F.;Se
"&...+170...Mobile".+1703...
.....i.F.B.@933b06863f5233fba3e46d
5d57dbbc83e5a3be2e6fff0d9427bf1992d37
f104f.....
.....1..vnd.sec.contact.phone..vnd.se
c.contact.phone..2..1..vnd.sec.contac
t.phone..vnd.sec.contact.phone..3....
.com.whatsapp..WhatsApp..423..@933b06
863f5233fba3e46d5d57dbbc83e5a3be2e6ff
f0d9427bf1992d37f104f.....Hank Freshm
en..221"&...+1703...Mobile".+1
```



SMS Mes...	7/16/2019 1:29:34 PM(UTC+0)	To: +170...	I'm doing this hands-free.	mmssms.db-wal : 0xC
SMS Mes...	7/16/2019 1:34:37 PM(UTC+0)	To: +170...	Stupid assistant can't do much so i'm texting while driving	mmssms.db-wal : 0x8
SMS Mes...	7/16/2019 1:34:40 PM(UTC+0)	To: +170...	Stupid assistant can't do much so i'm texting while driving	mmssms.db-wal : 0xC
SMS Mes...	7/16/2019 1:35:37 PM(UTC+0)	To: +170...	👤	mmssms.db-wal : 0xC
Call Log	7/16/2019 1:41:44 PM(UTC+0)	To: +170...	00:00:26	logs.db : 0x475FD
SMS Mes...	7/16/2019 1:53:56 PM(UTC+0)	To: +170...	Are you sending this through WhatsApp?	mmssms.db-wal : 0xC
Instant...	7/16/2019 1:54:39 PM(UTC+0)	From: 15... To: 1703...	I set this up distracted while driving, but now I can text you...	msgstore.db-wal : 0xf com.whatsapp_prefer msgstore.db : 0xAF66 wa.db-wal : 0x25333

Created: 7/16/2019 1:45:23 PM(UTC+0)
Accessed: 7/16/2019 1:45:23 PM(UTC+0)
Modified: 7/16/2019 1:45:24 PM(UTC+0)

Parsons Corporation | Cellebrite

Références

<https://www.youtube.com/watch?v=IGhXsfZXL6g> (Android Auto / iOS carplay)

<https://thebinaryhick.blog/2019/05/08/ridin-with-apple-carplay/>

<https://dfir.pubpub.org/pub/716tlra7/release/2>



La parole est à vous !