SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
SUMMIT & TRAINING
SUMMIT: JUL 25 - 26 | TRAINING: JUL 27 - AUG 1
AUSTIN, TX

sans.org/dfirsummit

They See Us Rollin'; They Hatin': Forensics of iOS CarPlay and Android Auto

Brought to you by:
Sarah Edwards and
Heather Mahalik

About Us

Sarah Edwards

- Mobile Forensics Engineer, Parsons Corporation
- SANS Principal Instructor/Author
- Mac Nerd

Heather Mahalik

- Senior Director of Digital Intelligence, Cellebrite
- SANS Senior Instructor/Author
- Loves a great ’stache
- Mobile obsessed

Setup

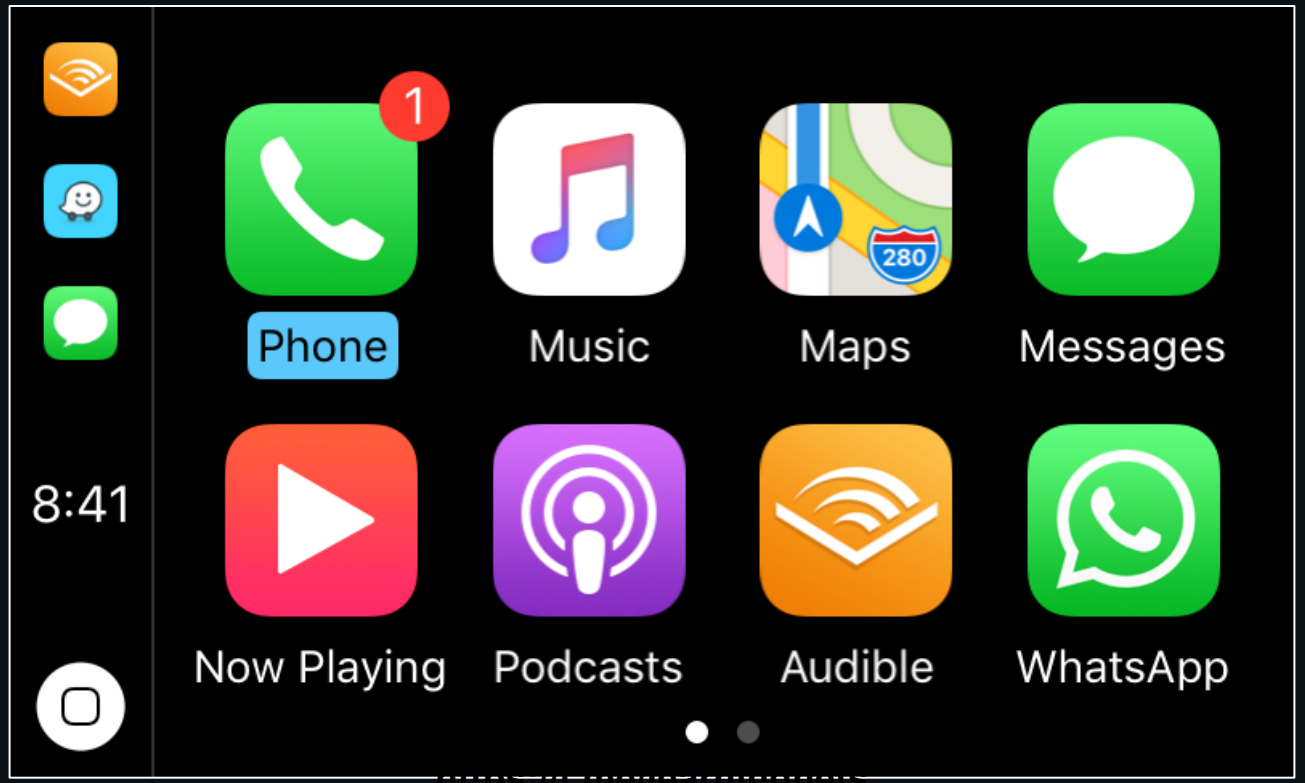
iOS and CarPlay

- Vehicle(s) Used
  - Audi S3
- iPhone Details
  - iPhone X, 12.1.1 (Jailbroken)

Android and Android Auto

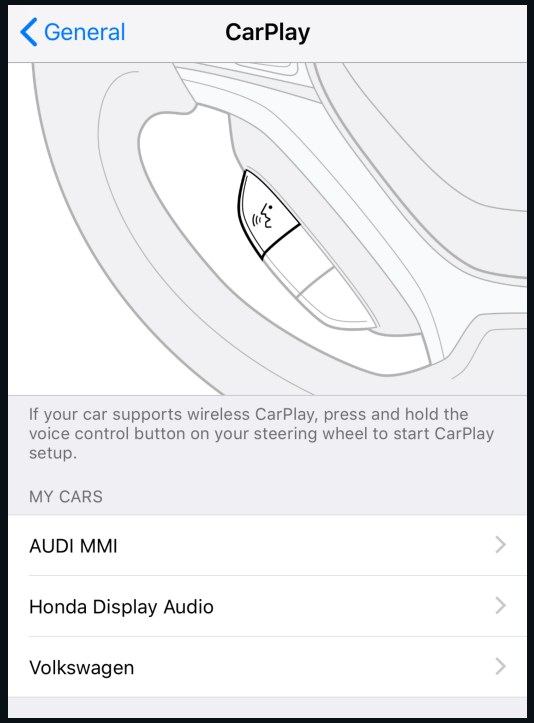
- Vehicles Used:
  - GMC Yukon Denali
  - Nissan Sentra (Rental)
- Androids Used:
  - Rooted Samsung – Full Physical
  - Samsung J7 Prime – Exynos – File System

CarPlay Interface



CarPlay Configuration

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

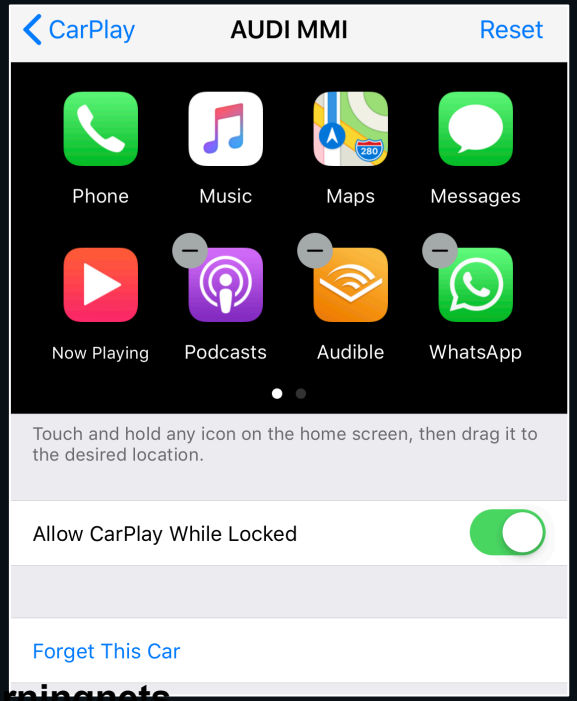


▼ Root	Dictionary	(2 items)
▼ AppBlacklist	Array	(2 items)
Item 0	String	com.apple.carplay.blacklisted
Item 1	String	com.apple.carplay.blacklisted-nav
▼ pairings	Dictionary	(3 items)
▼ C2BF6EB1-751D-4C82-864C-BD845ABC1619	Dictionary	(2 items)
name	String	Volkswagen
▼ carPlayProtocols	Array	(1 item)
Item 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

Per Car App Icon Configuration

- /mobile/Library/Springboard/<GUID>-CarDisplay[Desired]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)



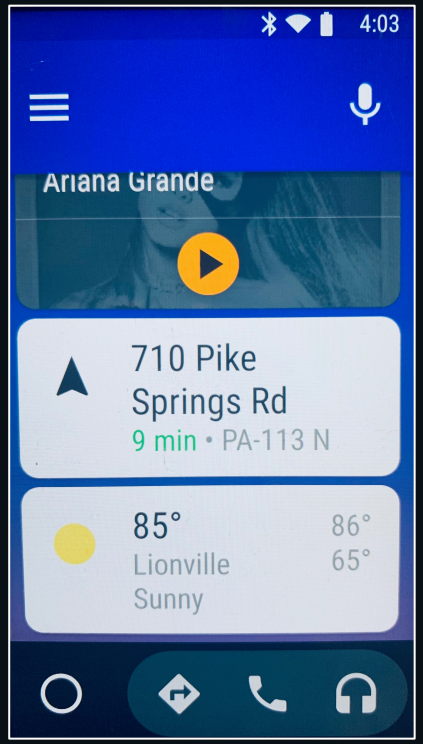
Device Connections (knowledgeC.db)

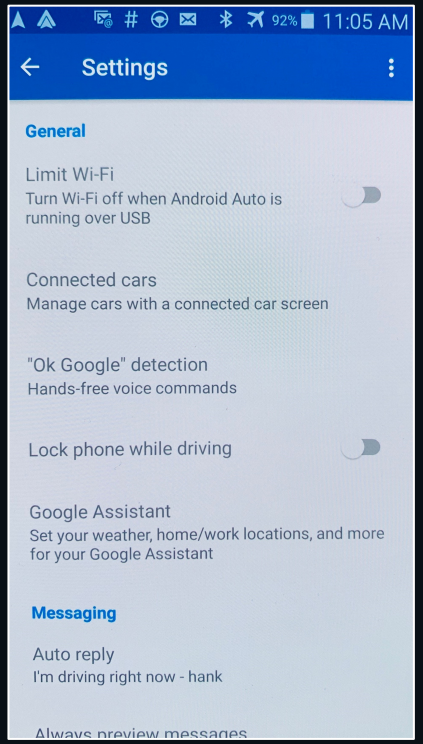
	Local Time	Activity	Output
1	2019-07-18 06:46:24	Device Plug In Status	[IS PLUGGED IN: UNPLUGGED] [USAGE IN SECONDS: 8328] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 20
2	2019-07-18 09:05:12	Device Plug In Status	[IS PLUGGED IN: PLUGGED IN] [USAGE IN SECONDS: 316] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START: 2019
3	2019-07-18 09:07:12	CarPlay Connected	[CARPLAY CONNECTED: CONNECTED] [USAGE IN SECONDS: 4] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START
4	2019-07-18 09:10:27	CarPlay Connected	[CARPLAY CONNECTED: DISCONNECTED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [ST
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-
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: 201
7	2019-07-18 09:10:33	CarPlay Connected	[CARPLAY CONNECTED: CONNECTED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START
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: 2
9	2019-07-18 09:35:10	CarPlay Connected	[CARPLAY CONNECTED: DISCONNECTED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [ST
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
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: 2
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: 201
13	2019-07-18 17:54:13	CarPlay Connected	[CARPLAY CONNECTED: CONNECTED] [USAGE IN SECONDS: 0] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [START
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: 201
15	2019-07-18 18:27:50	CarPlay Connected	[CARPLAY CONNECTED: DISCONNECTED] [USAGE IN SECONDS: 4] [DAY OF WEEK: Thursday] [GMT OFFSET: -4] [ST

Android Auto Car Configuration

- 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

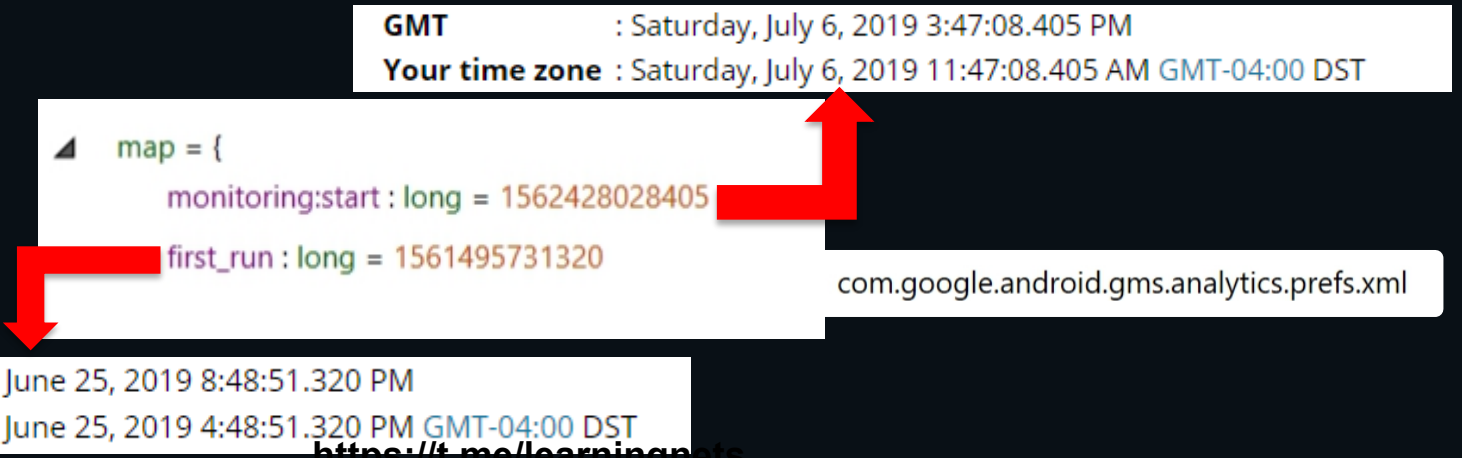
```
map = {
    key_settings_autolaunch_enable : boolean = True
    bt_autolaunch/GMC+IntelliLink/9C:8D:7C:18:8A:F8 : boolean = True
```





Android Auto Connections (1)

- Car Connections – Everywhere!
  - Data Usage
  - Syncing Artifacts
  - Bluetooth/USB Connections



Android Auto Connections (2)

- 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.
15	goodbyefelicia11@gmail.com	2019-06-25 20:24:03	CP2 sync start x2

Android Auto Connections (3)

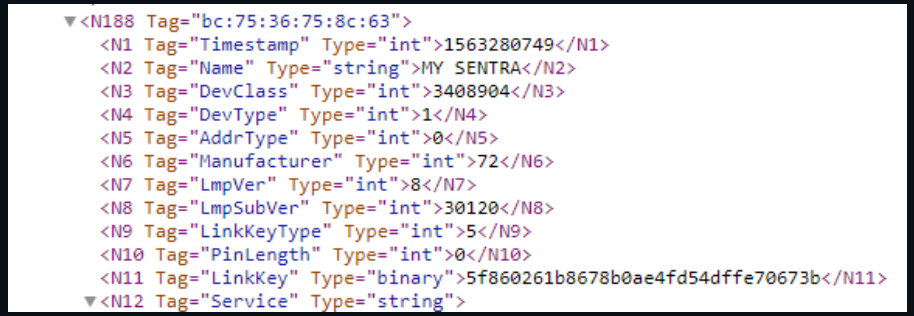
- Bluetooth/USB - /system/powerManager
- Bluetooth - /com.android.settings/databases/search_index.db

```
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

Which Car Was It?

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



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

Messages (1) – 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 1
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 1
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 1
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 1
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

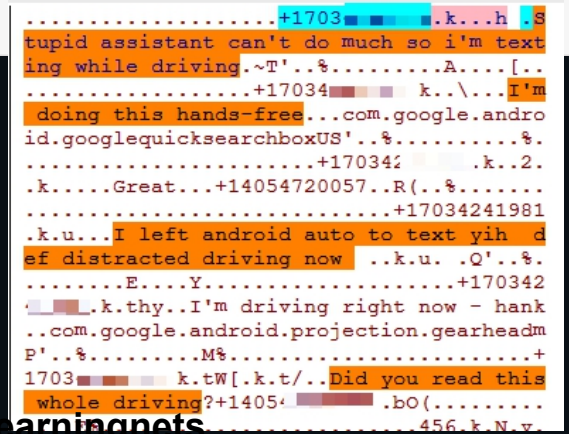
Messages (2) – KnowledgeC.db, InteractionsC.db, sms.db

	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] [ZRECIPIENTCO
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.

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 : 0x com.whatsapp_prefer msgstore.db : 0xAF66 wa.db-wal : 0x25333



App Usage in Vehicle?

- knowledgeC.db & cache_encryptedC.db

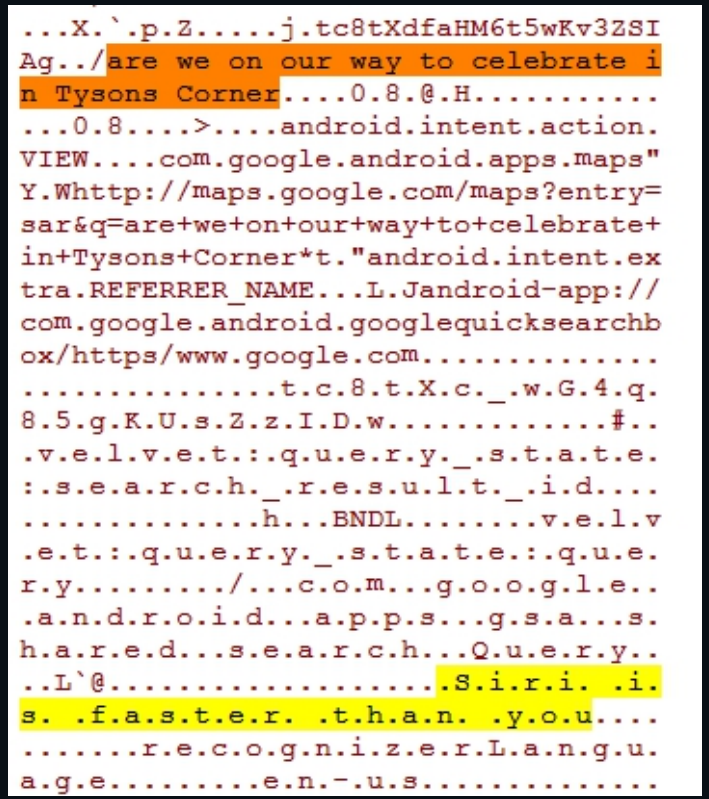
2019-07-18 18:17:07	Motion	[START TIME: 2019-07-18 22:17:07] [TIMESTAMP: 119538.986257] [TYPE: 4096] [CONFIDENCE: 3] [MOUNTED: 1] [MOUNTED CONFIDENCE: 2] [TURN: 0] [IS VEHICULAR: 1] [IS MOVING: 1] [VEHICL
2019-07-18 18:18:14	Application In Focus	[BUNDLE ID: com.apple.podcasts] [USAGE IN SECONDS: 1] [DAY 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 2
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: 2019-0
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: 2019-07-1
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

Distracted Driving?
Location DBs & knowledgeC.db

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 ACC
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 ACC
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 ACCU
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 ACCU
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
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: 20
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-

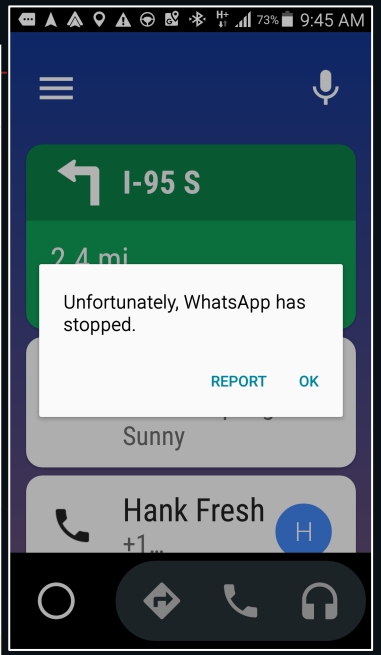
Android Auto Voice Directions

- Directions
  - /data/com.google.android.apps.maps/app_tts-cache/849148683_1561591091581



Android Auto Distracted Driving?

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



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 : 0x 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)

Shout Out

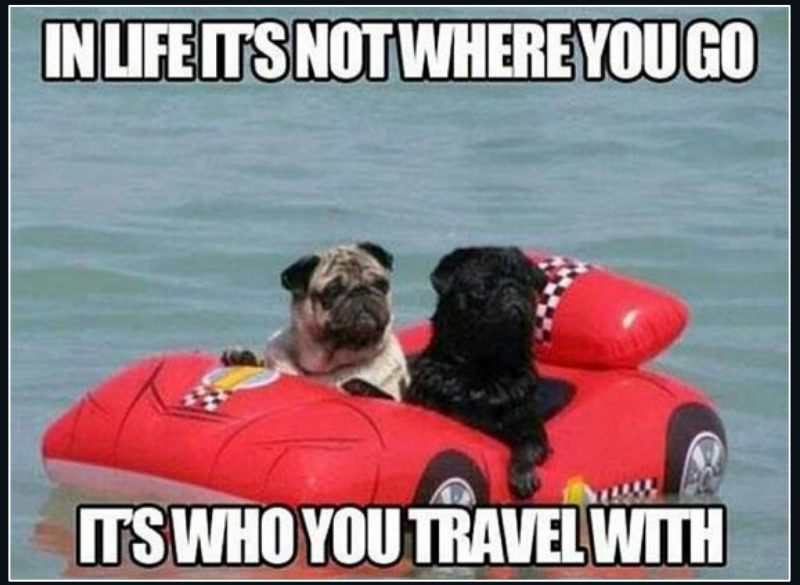
- Josh Hickman
  - https://thebinaryhick.blog/2019/05/08/ridin-with-apple-carplay/
  - https://dfir.pubpub.org/pub/716tlra7

What Next?

- More Research
  - Overall timeline for Android Auto
  - Blog about artifacts
- APOLLO
  - Maybe some Android modules!

Like This?

- Research Addicts – Keep your eye out for more talks and blogs
  - smartforensics.com
  - mac4n6.com
- FOR518 and FOR585 – Yep – We teach for SANS
- Webcasts



THANK YOU FOR ATTENDING

Questions?

@iamevltwin | mac4n6.com

@heathermahalik | smarterforensics.com

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE
SUMMIT & TRAINING

AUSTIN, TX

SUMMIT: JUL 25-26 TRAINING: JUL 27 – AUG 1

www.sans.org/dfirsummit