DFIR Review

Ka-Chow!!! Driving Android Auto

Joshua Hickman

Published on: Apr 03, 2019

DOI: 10.21428/482a8d7a

License: [Creative Commons Attribution 4.0 International License \(CC-BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

Synopsis

Forensic question: What information is recoverable from an Android device that is connected to a vehicle with using the Android Auto app?
OS Version: Android 8.1 (Oreo) Files: Event Trace Logs (ETL)	Android Auto v3.8.584564 - Installed 01/16/2019 13:15 (EST) Google v8.91.5.21 - Installed 01/16/2019 13:10 (EST) Maps v10.7.1 - Installed 01/16/2019 13:01 (EST)
Tools: WinHex, Version 19.7 (Specialist License) Cellebrite UFED 4PC, Version 7.12.1.100 DCode, Version 4.02a	

Introduction

Recently I purchased a new car. I am talking brand spankin' new. I had been looking for a compact SUV for a while because of a growing family, and I found it: a 2019 Nissan Rogue. I purchased it in 2018, so this would make the car, like, *really* new. I was super excited as this was the first time I had ever purchased a new car.

While signing the novel-sized stack of paperwork that is part of any car purchase, the woman I was working with and I were chatting about all the bells and whistles that were in my newly purchased ride, and she mentioned that she had a term for newer cars: laptops on wheels. She was absolutely correct. My car keeps track of all sorts of things: gas mileage, proximity to objects, tire pressure, what I'm listening to on the radio, external temperature, and other things I probably don't know about. The on-board electronics are crazy compared to my first car (a 1985 Chevy S-10 pickup). Additionally, my new car supports Apple's CarPlay and Google's Android Auto, the two automotive interfaces developed for the two major mobile software platforms

While I have been using CarPlay for some time now, I have never used Android Auto. I was aware of its existence, but that was about it. When I bought the car, I was in the middle of creating a clean Android image for the DFIR community, so I thought it would be great to have this in the image since phone-to-car interfaces will become more and more common. Currently, there are 29 different auto manufacturers that have various models which support Android Auto, and the list continues to grow. Additionally, there are after-market radio manufacturers (e.g. Pioneer, Kenwood, etc.) that are baking Android Auto in to their units, so I feel that this will become more common place as time goes on.

Method

After using Android Auto for just over a week, I created my Android image, and immediately starting poking around to see what I could find. Surprisingly, there is not much in the way of Android Auto itself; it projects certain Android apps on to your car's in-dash receiver which allows you to interact with those apps. My car has a mic (in the roof) that also worked with Android Auto and allows for voice commands/inquiries to Google Assistant without picking up the phone. Now, Android Auto does have the ability to be used on-device, but, for the purposes here, I concentrated on the in-dash flavor.

The data for Android Auto itself is accessible via an Android backup or a file system extraction. However, the good stuff, as is typical with Android, was sitting in the **/data** area, which, as we all know, is not easily accessible these days. Thus, this disclosure: the phone I was using was rooted using TWRP and Magisk.

The tests were conducted using a Nexus 5X (Model H790, Bluetooth 64:BC:0C:F5:D1:C9) running Android 8.1 with a patch level date of December 5, 2018. The image file that contains the data discussed in this article can be downloaded [here](#).

Setup

As I previously mentioned, this research involved the use of my new car. The first thing to do was to download the app itself. Android Auto does not come as a default application with the image I downloaded (bullhead OPM 7), and I am not sure if Android OEMs install it as part of their skinning process. I checked with some co-

workers who have Android devices, and Android Auto was not on their devices; those guys have Samsungs, and I do not know anyone who has anything else.

The setup process was slightly different than what I was used to with CarPlay. With CarPlay it is a matter of plugging in my iPhone and driving off. The phone and the car recognize each other, and I did not have to do anything beyond organizing the apps on the screen (like I do on my phone). Android Auto is slightly different. When I plugged the phone in to the car it immediately started Android Auto. From there, it was like any typical Android app that is started for the first time: the app permissions dance.

Android Auto requested the following:

- Calendar
- Contacts
- Location
- Microphone
- Phone
- SMS

Additionally, I had to pair it to my car via Bluetooth. Again, this is not something that I had to do with CarPlay. I took the defaults on everything, agreed to the terms of service, and proceeded onward.

External Inspection

The home screen is straight forward. See Figure 1.

Figure 1

The home screen displays various information via cards. In Figure 1 you can see stuff that may be relevant to me. Here you can see the weather and a frequent location. If you scroll down, you can see new text messages that have not yet be read (pictured in Figure 2).

Figure 2

The icons at the bottom of the screen correspond to the different applications that are available through Android Auto. From left to right: Maps (Figure 3), Telephone (Figure 4), the Android home button, various applications that can use Android Auto (Figures 5 and 6), and an exit mechanism to return to my radio's native interface (Figure 7).

Figure 3

Figure 4

Figure 5

Figure 6

Figure 7

Although not visible from the interface, Google Assistant is available. My particular vehicle has a button on the steering wheel that is able to summon Google Assistant without using the hot word (Ok, Google). I did not test the ability to summon Google Assistant by leveraging the hot word.

Internal Examination

For just over a week, I drove around with Android Auto. I got directions, had it read messages to me (that I sent myself – no one has the number assigned to the test device), and played podcasts. After generating the data, I performed a physical extraction, and loaded it in to WinHex to see if I could find any data left behind by Android Auto that would indicate how the application was used.

Navigating to the `/data/data` directory finds the Android Auto folder. It is listed as **com.google.android.projection.gearhead** (Figure 8).

com.google.android.printservice.recommendation	recommendation
com.google.android.projection.gearhead	gearhead
com.google.android.setupwizard	setupwizard
com.google.android.storagemanager	storagemanager

Figure 8

Inside the folder was a typical layout for an Android application (Figure 9).

.	= com.google.android.projection.gearhead
app_impl	
cache	
code_cache	
databases	
files	
shared_prefs	

Figure 9

The **app_impl** folder contained .apk files that appeared to be relevant to the operating of the application. The **cache** folder acts as a “scratchpad” of sorts where the applications that can use Android Auto can deposit assets as needed. In my case, there was album art from the podcasts that I listened to along with picture files that were used to display the weather conditions that were displayed. These files had a .0 file extension.

The **code_cache** folder was empty.

The **databases** folder contained four files. The first was *CloudCards.db*, which contained only one table. The table contained one entry that had a URL that referred to a .png file of what was supposed to be a sun for the weather card that was displayed on the home screen. This file had a corresponding journal file that was empty.

The second file in this folder was the *google_analytics_v4 6308.db* file. This file has one table that contains any data: properties. The table contains the Google Analytics Client ID (explained below), the Tracking ID (*tid* - described as an ID that distinguishes to which Google Analytics property to send data), and information about the app version. As with the *CloudCards.db* file, this file also has a corresponding journal file that is empty.

The **files** folder contained two files. The first is *gaClientId*, which is the Google Analytics Client ID. The Client ID is a randomly generated UUID (version 4) that is

used to anonymously identify a particular user or device.

There was a file named *phenotype.lock*, but the file had no contents.

The **shared_prefs** folder is where the interesting information resides. See Figure 10 for a file listing.

File Name	File Type
app_state_shared_preferences.xml	xml
auto_launch_prompt.xml	xml
AvailableAppCache.xml	xml
AvailableAppCache.xml.bak	bak
bluetooth_capabilities_prefs.xml	xml
bluetooth_metadata.xml	xml
com.google.android.gms.analytics.prefs.xml	xml
com.google.android.gms.analytics.prefs.xml.bak	bak
com.google.android.projection.gearhead_preferences.xml	xml
common_user_settings.xml	xml
common_user_settings_shadow_common.xml	xml
common_user_settings_shadow_projection.xml	xml
default_app.xml	xml
gearhead_config.xml	xml
GH.RatingPromptManager.xml	xml
location_manager.xml	xml
NotificationListenerComponentNameManager.Preferences.xml	xml
passenger_mode_shared_preferences.xml	xml

Figure 10

The first file, *app_state_shared_preferences.xml*, contains the time Android Auto was last run stored in Unix Epoch Time with the tag “pref_lastrun.” See Figure 11.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <map>
  <boolean value="true" name="pref_projected_activation"/>
  <long value="1548616472427" name="pref_lastrun"/>
  <boolean value="true" name="pref_assistant_promo_seenPROJECTED"/>
  <boolean value="true" name="pref_android_auto_activation"/>
</map>
```

Figure 11

The next file of interest is the *common_user_settings.xml*. This file contained the Bluetooth MAC address for my car. The file here had one entry. I did not have access to a second car that could run Android Auto, so I do not know if this file could contain multiple listings. See Figure 12.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <map>
  - <set name="AndroidAutoBluetooth">
    <string>B4:EC:02:73:FF:93</string>
  </set>
</map>
```

Figure 12

The last file in this folder is *location_manager.xml*. See Figure 13.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <map>
  <string name="car_name">Nissan</string>
  <string name="latitude">34.99277</string>
  <string name="delay_ms">971</string>
  <string name="accuracy">3.0</string>
  <string name="time">1548620033971</string>
  <string name="speed">0.0</string>
  <string name="longitude">-78.13563</string>
</map>
```

Figure 13

This file contains some interesting data. For starters, it has the name of my car, “Nissan.” The latitude and longitude geolocates to the location where I was when I last disconnected the test device from the car, and the time was the time I disconnected (in Unix Epoch Time). As far as the value in the accuracy tag, I can only hypothesize; however, I can tell you the latitude and longitude are extremely close to where I was located when I disconnected the test device (I would estimate within three meters of where my car was located when I disconnected).

Other Data

My usage of Android Auto was limited to getting directions, reading messages, and playing podcasts, so I expected to find some references or artifacts to these activities. My examination revealed none of that. My next step was to examine the applications that actually did the work: Google and Maps.

The main method by which I interacted with Android Auto was via voice commands, which is handled by Google Assistant. For the purposes of this paper I will not deep-dive in to Google Assistant; I have [posted additional research](#) in that area that utilized some of the data here. However, I do want to highlight how Android Auto and Google interact in order to facilitate hands-free use while driving.

The Google app resides in the **/data/data** directory. The folder is **com.google.android.googlequicksearchbox**. See Figure 14.

com.google.android.GoogleCamera	GoogleCamera
com.google.android.googlequicksearchbox	googlequicksearchbox
com.google.android.gsf	gsf

Figure 14

The folder has the usual suspect folders along with several others. See Figure 15 for the folder listings.

. = data	
. = com.google.android.googlequicksearchbox	googlequicksearchbox
app_dictation	
app_download_internal	
app_g3_models	
app_monet_init_data	
app_prediction	
app_session	
app_shared_prefs	
app_si	
app_sid	
app_textures	
app_vactions	
app_webview	
cache	
code_cache	
databases	
files	
no_backup	
shared_prefs	

Figure 15

The folder of interest here is **app_session**. This folder has a great deal of data that is relevant to my usage of Android Auto. It could also house data that is relevant to any number of ways which a user interacts with their device by the use of their voice. The folder contains several .binarypb files. See Figure 16.

com.google.android.googlequicksearchbox	googlequicksearchbox
app_session	
00000000290354543320.binarypb	binarypb
00000000359074311786.binarypb	binarypb
00000000359074312067.binarypb	binarypb
00000000359074312800.binarypb	binarypb
000000001321156222687.binarypb	binarypb
000000001664754413099.binarypb	binarypb
000000001664754413128.binarypb	binarypb

Figure 16

Each .binarypb file here represents a “session,” which I will define as each time Google Assistant was invoked. I will focus on the files that were generated by use of Android Auto; some of the files were generated as a result of a different manner of invocation for other purposes. Based on my notes, I know when I summoned Google Assistant and what I did when I summoned it. By comparing my notes to the MAC times associated with each .binarypb file I identified the applicable files. The first time I summoned Google Assistant is represented in the file with the last five digits of 43320.binarypb. Figure 17 shows the header of the file.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0	09	D8	BA	7A	9A	43	00	00	00	15	59	51	EF	11	1A	0D	ø°zšC YQi
16	63	61	72	5F	61	73	73	69	73	74	61	6E	74	DA	B5	BB	car assistantÙ»
32	F8	03	00	8A	84	C6	F8	03	16	0A	04	00	00	00	00	15	ø Š„Æø
48	00	00	00	00	18	00	21	3A	5B	21	00	00	00	00	00	E2	!:[! â
64	D4	C8	F8	03	D8	52	0A	E0	48	FF	F3	44	C4	00	10	F9	ÔÈø ØR àHÿóDÄ ù
80	62	18	00	D0	44	94	17	FE	79	2B	05	8B	96	A9	62	BA	b ËD” py+ <-@b°
96	4D	95	E2	90	B9	12	0A	F2	FA	98	B5	95	CD	FC	90	F8	M•â ’ òúñ•íü ø
112	D8	26	FC	A7	E4	66	3A	51	90	28	B3	A6	79	15	F3	FF	Ø&úŠäf:Q (’!y óÿ
128	AB	84	10	72	0E	39	0B	18	3E	51	C9	AB	FF	D0	95	BE	«„ r 9 >QÉ«ÿÐ•¼
144	11	3E	A7	79	F2	85	DF	F7	7F	26	1F	23	18	D8	0B	1A	>Šÿò...ß÷ & # Ø

Figure 17

The ASCII “car_assistant” seems to imply this request had been passed to Google Assistant from Android Auto. In each test that I ran, this phrase appeared at the beginning of the file. Additionally, the string in the smaller orange box (0x5951EF)

accompanied the phrase at the same byte offset each time. I hesitate to call this a true “file header,” though. I think someone with more time in DFIR should make that call.

The data in the red boxes, though, caught my attention.

Here is a fun fact about me: one of the jobs I held in college was that of a disc jockey. During this time, digital audio workstations were really coming in to their own, so I sat in front of Pro Tools quite a bit; I saw *a lot* of audio files in hex/ASCII. I continued to use Pro Tools extensively through the mp3 craze of the late 90’s and early 2000’s and had worked with mp3 files quite a bit. While it had been some time, my eyeballs immediately saw the “yoda” string. It also helps that I am a Star Wars fan.

The “yoda” string (0xFFF344C4) is a frame sync header for mp3 files. I will not go in to detail, but just know that this string tipped me off that something else, not expected, may be in this file. I decided to scroll to the end of the gobbly-goo to see what I could find. Needless to say, I was surprised. See Figure 18.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
9040	98	C2	C6	24	B9	82	30	20	80	85	25	E4	4C	75	A8	CD	Ä&²,0 €...äLu"í
9056	DE	C8	3E	43	19	9A	A7	B0	39	58	E6	59	1A	86	0A	08	È>C šš°9XæY †
9072	10	74	0F	1A	7C	D0	A8	A8	A0	B3	54	DE	AE	0B	0B	0A	t Ð"" 'TÐ
9088	88	DD	F1	5F	14	6F	F1	7E	CC	FF	F3	44	C4	EA	15	A9	ˆÝñ_oñ~ÿóDÄê ©
9104	5A	40	00	E0	C6	94	0A	15	14	16	68	B0	B3	3F	FD	5A	Z@_àÆ" h°?ýZ
9120	85	95	4C	41	4D	45	33	2E	39	39	2E	35	55	55	55	55	•LAME3.99.5UUUU
9136	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9152	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9168	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9184	55	55	55	55	55	55	55	55	55	FF	F3	44	C4	E6	13	20	UUUUUUUUUUÿóDÄê
9200	EA	2C	00	C0	C6	70	55	55	55	55	55	55	55	55	55	55	ê, ÄÆpUUUUUUUUUUUU
9216	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9232	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9248	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9264	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9280	55	55	55	55	55	55	55	55	55	FF	F3	44	C4	EC	14	50	UUUUUUUUUUÿóDÄi P
9296	9D	64	00	D6	06	4C	55	55	55	55	55	55	55	55	55	55	d Ö LUUUUUUUUUUUUU
9312	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9328	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9344	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9360	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
9376	55	55	55	55	55	55	55	55	55	11	40	00	00	00	00	00	UUUUUUUUUU @
9392	00	00	1A	93	09	0A	84	09	01	44	60	40	80	04	02	00	" „ D`@€
9408	00	00	00	00	00	00	00	00	01	00	00	00	00	00	00	00	
9424	00	00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYY
9440	FF	FF	FF	FF	FE	FF	FF	FF	FE	FF	FF	FF	00	00	00	00	YYYYpYYYYpYYY
9456	00	00	00	00	FF	FF	FF	FF	72	3D	DC	57	68	41	16	01	YYYYr=ÜWhA
9472	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	D4	00	00	00	YYYYYYYYYYYYYô
9488	42	4E	44	4C	02	00	00	00	17	00	00	00	61	00	70	00	BNDL a p

Figure 18

The orange box is important. In it is “LAME3.99.5.” LAME is a free, open-source mp3 encoder (codec). This particular version, 3.99.5, was released in February of 2012. The additional yoda strings along with the 0x55 values in between is what happens when mp3 frames need to be padded (i.e. filled in order to round out a frame to fit the bit rate at which the audio is captured). Each mp3 encoder handles padding differently, but the repetitive data in between yodas was indicative. All of this further heightened my suspicion that what I was looking at was mp3 data.

So, I carved from the first yoda (seen in Figure 17), to the last (seen in Figure 18), for a total of 11.1 KB. I then saved the file with no extension and opened it in VLC Player. The following came out of the speakers:

“You’ve got a few choices. Pick the one you want.”

Based on my notes, this was the last phrase Google Assistant spoke to me prior to handing me off to Maps. In this session, I had asked for directions to Starbucks and had not been specific about which one, which caused the returned reply that I had just heard.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
01	00	00	00	20	00	00	00	20	00	00	00	22	0F	3A	03	" :
77	65	62	6A	08	67	65	61	72	68	65	61	64	2A	0D	63	webj gearhead* c ar_assistant gearhead"TYYYYYY YYYYYY
61	72	5F	61	73	73	69	73	74	61	6E	74	12	00	1A	08	
67	65	61	72	68	65	61	64	22	54	FF	FF	FF	FF	FF	FF	
FF	FF	FF	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	
00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00
00	00	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	00	00	00	YYYYYYYY
00	00	00	00	00	00	00	00	00	00	00	00	00	00	BA	F1	°ñ
C8	F8	03	BB	31	0A	89	0B	0A	DC	0A	01	4C	60	40	80	Eø »1 % Ü L'@€
04	02	00	00	00	00	00	00	00	00	00	00	00	00	00	1E	
00	00	00	49	00	20	00	6E	00	65	00	65	00	64	00	20	I need
00	64	00	69	00	72	00	65	00	63	00	74	00	69	00	6F	directions
00	6E	00	73	00	20	00	74	00	6F	00	20	00	53	00	74	to Starbucks
00	61	00	72	00	62	00	75	00	63	00	6B	00	73	00	00	recognizer
00	00	00	12	00	00	00	12	00	00	00	72	00	65	00	63	language
00	6F	00	67	00	6E	00	69	00	7A	00	65	00	72	00	4C	en-us
00	61	00	6E	00	67	00	75	00	61	00	67	00	65	00	00	" I need the directions to Starbucks s YYYYYYYYp YYYpYYY Y YYYr=ÜWhA YYYYY YYYYYYYÔ BNDL
00	00	00	05	00	00	00	65	00	6E	00	2D	00	75	00	73	
00	00	00	00	00	00	00	1E	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	01	00	00	00	22	00	00	00	49	
00	20	00	6E	00	65	00	65	00	64	00	20	00	74	00	68	
00	65	00	20	00	64	00	69	00	72	00	65	00	63	00	74	s YYYYYYYYp YYYpYYY Y YYYr=ÜWhA YYYYY YYYYYYYÔ BNDL
00	69	00	6F	00	6E	00	73	00	20	00	74	00	6F	00	20	
00	53	00	74	00	61	00	72	00	62	00	75	00	63	00	6B	
00	73	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FE	
FF	FF	FF	FE	FF	FF	FF	00	00	00	00	00	00	00	00	FF	
FF	FF	FF	72	3D	DC	57	68	41	16	01	FF	FF	FF	FF	FF	YYYr=ÜWhA YYYYY
FF	FF	FF	FF	FF	FF	FF	D4	00	00	00	42	4E	44	4C	02	YYYYYYYÔ BNDL

Figure 19

Scrolling further in to the file I found the area shown in Figure 19. The purple box with the arrow next to it was my actual voice inquiry via Android Auto, and the orange box contains the "car_assistant" string. The strings in the blue and green boxes were interesting as I had seen them elsewhere while examining other data in this folder.

Also, there is a second phrase there (bottom purple box) that is a variation of what is in the first purple box. Interesting...

The following morning, I headed to Starbucks again. This time I was a little more specific about which one I wanted. I invoked Google Assistant, asked for directions, and navigated to the location. This session is represented *12067.binarypb* file. See Figure 20.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0	09	83	2F	7F	9A	53	00	00	00	15	59	51	EF	11	1A	0D	f/ ŠS YÖi
16	63	61	72	5F	61	73	73	69	73	74	61	6E	74	DA	B5	BB	car_assistantju»
32	F8	03	00	8A	84	C6	F8	03	F3	01	0A	E0	01	D8	00	00	ø S„Æø ó à Ø
48	00	42	4E	44	4C	01	00	00	00	2F	00	00	00	63	00	6F	BNDL / c o
64	00	6D	00	2E	00	67	00	6F	00	6F	00	67	00	6C	00	65	m . g o o g l e
80	00	2E	00	61	00	6E	00	64	00	72	00	6F	00	69	00	64	. a n d r o i d
96	00	2E	00	61	00	70	00	70	00	73	00	2E	00	67	00	73	. a p p s . g s
112	00	61	00	2E	00	73	00	65	00	61	00	72	00	63	00	68	a . s e a r c h
128	00	2E	00	63	00	6F	00	72	00	65	00	2E	00	61	00	6C	. c o r e . a l
144	00	2E	00	61	00	2E	00	61	00	75	00	00	00	03	00	00	. a . a u
160	00	64	00	00	00	42	4E	44	4C	01	00	00	00	29	00	00	d BNDL)
176	00	49	00	43	00	49	00	4E	00	47	00	5F	00	43	00	4F	I C I N G _ C O
192	00	4E	00	4E	00	45	00	43	00	54	00	49	00	4F	00	4E	N N E C T I O N
208	00	5F	00	49	00	4E	00	49	00	54	00	49	00	41	00	4C	_ I N I T I A L
224	00	49	00	5A	00	41	00	54	00	49	00	4F	00	4E	00	5F	I Z A T I O N _
240	00	54	00	49	00	4D	00	45	00	5F	00	4D	00	53	00	45	T I M E _ M S E
256	00	43	00	00	00	01	00	00	00	42	00	00	00	15	00	00	C _ B
272	00	00	18	00	21	5B	4B	AA	00	00	00	00	00	E2	D4	C8	! [Kª ÁÔÈ
288	F8	03	F9	8D	01	0A	80	84	01	FF	F3	44	C4	00	12	00	ø ù €„ YóDÄ
304	05	CC	01	41	18	00	00	20	08	06	30	7C	1F	3F	50	21	ì A 0 ?P!
320	FF	FF	FF	FF	4F	48	21	A8	13	0F	D6	0F	82	00	80	40	ÿÿÿÿOH!~ Ö , €@
336	10	04	C1	F0	7C	1F	07	C1	00	40	10	04	01	30	7C	1F	Áš Á @ 0
352	07	C1	F0	40	10	04	01	00	4C	1F	07	C1	F0	7C	10	04	Áš@ L Áš
368	01	00	40	13	07	C1	F0	7C	1F	04	01	00	40	10	C4	B3	@ Áš @ Ä³

Figure 20

The same “car_assistant” phrase was there, along with the 0x5951EF string. There is also another yoda. Time to scroll...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
16832	A1	96	4D	41	03	63	4C	B8	48	7D	00	47	90	07	19	16	;-MA cL,H} G
16848	2E	10	34	F3	22	C2	A9	53	44	41	BE	69	E2	B8	0C	32	. 4ó"Â@SDA%ia, 2
16864	E4	38	48	D0	E4	54	56	E4	DB	BF	6F	CD	3F	FC	5B	55	ã8HðãTVãÛ¿oÍ?ü[U
16880	97	6E	29	44	42	58	6C	50	2E	19	22	2E	DB	32	D9	38	-n)DBXlP. ".Û2Û8
16896	F4	40	42	93	44	91	27	8A	01	FF	F3	44	C4	FF	28	BB	ô@B"D'Š ŸóDÃŸ(>
16912	19	A4	00	7A	4C	BD	48	84	9E	15	04	89	3C	B1	20	A8	¤ zL¤H,,ž %<± "
16928	08	95	44	82	AE	09	01	48	F0	90	14	81	E7	61	20	29	•D,® Hð ça)
16944	13	B0	AB	96	02	11	12	0A	8C	C0	44	99	FC	58	0A	8D	°«- ÈAD™UX
16960	2D	09	01	74	77	51	D8	31	0C	E1	25	4C	41	4D	45	33	- twQØ1 á%LAME3
16976	2E	39	39	2E	35	55	55	55	55	55	55	55	55	55	55	55	99.5UUUUUUUUUUUU
16992	55	55	55	55	55	55	55	55	55	FF	F3	44	C4	AF	11	78	UUUUUUUUUUyóDÃ x
17008	81	FC	00	60	C6	48	55	55	55	55	55	55	55	55	55	55	ü `EHUUUUUUUUUUUU
17024	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
17040	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
17056	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
17072	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
17088	55	55	55	55	55	55	55	55	55	FF	F3	44	C4	BC	12	A0	UUUUUUUUUUyóDÃ
17104	59	D0	00	4A	4C	24	55	55	55	55	55	55	55	55	55	55	Yð JLSUUUUUUUUUUUU
17120	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
17136	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
17152	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
17168	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUUUU
17184	55	55	55	55	55	55	55	55	55	11	44	00	00	00	00	00	UUUUUUUUU D
17200	00	00	1A	93	09	0A	84	09	01	44	60	40	80	04	02	00	" „ D`@€
17216	00	00	00	00	00	00	00	00	01	00	00	00	00	00	00	00	
17232	00	00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYYY
17248	FF	FF	FF	FF	FE	FF	FF	FF	FE	FF	FF	FF	00	00	00	00	YYYYpYYYYpYYYY
17264	00	00	00	00	FF	FF	FF	FF	6E	47	4D	58	68	35	AD	00	yyyynGMXh5-
17280	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	D4	00	00	00	YYYYYYYYYYYYYô
17296	42	4E	44	4C	02	00	00	00	17	00	00	00	61	00	70	00	BNDL a p

Figure 21

There is the LAME codec reference, the padding, and the final yoda in Figure 21. As before, I carved, saved, and played in VLC Player. I heard the following:

"Starbucks is ten minutes from your location by car and light traffic."

Based on my notes, this was, again, the last thing I heard prior to Maps initializing and taking over. I continued to scroll through the file to see if I could find the voice request I had originally given Google Assistant. See Figure 22.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
18320	01	00	00	00	20	00	00	00	20	00	00	00	22	0F	3A	03	" :
18336	77	65	62	6A	08	67	65	61	72	68	65	61	64	2A	0D	63	webj gearhead* c
18352	61	72	5F	61	73	73	69	73	74	61	6E	74	12	00	1A	08	ar_assistant
18368	67	65	61	72	68	65	61	64	22	54	FF	FF	FF	FF	FF	FF	gearhead"Tytytyty
18384	FF	FF	FF	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	tytytyty
18400	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00	
18416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	
18432	00	00	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	00	00	00	tytytytyty
18448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	BA	F1	°ñ
18464	C8	F8	03	86	30	0A	C3	0E	0A	80	0E	01	4C	60	40	80	Èø t0 Å € L`@€
18480	04	02	00	00	00	00	00	00	00	00	00	00	00	00	00	34	4
18496	00	00	00	67	00	69	00	76	00	65	00	20	00	6D	00	65	g i v e m e
18512	00	20	00	64	00	69	00	72	00	65	00	63	00	74	00	69	d i r e c t i
18528	00	6F	00	6E	00	73	00	20	00	74	00	6F	00	20	00	74	o n s t o t
18544	00	68	00	65	00	20	00	53	00	74	00	61	00	72	00	62	h e S t a r b
18560	00	75	00	63	00	6B	00	73	00	20	00	69	00	6E	00	20	u c k s i n
18576	00	46	00	75	00	71	00	75	00	61	00	79	00	20	00	56	F u q u a y V
18592	00	61	00	72	00	69	00	6E	00	61	00	00	00	00	00	12	a r i n a
18608	00	00	00	12	00	00	00	72	00	65	00	63	00	6F	00	67	r e c o g
18624	00	6E	00	69	00	7A	00	65	00	72	00	4C	00	61	00	6E	n i z e r L a n
18640	00	67	00	75	00	61	00	67	00	65	00	00	00	00	00	05	g u a g e
18656	00	00	00	65	00	6E	00	2D	00	75	00	73	00	00	00	00	e n - u s
18672	00	00	00	34	00	00	00	00	00	00	00	00	00	00	00	00	4
18688	00	00	00	04	00	00	00	34	00	00	00	67	00	69	00	76	4 g i v
18704	00	65	00	20	00	6D	00	65	00	20	00	64	00	69	00	72	e m e d i r
18720	00	65	00	63	00	74	00	69	00	6F	00	6E	00	73	00	20	e c t i o n s
18736	00	74	00	6F	00	20	00	74	00	68	00	65	00	20	00	53	t o t h e S
18752	00	74	00	61	00	72	00	62	00	75	00	63	00	6B	00	73	t a r b u c k s
18768	00	20	00	69	00	6E	00	20	00	46	00	75	00	71	00	75	i n F u q u
18784	00	61	00	79	00	2D	00	56	00	61	00	72	00	69	00	6E	a y - V a r i n
18800	00	61	00	00	00	00	00	33	00	00	00	67	00	65	00	74	a 3 g e t
18816	00	20	00	6D	00	65	00	20	00	64	00	69	00	72	00	65	m e d i r e
18832	00	63	00	74	00	69	00	6F	00	6E	00	73	00	20	00	74	c t i o n s t
18848	00	6F	00	20	00	74	00	68	00	65	00	20	00	53	00	74	o t h e S t
18864	00	61	00	72	00	62	00	75	00	63	00	6B	00	73	00	20	a r b u c k s
18880	00	69	00	6E	00	20	00	46	00	75	00	71	00	75	00	61	i n F u q u
18896	00	79	00	20	00	56	00	61	00	72	00	69	00	6E	00	61	y V a r i n a
18912	00	00	00	35	00	00	00	67	00	69	00	76	00	65	00	20	5 g i v e
18928	00	6D	00	65	00	20	00	64	00	69	00	72	00	65	00	63	m e d i r e c
18944	00	74	00	69	00	6F	00	6E	00	73	00	20	00	74	00	6F	t i o n s t o
18960	00	20	00	74	00	68	00	65	00	20	00	53	00	74	00	61	t h e S t a
18976	00	72	00	62	00	75	00	63	00	6B	00	73	00	20	00	69	r b u c k s i
18992	00	6E	00	20	00	46	00	75	00	71	00	75	00	61	00	79	n F u q u a y
19008	00	20	00	56	00	61	00	72	00	69	00	6E	00	61	00	2E	V a r i n a .
19024	00	00	00	39	00	00	00	67	00	69	00	76	00	65	00	20	9 g i v e
19040	00	6D	00	65	00	20	00	64	00	69	00	72	00	65	00	63	m e d i r e c
19056	00	74	00	69	00	6F	00	6E	00	73	00	20	00	74	00	6F	t i o n s t o
19072	00	20	00	74	00	68	00	65	00	20	00	53	00	74	00	61	t h e S t a
19088	00	72	00	62	00	75	00	63	00	6B	00	73	00	20	00	69	r b u c k s i
19104	00	6E	00	20	00	46	00	75	00	71	00	75	00	61	00	79	n F u q u a y

The strings in the blue and green boxes are here, but the string in the red box is different. As before, the purple box with the arrow next to it is what I actually said. As with the previous request, there are multiple versions of what I said below. It could be that the app is generating variations of what I said, assigning some score/weight to them, and then picking which one it *thinks* is what I said. At this point, this is merely speculation on my part. There is definitely more research that can be done in this area.

A couple of days later I had to pick up my child who had been on vacation with the grandparents the previous week. As is normal, my parents and I meet halfway so it isn't too burdensome on either party. This time, I had a couple of text messages that needed to be read prior to starting the navigation. This session is represented by the file `22686.binarypb`. See Figure 23.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
0	09	DF	1E	0C	9B	33	01	00	00	15	59	51	EF	11	1A	0D	B >3	YQİ
16	63	61	72	5F	61	73	73	69	73	74	61	6E	74	DA	B5	BB	car_assistant	ju»
32	F8	03	00	8A	84	C6	F8	03	16	0A	04	00	00	00	00	15	ø S„Eø	
48	00	00	00	00	18	00	21	13	26	6A	01	00	00	00	00	E2	! &j	â
64	D4	C8	F8	03	F9	BD	01	0A	80	B4	01	FF	F3	44	C4	00	ÔÈø ù% €'	ÿóDÄ
80	12	2A	F9	D0	01	41	10	01	00	00	00	00	00	E3	18	C7	*ùÐ A	ã Ç
96	FF	FF	E4	39	DF	9C	E7	21	08	42	10	84	21	CE	73	9C	ÿÿä9Bøç! B „!İsø	
112	E7	39	C8	42	10	84	21	08	73	9C	EF	FF	FF	FF	FF	FF	ç9ÈB „! sœiÿÿÿÿÿ	
128	FF	FF	FF	FF	A9	C8	42	31	08	42	10	E7	39	CE	73	9C	ÿÿÿÿ@ÈB1 B ç9İsø	
144	E4	21	08	42	10	84	16	73	9C	E7	39	CE	20	00	00	00	ä! B „ sœç9İ	

Figure 23

The usual suspects are here, so I repeated my steps with regards to carving out the mp3 file, and got the following audio:

“Smithfield Chicken and BBQ is 51 minutes from your location by car and light traffic.”

Now, this is interesting. This audio file is, in fact, the last thing Google Assistant said to me prior to handing me off to Maps. However, this audio file, as with the others, sits at the front of the `.binarypb` file. This particular session started out by reading my text messages. I decided to scroll through to see if I could find that part of the session.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
49536	44	4C	04	00	00	00	18	00	00	00	76	00	65	00	6C	00	DL	vel
49552	76	00	65	00	74	00	3A	00	71	00	75	00	65	00	72	00	vet:	quer
49568	79	00	5F	00	73	00	74	00	61	00	74	00	65	00	3A	00	y_	state:
49584	71	00	75	00	65	00	72	00	79	00	00	00	00	00	04	00	query	
49600	00	00	2F	00	00	00	63	00	6F	00	6D	00	2E	00	67	00	/	com.g
49616	6F	00	6F	00	67	00	6C	00	65	00	2E	00	61	00	6E	00	oogle.an	
49632	64	00	72	00	6F	00	69	00	64	00	2E	00	61	00	70	00	droid.ap	
49648	70	00	73	00	2E	00	67	00	73	00	61	00	2E	00	73	00	ps.gsa.s	
49664	68	00	61	00	72	00	65	00	64	00	2E	00	73	00	65	00	hared.se	
49680	61	00	72	00	63	00	68	00	2E	00	51	00	75	00	65	00	arch.Que	
49696	72	00	79	00	00	00	01	4C	60	40	80	04	02	00	00	00	ry	L`@€
49712	00	00	00	00	00	00	00	00	00	00	1C	00	00	00	72	00		r
49728	65	00	61	00	64	00	20	00	6D	00	79	00	20	00	6E	00	ead	my n
49744	65	00	77	00	65	00	73	00	74	00	20	00	74	00	65	00	ewest	te
49760	78	00	74	00	20	00	6D	00	65	00	73	00	73	00	61	00	xt	messa
49776	67	00	65	00	73	00	00	00	00	00	12	00	00	00	12	00	ges	
49792	00	00	72	00	65	00	63	00	6F	00	67	00	6E	00	69	00		recogni
49808	7A	00	65	00	72	00	4C	00	61	00	6E	00	67	00	75	00	zerLangu	
49824	61	00	67	00	65	00	00	00	00	00	05	00	00	00	65	00	age	e
49840	6E	00	2D	00	75	00	73	00	00	00	00	00	00	00	1C	00	n-us	
49856	00	00	00	00	00	00	00	00	00	00	00	00	00	00	02	00		
49872	00	00	1F	00	00	00	72	00	65	00	61	00	64	00	20	00		read
49888	6D	00	65	00	20	00	6D	00	79	00	20	00	6E	00	65	00	me	my ne
49904	77	00	65	00	73	00	74	00	20	00	74	00	65	00	78	00	west	tex
49920	74	00	20	00	6D	00	65	00	73	00	73	00	61	00	67	00	t	messa
49936	65	00	73	00	00	00	1C	00	00	00	52	00	65	00	69	00	es	Rei
49952	64	00	20	00	6D	00	79	00	20	00	6E	00	65	00	77	00	d	my new
49968	65	00	73	00	74	00	20	00	74	00	65	00	78	00	74	00	est	text
49984	20	00	6D	00	65	00	73	00	73	00	61	00	67	00	65	00		message
50000	73	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FE	FF	s	YYYYYYYYpY
50016	FF	FF	FE	FF	FF	FF	00	00	00	00	00	00	00	00	FF	FF	YpYYY	YY
50032	FF	FF	F6	F8	9D	85	68	E5	31	00	FF	FF	FF	FF	FF	FF	yyöø ...hå1	YYYYYY
50048	FF	FF	FF	FF	FF	FF	D4	00	00	00	42	4E	44	4C	02	00	YYYYYYÔ	BNDL

Figure 24

The text in Figure 24 is what started the session. The purple box with the arrow represents what I actually said when I initially invoked Google Assistant. The second purple box, as before, is a variation of what I said. Also, the string in the green box is present, but the string in the blue box is absent. Figure 25 is the message that was read to me. Notice that it added the contact information for the message; I sent it from my personal phone, which has an entry in the contacts app on the test device.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
53136	00	00	60	00	00	00	63	00	6F	00	6D	00	2E	00	67	00	` com.g
53152	6F	00	6F	00	67	00	6C	00	65	00	2E	00	61	00	6E	00	oogle.an
53168	64	00	72	00	6F	00	69	00	64	00	2E	00	61	00	70	00	droid.ap
53184	70	00	73	00	2E	00	67	00	73	00	61	00	2E	00	73	00	ps.gsa.s
53200	74	00	61	00	74	00	69	00	63	00	70	00	6C	00	75	00	taticplu
53216	67	00	69	00	6E	00	73	00	2E	00	61	00	63	00	74	00	gins.act
53232	69	00	6F	00	6E	00	73	00	2E	00	6D	00	6F	00	64	00	ions.mod
53248	75	00	6C	00	61	00	72	00	61	00	6E	00	73	00	77	00	ularansw
53264	65	00	72	00	2E	00	72	00	65	00	73	00	75	00	6C	00	er.resul
53280	74	00	73	00	2E	00	4E	00	6F	00	74	00	69	00	66	00	ts.Notif
53296	69	00	63	00	61	00	74	00	69	00	6F	00	6E	00	43	00	icationC
53312	6C	00	69	00	65	00	6E	00	74	00	52	00	65	00	73	00	lientRes
53328	75	00	6C	00	74	00	00	00	00	00	00	00	00	00	02	00	ult
53344	00	00	31	00	00	00	4F	00	6B	00	2C	00	20	00	6C	00	1 Ok, 1
53360	65	00	74	00	27	00	73	00	20	00	74	00	72	00	79	00	et's try
53376	20	00	74	00	68	00	69	00	73	00	20	00	6F	00	6E	00	this on
53392	65	00	2E	00	20	00	4D	00	61	00	6B	00	65	00	20	00	e. Make
53408	73	00	75	00	72	00	65	00	20	00	79	00	6F	00	75	00	sure you
53424	20	00	72	00	65	00	63	00	6F	00	72	00	64	00	20	00	record
53440	69	00	74	00	2E	00	20	00	00	00	3C	00	00	00	4F	00	it. < O
53456	68	00	2C	00	20	00	61	00	6E	00	64	00	20	00	64	00	h, and d
53472	6F	00	6E	00	27	00	74	00	20	00	66	00	6F	00	72	00	on't for
53488	67	00	65	00	74	00	20	00	74	00	6F	00	20	00	64	00	get to d
53504	6F	00	63	00	75	00	6D	00	65	00	6E	00	74	00	20	00	ocument
53520	65	00	76	00	65	00	72	00	79	00	74	00	68	00	69	00	everything
53536	6E	00	67	00	20	00	66	00	6F	00	72	00	20	00	79	00	ng for y
53552	6F	00	75	00	72	00	20	00	70	00	61	00	70	00	65	00	our pape
53568	72	00	2E	00	20	00	00	00	00	00	0C	00	00	00	4A	00	r. J
53584	6F	00	73	00	68	00	20	00	48	00	69	00	63	00	6B	00	osh Hick
53600	6D	00	61	00	6E	00	00	00	00	00	FF	FF	FF	FF	0C	00	man yyyy
53616	00	00	0A	0A	08	01	10	02	18	03	20	04	28	05	01	00	(
53632	00	00	01	00	00	00	01	00	00	00	60	00	00	00	63	00	` c
53648	6F	00	6D	00	2E	00	67	00	6F	00	6F	00	67	00	6C	00	om.googl
53664	65	00	2E	00	61	00	6E	00	64	00	72	00	6F	00	69	00	e.androi
53680	64	00	2E	00	61	00	70	00	70	00	73	00	2E	00	67	00	d.apps.g
53696	73	00	61	00	2E	00	73	00	74	00	61	00	74	00	69	00	sa.stat
53712	63	00	70	00	6C	00	75	00	67	00	69	00	6E	00	73	00	cplugins
53728	2E	00	61	00	63	00	74	00	69	00	6F	00	6E	00	73	00	.actions
53744	2E	00	6D	00	6F	00	64	00	75	00	6C	00	61	00	72	00	.modular
53760	61	00	6E	00	73	00	77	00	65	00	72	00	2E	00	72	00	answer.r
53776	65	00	73	00	75	00	6C	00	74	00	73	00	2E	00	4E	00	esults.N
53792	6F	00	74	00	69	00	66	00	69	00	63	00	61	00	74	00	otificat
53808	69	00	6F	00	6E	00	43	00	6C	00	69	00	65	00	6E	00	ionClie
53824	74	00	52	00	65	00	73	00	75	00	6C	00	74	00	00	00	tResult

Figure 25

After the message was completed, Google Assistant asked if I wanted to reply. You can see what I said in Figure 26.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
63360	00	64	00	00	00	06	00	00	00	00	00	00	00	00	00	00	d	
63376	00	12	BC	6B	B4	35	00	00	42	4E	44	4C	04	00	00	00	4k'5	BNDL
63392	18	00	00	00	76	00	65	00	6C	00	76	00	65	00	74	00	velvet	
63408	3A	00	71	00	75	00	65	00	72	00	79	00	5F	00	73	00	:query_s	
63424	74	00	61	00	74	00	65	00	3A	00	71	00	75	00	65	00	tate:que	
63440	72	00	79	00	00	00	00	00	04	00	00	00	2F	00	00	00	ry	/
63456	63	00	6F	00	6D	00	2E	00	67	00	6F	00	6F	00	67	00	com.goog	
63472	6C	00	65	00	2E	00	61	00	6E	00	64	00	72	00	6F	00	le.andro	
63488	69	00	64	00	2E	00	61	00	70	00	70	00	73	00	2E	00	id.apps.	
63504	67	00	73	00	61	00	2E	00	73	00	68	00	61	00	72	00	gsa.shar	
63520	65	00	64	00	2E	00	73	00	65	00	61	00	72	00	63	00	ed.searc	
63536	68	00	2E	00	51	00	75	00	65	00	72	00	79	00	00	00	h.Query	
63552	01	4C	60	40	80	04	02	00	00	00	00	00	00	00	00	00	L'@€	
63568	00	00	00	00	0A	00	00	00	49	00	27	00	6C	00	6C	00	I'll	
63584	20	00	72	00	65	00	70	00	6C	00	79	00	00	00	00	00	reply	
63600	12	00	00	00	12	00	00	00	72	00	65	00	63	00	6F	00	reco	
63616	67	00	6E	00	69	00	7A	00	65	00	72	00	4C	00	61	00	gnizerLa	
63632	6E	00	67	00	75	00	61	00	67	00	65	00	00	00	00	00	nguage	
63648	05	00	00	00	65	00	6E	00	2D	00	75	00	73	00	00	00	en-us	
63664	00	00	00	00	0A	00	00	00	00	00	00	00	00	00	00	00		
63680	00	00	00	00	02	00	00	00	09	00	00	00	61	00	6C	00	al	
63696	6C	00	20	00	72	00	65	00	70	00	6C	00	79	00	00	00	l reply	
63712	0A	00	00	00	61	00	75	00	74	00	6F	00	20	00	72	00	auto r	
63728	65	00	70	00	6C	00	79	00	00	00	00	00	FF	FF	FF	FF	e p l y	YYYY
63744	FF	FF	FF	FF	FE	FF	FF	FF	FE	FF	FF	FF	00	00	00	00	YYYYYYYYYYYY	
63760	00	00	00	00	FF	FF	FF	FF	F8	F8	9D	85	68	E5	31	00	YYYYøø ...hå1	
63776	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	D4	00	00	00	YYYYYYYYYYYYÛ	
63792	42	4E	44	4C	02	00	00	00	17	00	00	00	61	00	70	00	BNDL	a p

Figure 26

The string in the green box is present...again...and a variation of what I said is seen in the bottom purple box. I then proceeded to dictate my message, which is seen in Figure 27.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
77136	12	C4	7A	3C	3D	00	00	42	4E	44	4C	04	00	00	00	18	Äz<=	BNDL
77152	00	00	00	76	00	65	00	6C	00	76	00	65	00	74	00	3A		velvet:
77168	00	71	00	75	00	65	00	72	00	79	00	5F	00	73	00	74		query_st
77184	00	61	00	74	00	65	00	3A	00	71	00	75	00	65	00	72		ate:quer
77200	00	79	00	00	00	00	00	04	00	00	00	2F	00	00	00	63		y / c
77216	00	6F	00	6D	00	2E	00	67	00	6F	00	6F	00	67	00	6C		om.google
77232	00	65	00	2E	00	61	00	6E	00	64	00	72	00	6F	00	69		e.androi
77248	00	64	00	2E	00	61	00	70	00	70	00	73	00	2E	00	67		d.apps.g
77264	00	73	00	61	00	2E	00	73	00	68	00	61	00	72	00	65		sa.share
77280	00	64	00	2E	00	73	00	65	00	61	00	72	00	63	00	68		d.search
77296	00	2E	00	51	00	75	00	65	00	72	00	79	00	00	00	01		.Query
77312	4C	60	40	80	04	02	00	00	00	00	00	00	00	00	00	00		L'@€
77328	00	00	00	3D	00	00	00	73	00	75	00	72	00	65	00	2E		= sure.
77344	00	20	00	49	00	27	00	6C	00	6C	00	20	00	6D	00	61		I'll ma
77360	00	6B	00	65	00	20	00	73	00	75	00	72	00	65	00	20		ke sure
77376	00	74	00	6F	00	20	00	77	00	72	00	69	00	74	00	65		to write
77392	00	20	00	64	00	6F	00	77	00	6E	00	20	00	65	00	76		down ev
77408	00	65	00	72	00	79	00	74	00	68	00	69	00	6E	00	67		everything
77424	00	20	00	62	00	65	00	66	00	6F	00	72	00	65	00	20		before
77440	00	49	00	20	00	6C	00	65	00	61	00	76	00	65	00	2E		I leave.
77456	00	00	00	12	00	00	00	12	00	00	00	72	00	65	00	63		rec
77472	00	6F	00	67	00	6E	00	69	00	7A	00	65	00	72	00	4C		ognizerL
77488	00	61	00	6E	00	67	00	75	00	61	00	67	00	65	00	00		anguage
77504	00	00	00	05	00	00	00	65	00	6E	00	2D	00	75	00	73		en-us
77520	00	00	00	00	00	00	00	3D	00	00	00	00	00	00	00	00		=
77536	00	00	00	00	00	00	00	03	00	00	00	42	00	00	00	73		B s
77552	00	75	00	72	00	65	00	20	00	73	00	75	00	72	00	65		ure sure
77568	00	2E	00	20	00	49	00	27	00	6C	00	6C	00	20	00	6D		. I'll m
77584	00	61	00	6B	00	65	00	20	00	73	00	75	00	72	00	65		ake sure
77600	00	20	00	74	00	6F	00	20	00	77	00	72	00	69	00	74		to writ
77616	00	65	00	20	00	64	00	6F	00	77	00	6E	00	20	00	65		e down e
77632	00	76	00	65	00	72	00	79	00	74	00	68	00	69	00	6E		verythin
77648	00	67	00	20	00	62	00	65	00	66	00	6F	00	72	00	65		g before
77664	00	20	00	49	00	20	00	6C	00	65	00	61	00	76	00	65		I leave
77680	00	2E	00	00	00	00	00	3D	00	00	00	53	00	68	00	65		. = She
77696	00	72	00	2E	00	20	00	49	00	27	00	6C	00	6C	00	20		r. I'll
77712	00	6D	00	61	00	6B	00	65	00	20	00	73	00	75	00	72		make sur
77728	00	65	00	20	00	74	00	6F	00	20	00	77	00	72	00	69		e to wri
77744	00	74	00	65	00	20	00	64	00	6F	00	77	00	6E	00	20		te down
77760	00	65	00	76	00	65	00	72	00	79	00	74	00	68	00	69		everythi
77776	00	6E	00	67	00	20	00	62	00	65	00	66	00	6F	00	72		ng befor
77792	00	65	00	20	00	49	00	20	00	6C	00	65	00	61	00	76		e I leav
77808	00	65	00	2E	00	00	00	3E	00	00	00	53	00	68	00	75		e. > Shu
77824	00	72	00	65	00	2E	00	20	00	49	00	27	00	6C	00	6C		re. I'll
77840	00	20	00	6D	00	61	00	6B	00	65	00	20	00	73	00	75		make su
77856	00	72	00	65	00	20	00	74	00	6F	00	20	00	77	00	72		re to wr
77872	00	69	00	74	00	65	00	20	00	64	00	6F	00	77	00	6E		ite down
77888	00	20	00	65	00	76	00	65	00	72	00	79	00	74	00	68		everyth
77904	00	69	00	6E	00	67	00	20	00	62	00	65	00	66	00	6F		ing befo
77920	00	72	00	65	00	20	00	49	00	20	00	6C	00	65	00	61		re I lea

You can see the string in the green box is present, and what I actually dictated is in the purple box with the arrow next to it. The variations are in the purple boxes below the first. The message was read back to me, and then I was asked if I wanted to send it. See Figure 28.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
92768	00	61	00	74	00	65	00	3A	00	73	00	65	00	61	00	72	a t e : s e a r
92784	00	63	00	68	00	5F	00	72	00	65	00	73	00	75	00	6C	c h _ r e s u l
92800	00	74	00	5F	00	69	00	64	00	00	00	06	00	00	00	00	t _ i d
92816	00	00	00	00	00	00	00	12	84	3B	7C	1D	00	00	42	4E	": BN
92832	44	4C	04	00	00	00	18	00	00	00	76	00	65	00	6C	00	DL v e l
92848	76	00	65	00	74	00	3A	00	71	00	75	00	65	00	72	00	v e t : q u e r
92864	79	00	5F	00	73	00	74	00	61	00	74	00	65	00	3A	00	y _ s t a t e :
92880	71	00	75	00	65	00	72	00	79	00	00	00	00	00	04	00	q u e r y
92896	00	00	2F	00	00	00	63	00	6F	00	6D	00	2E	00	67	00	/ c o m . g
92912	6F	00	6F	00	67	00	6C	00	65	00	2E	00	61	00	6E	00	o o g l e . a n
92928	64	00	72	00	6F	00	69	00	64	00	2E	00	61	00	70	00	d r o i d . a p
92944	70	00	73	00	2E	00	67	00	73	00	61	00	2E	00	73	00	p s . g s a . s
92960	68	00	61	00	72	00	65	00	64	00	2E	00	73	00	65	00	h a r e d . s e
92976	61	00	72	00	63	00	68	00	2E	00	51	00	75	00	65	00	a r c h . Q u e
92992	72	00	79	00	00	00	01	4C	60	40	80	04	02	00	00	00	r y L`@€
93008	00	00	00	00	00	00	00	00	00	00	07	00	00	00	73	00	s
93024	65	00	6E	00	64	00	20	00	69	00	74	00	00	00	12	00	e n d i t
93040	00	00	12	00	00	00	72	00	65	00	63	00	6F	00	67	00	r e c o g
93056	6E	00	69	00	7A	00	65	00	72	00	4C	00	61	00	6E	00	n i z e r L a n
93072	67	00	75	00	61	00	67	00	65	00	00	00	00	00	05	00	g u a g e
93088	00	00	65	00	6E	00	2D	00	75	00	73	00	00	00	00	00	e n - u s
93104	00	00	07	00	00	00	00	00	00	00	00	00	00	00	00	00	
93120	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FE	FF	YYYYYYYYpY
93136	FF	FF	FE	FF	FF	FF	00	00	00	00	00	00	00	00	FF	FF	YpYpY YpY
93152	FF	FF	FA	F8	9D	85	68	E5	31	00	FF	FF	FF	FF	FF	FF	Yyúø ...há1 YYYYYY
93168	FF	FF	FF	FF	FF	FF	D4	00	00	00	42	4E	44	4C	02	00	YYYYYYYô BNDL

Figure 28

There's that pesky green box again. This time, apparently, Google Assistant felt that it understood what it was I said. There are no variations of what I said here.

The next thing I asked Google Assistant for was directions. See Figure 29.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII	
BA	F1	C8	F8	03	93	ED	04	0A	C9	10	0A	F0	0F	01	4C	°ñEø	"i E ð L
60	40	80	04	02	00	00	00	00	00	00	00	00	00	00	00	`@€	
00	00	4A	00	00	00	67	00	65	00	74	00	20	00	6D	00	J	get m
65	00	20	00	64	00	69	00	72	00	65	00	63	00	74	00	e	direct
69	00	6F	00	6E	00	73	00	20	00	74	00	6F	00	20	00	i	ons to
74	00	68	00	65	00	20	00	53	00	6D	00	69	00	74	00	t	he Smit
68	00	66	00	69	00	65	00	6C	00	64	00	20	00	43	00	h	field C
68	00	69	00	63	00	6B	00	65	00	6E	00	20	00	26	00	h	icken &
20	00	42	00	42	00	51	00	20	00	69	00	6E	00	20	00	B	BQ in
57	00	61	00	72	00	73	00	61	00	77	00	20	00	4E	00	W	arsaw N
6F	00	72	00	74	00	68	00	20	00	43	00	61	00	72	00	o	rth Car
6F	00	6C	00	69	00	6E	00	61	00	00	00	00	00	12	00	o	lina
00	00	12	00	00	00	72	00	65	00	63	00	6F	00	67	00		recog
6E	00	69	00	7A	00	65	00	72	00	4C	00	61	00	6E	00	n	izer Lan
67	00	75	00	61	00	67	00	65	00	00	00	00	00	05	00	g	uage
00	00	65	00	6E	00	2D	00	75	00	73	00	00	00	00	00	e	n - us
00	00	4A	00	00	00	00	00	00	00	00	00	00	00	00	00	J	
00	00	04	00	00	00	4B	00	00	00	67	00	69	00	76	00		K giv
65	00	20	00	6D	00	65	00	20	00	64	00	69	00	72	00	e	me dir
65	00	63	00	74	00	69	00	6F	00	6E	00	73	00	20	00	e	ctions
74	00	6F	00	20	00	74	00	68	00	65	00	20	00	53	00	t	o the S
6D	00	69	00	74	00	68	00	66	00	69	00	65	00	6C	00	m	ithfiel
64	00	20	00	43	00	68	00	69	00	63	00	6B	00	65	00	d	Chicke
6E	00	20	00	26	00	20	00	42	00	42	00	51	00	20	00	n	& BBQ
69	00	6E	00	20	00	57	00	61	00	72	00	73	00	61	00	i	n Warsa
77	00	20	00	4E	00	6F	00	72	00	74	00	68	00	20	00	w	North
43	00	61	00	72	00	6F	00	6C	00	69	00	6E	00	61	00	C	arolina
00	00	4F	00	00	00	67	00	65	00	74	00	20	00	6D	00	O	get m
65	00	20	00	64	00	69	00	72	00	65	00	63	00	74	00	e	direct
69	00	6F	00	6E	00	73	00	20	00	74	00	6F	00	20	00	i	ons to
74	00	68	00	65	00	20	00	53	00	6D	00	69	00	74	00	t	he Smit
68	00	66	00	69	00	65	00	6C	00	64	00	20	00	43	00	h	field C
68	00	69	00	63	00	6B	00	65	00	6E	00	20	00	26	00	h	icken &
20	00	42	00	61	00	72	00	62	00	65	00	63	00	75	00		Barbecu
65	00	20	00	69	00	6E	00	20	00	57	00	61	00	72	00	e	in War
73	00	61	00	77	00	20	00	4E	00	6F	00	72	00	74	00	s	aw Nort
68	00	20	00	43	00	61	00	72	00	6F	00	6C	00	69	00	h	Caroli
6E	00	61	00	00	00	50	00	00	00	67	00	69	00	76	00	n	a P giv
65	00	20	00	6D	00	65	00	20	00	64	00	69	00	72	00	e	me dir
65	00	63	00	74	00	69	00	6F	00	6E	00	73	00	20	00	e	ctions
74	00	6F	00	20	00	74	00	68	00	65	00	20	00	53	00	t	o the S
6D	00	69	00	74	00	68	00	66	00	69	00	65	00	6C	00	m	ithfiel
64	00	20	00	43	00	68	00	69	00	63	00	6B	00	65	00	d	Chicke
6F	00	20	00	26	00	20	00	42	00	61	00	72	00	62	00	n	& Barb

Because of the length of my request, I could not fit everything into the screenshot, but I grabbed what I could. The blue box has returned in this request, and the ever-present green box is here. As usual, my actual request is marked by the purple arrow, with variations of what I said in the purple boxes below. The result of this inquiry was the mp3 file I had carved earlier, and I was then handed off to Maps.

Just an observation here...the hex string in the green box showed up each time Google Assistant listened for input from me, and the hex string in the blue box showed up each time I asked for directions to a location. Is the green box a header? Maybe. I'll defer to someone who has more experience in this area.

The next place I looked was Maps. Maps was a little thin in the way of unique data related to Android Auto. The biggest thing I found were audio files that contained the set of navigation directions that were used when I asked for directions to Smithfield Chicken & BBQ. Those files can be found in **/data/data/com.google.android.apps.maps/apps_tts-temp** folder. These file names are numbers starting with 0 and are in chronological order. There are no file extensions, but the file headers are "RIFF."

Conclusions

In the way of artifacts, Android Auto leaves very little behind with regards to user data, which is not surprising. The app merely functions as an interface to other apps and services in Android, and those apps keep the data to themselves; this makes sense as they are the ones doing all the work. It does, however, reveal some basic data about its use and (at least) one vehicle to which it has been connected.

As vehicles get more and more complex, vehicle manufacturers will continue to add Android Auto as a stock option to their various models. Additionally, Android Auto can be used on the device itself, without the need of an infotainment center. While this ability was not tested specifically, it stands to reason that the artifacts left behind are similar.

The information found in the Google Assistant area of the phone is interesting and could be a great research project. Hopefully, [someone will take it up](#).

Below you will find a chart that contains a quick reference about the artifacts/data discussed in this article.

File Name	Location	Artifact	Relevance
google_analytics_v46308.db	com.google.android.projection.gearhead/files	Google Analytics Client ID	Google Analytics Client ID (gaClientID) - Randomly generated UUID that is used to anonymously identify a particular device or user.
app_state_shared_preference.xml	com.google.android.projection.gearhead/shared_prefs	pref_lastrun	Last time Android Auto was run
cache folder	com.google.android.projection.gearhead/	any	Applications that can use Android Auto will drop assets/resources in this folder
common_user_settings.xml	com.google.android.projection.gearhead/shared_prefs	Bluetooth MAC Address	Bluetooth MAC address for the paired vehicle
common_user_settings.xml	com.google.android.projection.gearhead/shared_prefs	Car Name & Last Location	The name of the car paired, and the last location Android Auto was located
app_session folder	com.android.googlequicksearchbox/	Hands-free interaction	The binarypb files in this folder contain interaction with Google Assistant via Android Auto. The file header will indicate when Google Assistant received a request via Android Auto ("car_assistant")

DFIR Review

The author presents data he obtained from an Android device coupled to his car's entertainment console using Android Auto. The research is done rigorously, the author describes his very detailed note taking during the one week period for which he analyzed the data. The description goes into details regarding the possibilities of the interaction, giving valuable insight for examiners that might not have access to a live system.

The data analysed was obtained from the phone utilizing physical extraction. This was possible because the used phone was rooted, something that may often not be possible when analyzing a phone in a criminal investigation context. Especially for car crashes, where the information may frequently be of interest, it is unlikely that rooting of the phone is considered proportional, even if rooting is available.

The found data is of interest for all cases where interaction with an Android phone using the car as an intermediate takes place. Contrary to other voice controlled devices like Alexa, voice recordings of the driver do not seem to be stored. Only the interpreted data is stored, in multiple possible versions as it seems. It is therefore not possible to gain any information on the individual that issued the command.

The post provides an interesting insight into the traces that can be found in a similar case and is a solid foundation for the interpretation of traces found in a case. The limitation of the experiments are well indicated and provide a handhold limiting the risk of overstressing statements based on the research at hand. Care should be applied when applying the findings on ulterior versions of the application.

Future Work

Further research could delve into the information that can be found on the car's side of the interactions for cases where the device is not available for analysis.

Reviewers

- Addisu Afework Birhanu (Methodology Review)
- Timothy Bollé (Methodology Review)
- Ali Hadi (Methodology Review)
- Francesco Servida (Methodology Review)
- Hannes Spichiger (Methodology Review)