Grand Theft App: Digital Forensics of Vehicle Assistant Apps

Simon Ebbers
Münster University of Applied Sciences
Germany

Fabian Ising
Münster University of Applied Sciences
Germany

Christoph Saatjohann
Münster University of Applied Sciences
Germany

Sebastian Schinzel
Münster University of Applied Sciences
Germany

ABSTRACT

Due to the increasing connectivity of modern vehicles, collected data is no longer only stored in the vehicle itself but also transmitted to car manufacturers and vehicle assistant apps. This development opens up new possibilities for digital forensics in criminal investigations involving modern vehicles. This paper deals with the digital forensic analysis of vehicle assistant apps of eight car manufacturers. We reconstruct the driver's activities based on the data stored on the smartphones and in the manufacturer's backend.

For this purpose, data of the Android and iOS apps of the car manufacturers Audi, BMW, Ford, Mercedes, Opel, Seat, Tesla, and Volkswagen were extracted from the smartphone and examined using digital forensic methods following forensics guidelines. Additionally, manufacturer data was retrieved using Subject Access Requests. Using the extensive data gathered, we reconstruct trips and refueling processes, determine parking positions and duration, and track the locking and unlocking of the vehicle.

Our findings show that the digital forensic investigation of smartphone applications is a useful addition to vehicle forensics and should therefore be taken into account in the strategic preparation of future digital forensic investigations.

CCS CONCEPTS

• **Applied computing** → **Computer forensics**; **Investigation techniques**; • **Security and privacy** → **Mobile and wireless security**; *Privacy protections.*

KEYWORDS

Digital Forensics, Mobile Forensics, Automotive Forensics, Connected Car, GDPR

ACM Reference Format:
Simon Ebbers, Fabian Ising, Christoph Saatjohann, and Sebastian Schinzel. 2021. Grand Theft App: Digital Forensics of Vehicle Assistant Apps. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3465481.3465754

1 INTRODUCTION

Thanks to the large number of assistance systems and the possibilities offered by infotainment systems, modern vehicles give the impression of being computers on wheels. In the past, smart connected systems were reserved for luxury-class vehicles, but nowadays, they are introduced even into compact class vehicles. Interfaces between the vehicle network and the infotainment system allow sensor data to be checked not only from inside the vehicle via the on-board computer but also via a smartphone app [12].

The European New Car Assessment Programme (Euro NCAP) requires the installation of various assistant systems to achieve the highest safety rating [11]. Furthermore, the EU-mandated automatic emergency call system eCall requires manufacturers to install telecommunications technology in vehicles [1].

The associated collection and storage of sensitive data poses new opportunities for criminal investigations. For example, in 2017, investigators used timestamped voice commands from an infotainment system to prove a murder case [13]. While vehicle data is slowly becoming an essential information source for law enforcement, investigation of vehicle assistant app data is less common. Therefore, it is necessary to clarify which is stored and which options exist for criminal investigators to access it.

We consider a twofold approach to this data acquisition. Firstly, we assume that car manufacturers store their users' data and hand them over to investigating authorities where required by law. In the European Union, this obligation is covered by the General Data Protection Regulation (GDPR) (Article 23) [2]. Secondly, we analyze data stored on connected smartphones. Therefore, we aim to answer the following research question: Which data can be forensically acquired from vehicle assistant apps or the manufacturer, and which driver activities can be reconstructed based on this data?

To answer this question, we generate data using a specific usage profile, retrieve the data from smartphone storage using digital forensic methods, and request data from the manufacturer using Subject Access Requests (SARs). We then analyze the acquired data to reconstruct the driver's actions.

We analyzed ten popular vehicle assistant apps on both iOS and Android, focusing on six information categories. We found that all tested apps leave forensic data traces relevant to the driver's behavior on the phone storage.

An extended version of this paper is available at https://arxiv.org/abs/2106.04974.

Contributions. We make the following contributions:

- We provide the first public structured analysis of forensic data stored on smartphone storage by vehicle assistant apps.

ARES 2021, August 17–20, 2021, Vienna, Austria

ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3465754

- We gather data stored by manufacturers of connected vehicles using SARs and analyze relations to the driver's actions.
- We introduce a new data source for criminal investigations by combining forensic smartphone and vehicle data generated by vehicle assistant apps.
- We analyze the data of ten popular vehicle assistant apps for forensic data that could support criminal investigations.

Acknowledgments. The authors would like to thank Christof Wetter and the other vehicle owners for providing test vehicles for our analysis setup.

Fabian Ising and Christoph Saatjohann were supported by the research project "MITSicherheit.NRW", funded by the European Regional Development Fund North Rhine-Westphalia (EFRE.NRW). Fabian Ising was also supported by a graduate scholarship of Münster University of Applied Sciences.

2 RELATED WORK AND BACKGROUND

2.1 Digital forensic background

Locard's rule states that no perpetrator can commit a crime or leave a crime scene without leaving a multitude of traces [8]. This means that no interaction between two objects can occur without leaving mutual traces, even in the digital world. Digital forensics deals with the acquisition, restoration, and analysis of these electronic traces. Digital forensic investigations are subject to high requirements to meet legal demands as digital evidence in court. Thus, an investigation must comply with applicable government guidelines. The investigation aims to clarify the guiding questions of what happened, where, when, and how. In law enforcement and security assessment, it is also necessary to clarify who acted and whether the triggering incident can be repeated in the future. Digital forensics takes an objective role in clarifying these questions and determines both incriminating and exculpatory digital traces.

To guarantee objectivity, the German Federal Office for Information Security (BSI) places the following requirements on the investigation process: Acceptance, Credibility, Reproducibility, Integrity, Cause and Effect, Documentation [3]. Lawful documentation must also include complete proof of the digital traces' whereabouts, the chain of custody, to guarantee the authenticity of collected data.

2.2 Digital Forensics for Smart Vehicles

While assistant systems and smart applications in vehicles become ubiquitous, research into these vehicles' digital forensics is limited. In 2018, Le-Khac et al. presented a thorough analysis of forensic vehicle data, including a case study of a Volkswagen entertainment system [7]. While the authors make a case for using vehicle forensic data in criminal investigations, their research does not focus on smartphone apps for smart vehicles.

In 2015, Thomas Käfer [6] presented a security analysis of carsharing apps and the vehicle assistant app myAudi. The analysis is in a self-published book that the author sells for 280€ at the time of this writing. From the public table of contents, Käfer analyzed the overall security of the apps and looked for forensically interesting data. He did not perform SARs, and he also did not specifically look into manufacturer apps except for myAudi and BMW ConnectedDrive.

Android Auto and Apple CarPlay. In 2019, Joshua Hickman [5], and Sarah Edwards and Heather Mahalik [9] examined Google's Android Auto from a digital forensics perspective. The authors extracted the MAC address, name, and last location of the paired vehicle. Furthermore, they decoded transcribed voice recordings, dictated messages, and navigation instructions from the Google Assistant app. Additionally, log entries for phone calls and short messages sent while using Android Auto were found.

In 2019, Binary Hick [4], and Sarah Edwards and Heather Mahalik [9] forensically investigated Apple's CarPlay. They extracted the layout of CarPlay's home screen icons, the name of the paired vehicle, communication with Siri voice control, short messages, stored coordinates, and an event log that shows information such as new vehicle pairings or instructions to the music player.

3 METHODOLOGY

One of the best-known digital forensics approaches is the Computer Forensic - Secure, Analyze, Present (CFSAP) model, geared towards prosecuting of criminal offenses [10]. We base our forensic analysis on an extended CFSAP-based guide by the BSI [3].

We focus our analysis on the forensic data collection and investigation. All tests were performed in late 2020.

For all tested vehicle app pairings, we performed the same investigation procedure. First, we generated test data by using specific app features. Second, we acquired the internal storage. Third, we examined and analyzed the data stock. Fourth, the vehicle owner sent a SAR to the manufacturer. Finally fifth, we combined the data sets to identify forensically interesting data.

3.1 Setup

A jailbreaked Apple iPhone 6s and a Xiaomi Redmi Note 4 with a custom recovery were used. They ran the latest version of iOS 13 and Android 7 at the time of the study. The digital forensic investigation was done with freely available Linux-based tools.

3.2 Generation of test data

We generated test data by pairing the app with the vehicle and executing a pre-defined list of actions, if available. This list includes locking and unlocking the vehicle, refueling, driving, navigating, sending destinations from the smartphone to the vehicle, documenting the parking position, locating the vehicle, driving the car using the app, and changing the temperature using the app.

We then performed three data acquisitions. One while the user is logged into the app, one after logging out, and one after uninstalling the application. Our investigation is based on these three datasets. The scope of our analysis is information on the key forensic questions of what happened where, when, and how and is limited to the data of the tested apps.

Requests of Manufacturer Data. Finally, the results of the smartphone forensics were supplemented with the data stored by the car manufacturers. The vehicle owner requested these via a SAR according to Article 15 and Article 20 of the GDPR [2].

Table 1: List of vehicles and tested apps.

		Version	
Vehicle	**App**	**Android**	**iOS**
Audi A4 B9	myAudi	3.18.0	3.18.1
BMW 1er F20 140i	my BMW	1.0.1	1.0.1
Ford Kuga '13	FordPass	3.1.0	3.0.0
Mercedes C-Class W204	Mercedes me Adapter	3.11.50	3.6.50
Opel Astra K	myOpel	1.23.4	1.23.4
	OnStar Europe	3.28.0	3.28.0
Seat Mii electric Plus	DriveMii App	3.0	3.0
	Seat Connect	1.1.29	1.1.29
Tesla Model S 75D	Tesla	3.10.8	3.10.8
Tesla Model 3	Tesla	3.10.9	3.10.9
VW Tiguan II	We Connect Go	2.13.8	2.13.6

4 ANALYSIS

The analysis focuses on data that is directly relevant for criminal investigations. Generic application data such as the app's installation date is not presented in this work but is well analyzed [14].

Table 1 displays the vehicles and official manufacturers' apps analyzed for this work. The results of the forensic analysis are summarized in Table 2. All data was acquired from the default paths for app data. The respective section is concluded with an explanation of the data that was disclosed by the SARs. An overview of this data is displayed in Table 3.

4.1 myAudi

The myAudi app is linked to the vehicle via a verified account and a Bluetooth connection. A vehicle code issued by Audi must be entered into the app to gain access to the vehicle data. The app can be used to read the fuel level and range, lock and unlock the vehicle, check the status of windows and the hood, send a planned route to the vehicle's navigation system, keep fuel and mileage logs, and check the maintenance status and arrange service appointments.

iOS. We could reconstruct refueling transactions with timestamps, the fuel amount, and the user-provided price paid. Additionally, we found trips logged in the driver logbook with start and destination address and time.

Android. In addition to the data found on iOS, we found vehicle information, such as the model name and installed assistance systems. Furthermore, the user's date of birth, email address, name, and user id are available. Additionally, navigation start and destination coordinates and historical vehicle data – vehicle coordinates, locking and unlocking of doors, door status, inspection information, timestamped mileage, and vehicle nickname – could be recovered.

GDPR SAR. Audi provides customer data such as name, date of birth, (current and previous) address, telephone number, and email address. Furthermore, Audi communicates the vehicle identification numbers (VINs), model names, equipment, and ownership period of all vehicles listed in the customer order history. Direct contacts, such as email correspondence, are communicated without content. Additionally, the response includes a list of the services associated with the current vehicle, and the note that produced data from these services might be stored. The actual data was not included in the manufacturer's response but can be requested separately.

4.2 my BMW

The my BMW app requires the creation of a user account by entering the VIN. This sends a code to the vehicle, which must be entered into the app to verify the vehicle. Features include remote control of doors and interior ventilation, locating the vehicle, sending navigation destinations, an overview of various vehicle data such as fuel and mileage, and an overview of upcoming maintenance.

iOS. The app does not store relevant data on the filesystem.

Android. The app's data contains the year of manufacture and the VIN of the examined vehicle. Furthermore, it lists the vehicle status with the vehicle's location, timestamp, the status of the doors, upcoming services, and available vehicle features.

GDPR SAR. BMW provides customer data such as the name, date of birth, address, telephone number, and email address, and the sales partner's name and address. Also, the history of vehicles previously registered to the customer is listed with the VIN, model designation, date of first registration, and vehicle ownership. Furthermore, correspondence with the BMW customer service is listed by date.

4.3 FordPass

The app setup requires a Ford account and the vehicle's VIN and must be confirmed on the infotainment system display. The app displays mileage, tire pressure, and fuel level, list of driven routes and refueling operations, and allows sending navigation destinations. Additionally, service appointments can be made via the app.

iOS. The data of the iOS app contains the vehicle's model name, user-assigned nickname, the VIN, timestamped fuel levels, and information on installed modules – e.g., a head-up display or a door control module. The user's email address is available as well.

Furthermore, refueling operations with coordinates, last known vehicle position, navigation destinations, and pictures taken for the parking spot reminder functionality are available.

Android. We found several empty databases with table names indicating forensically relevant data, such as trip destinations or position data. We assume that these tables are only used for newer vehicle generations. However, we found detailed vehicle information, including the vehicle's exact name, VIN, year of manufacture, nickname, engine and transmission model, warranty period, and emission class. We also found the user's email address, name, account name, and salt and hash of the user-provided app PIN.

GDPR SAR. Ford only provides the customer's name and email address. Ford states that since the linked vehicle does not have an internet connection, no vehicle data is transmitted.

4.4 Mercedes me Adapter

The app requires a Mercedes Bluetooth adapter plugged into the vehicle's On-Board Diagnostic (OBD) interface. The user account must be verified at an official Mercedes dealer by presenting the vehicle registration document and the ID card. The app offers trip lists, navigation to the parked vehicle, a live overview of vehicle

Table 2: Overview of the forensic analysis results.

	Android								*iOS*							
App name	**drive log**	**recent location**	**parking**	**refueling**	**user info**	**car info**	**logout**	**uninstall**	**drive log**	**recent location**	**parking**	**refueling**	**user info**	**car info**	**logout**	**uninstall**
myAudi	◐	–	–	●	●	●	●	–	◐	–	–	●	–	–	–	–
my BMW	∅	●	∅	∅	∅	●	–	–	∅	–	∅	∅	–	–	–	–
FordPass	–	∅	∅	∅	●	●	–	–	–	●	●	●	●	–	–	–
Mercedes me Adapter	○	○	○	○	◐	○	∅	–	●	●	●	●	●	●	●	–
myOpel	∅	∅	∅	∅	●	●	●	–	∅	∅	∅	∅	●	●	●	–
OnStar Europe	∅	∅	∅	∅	◐	●	●	–	∅	∅	∅	∅	–	–	∅	–
DriveMii App	◐	○	∅	∅	∅	◐	∅	–	◐	○	∅	∅	∅	◐	∅	–
Seat Connect	∅	–	–	∅	●	●	●	–	∅	–	–	∅	●	●	●	–
Tesla	◐	◐	◐	◐	◐	◐	◐	–	–	◐	◐	◐	◐	◐	◐	–
We Connect Go	●	●	●	●	–	●	–	–	●	●	●	●	–	●	–	–

● extensive data ◐ data cached/partially available ○ encrypted database ∅ feature not available/not tested – no data

data such as temperatures and accelerator pedal position, a display of error messages and upcoming maintenance, and various statistics on kilometers driven and fuel consumption.

iOS. Our dataset contains the distance of the last trip taken with the vehicle, any data displayed in the app's dashboard, user information, and data on refueling. Additionally, the driver logbook's records are available, including trip start and destination addresses and the vehicle's current location in ten-second intervals.

Android. In the Android version of this app, we found two encrypted databases with names matching those from iOS. Therefore, we assume that the same data is stored in them. However, we were unable to decrypt them to prove this. Other files allowed extracting the owner's address, the VIN, the OBD adapter's identification number, the remaining distance until the next service appointment, and timestamps of the last usage and account creation.

We also found cached Google Maps URLs showing map sections displayed in the app during data collection. Additionally, pictures taken for the parking spot reminder function are available.

GDPR SAR. The Mercedes-Benz AG provides the customer's name, date of birth, email address, and address, and the time the user agreed to the user conditions. No vehicle information is provided.

4.5 myOpel

The myOpel account can be linked to the vehicle by entering the VIN. The vehicle connection must be verified by presenting the vehicle registration document to an Opel dealer. With the test vehicle, only the mileage could be viewed via the app, and a service appointment could be made. Further features were not available.

iOS. We were able to determine user information such as the email address and the VIN. Additionally, vehicle information, warranty data, and the registered service partner are available. We also found timestamped coordinates of the smartphone in the dataset.

The data structure of the `BTAModel.sqlite` database suggests that it records traveled routes with timestamps and location information. Due to the limited range of functions of the available vehicle, there are no corresponding entries in the investigated dataset.

Android. All iOS data was available in Android as well. Moreover, we found an HTTP Cache with cached communication between the app and backend, i.e., a download of the vehicle manual.

GDPR SAR. Opel provides the name of the customer and the address, telephone number, and email address. Additionally, the registration number, VIN, and model designation are listed.

4.6 OnStar Europe

An OnStar account number must be requested via the vehicle's OnStar button to create an account. The app can display mileage, and the parking position can be set and documented with a picture. The OnStar web app, however, displays more extensive data.

iOS. The app does not store relevant data on the filesystem.

Android. We successfully recovered information about the vehicle, such as the VIN and the model designation, from a JSON file. An SQLite database contains information about the vehicle, such as the model name, the tire pressure, and mileage.

GDPR SAR. OnStar's response contains the customer data, such as name, address, telephone number, email address, and date of account creation. Furthermore, it contains the vehicle's VIN and GSM module's identifiers. Also, it is shown at which time the customer used which OnStar product packages such as extended service offers. A log records timestamped warnings. In our case, this log includes the messages `oil` and `low tires`.

Additionally, in-vehicle phone calls with OnStar advisors are logged, including the vehicle's coordinates and start and end time. This conversation history goes back to when the applicant did not own the vehicle. Correspondence is listed without content.

4.7 DriveMii App

Seat's DriveMii app offers offline navigation, an Ecotrainer that displays the energy consumed and recuperated, a media player, and information about the current trip. The smartphone can be connected to the vehicle via Bluetooth without account registration.

iOS & Android. We recovered the paired vehicle's VIN and records about the recuperated energy every minute. We found several apparently encrypted SQLite databases in the app folder. From the files' names, e.g., `locations.sqlite` or `tracks.sqlite`, it can be assumed that relevant data such as location, itinerary, and track data is stored. A Tag-Length-Value file contains the user-entered navigation destinations, such as the town or street name.

GDPR SAR. See the next section for the SAR sent to Seat.

4.8 Seat Connect

The Seat Connect app uses a Seat account, which must be linked to the vehicle via the VIN. The app displays the remaining range till recharge, whether the doors and windows are locked, whether the lights are switched off, the average energy consumption, and the time until the next scheduled service. Furthermore, the batteries' charging can be planned, the vehicle's current position can be determined, and the air conditioning can be controlled remotely.

iOS. We found a timestamp of the last user login, the VIN, and the user's phone number, date of birth, and email address.

Android. The app's SQLite databases store the user account's email address, the VIN, the vehicle's exact name, and nickname.

GDPR SAR. Seat provided the customer's name, date of birth, address, nickname, phone number, and email address. Furthermore, they log vehicle access, allowing reconstruction of vehicle usage.

4.9 Tesla

The user must log in via their Tesla account and allow mobile access to the vehicle. Then, the vehicle's range and temperatures can be read in the app. In addition, several car features can be controlled, including the lights, doors, the interior temperature, and the seat heating. Also, the vehicle can be driven forward and backward from outside via the app, when the user is in proximity. The analysis outcomes for all Tesla app versions and cars were the same.

iOS. We recovered static vehicle data, such as the vehicle name and the VIN. Dynamic data, namely the coordinates of the last location, interior temperature, and the timestamped state of charge, is recoverable from a JavaScript Object Notation (JSON) file.

Android. The app uses an SQLite database that stores, among other information, the user's email address. We found data packages in JSON format that contain the VIN, user ID, and vehicle status. The most important information of the status includes the vehicle's location, the speed, and the gear enriched with timestamps. Other files contain the user's first and last name, the account name, which corresponds to the email address, various configurations and equipment of the vehicle, and the vehicle's name.

GDPR SAR. In addition to the customer information, Tesla's response contains extensive vehicle data: the model name, the VIN, warranty, and the vehicle's number plate. Additionally, tables with up to 229 columns for six days were included in the information provided. These, for example, contain data labeled `Autosteer Driver Hands On Detection` and `Primary Steering Angle Sensor (degrees) (Positive indicates right turn)`. This data is collected up to ten times per second. An attached document states that the regularly collected data may be transmitted to Tesla to ensure the vehicle's continuous performance and predictive maintenance.

4.10 We Connect Go

A VW DataPlug must be plugged into the vehicle's OBD interface to use the We Connect Go app. After registering an account, the app can connect to the VW DataPlug via Bluetooth using a code printed on the DataPlug. The app displays fuel level, range, current mileage, and other vehicle data. The app offers the possibility to keep fuel and trip logs and arrange service appointments. Furthermore, the app offers additional statistics and driving style analysis.

iOS & Android. For both apps, we recovered a parking position image taken by the user. The app data is stored in SQLite databases, which include data identifying the paired VW DataPlug. The main database stores extensive data, including detailed static vehicle information such as the VIN, model code, engine, and transmission designation. It also contains statistical data such as average fuel consumption and timestamped fuel levels. The stored trip data comprises timestamped refueling processes with coordinates, traveled distances, timestamped start and destination addresses with coordinates, and acceleration and deceleration values with corresponding velocities. Finally, timestamped parking coordinates are listed.

After a logout, the parking position image and the DataPlug information are still recoverable. It is deleted after uninstalling.

GDPR SAR. Volkswagen AG disclosed the customer data with name, date of birth, address, email address, telephone numbers stored, and the vehicle's VIN and registration number. Further personal data is divided into categories, including Car2X, accident, contract, and position data, all of which can be requested separately.

5 EVALUATION AND DISCUSSION

Our investigation shows that the apps handle data, such as logged locations, in diverse ways. While only the Mercedes Me adapter iOS application left extensive data of all categories on the phone storage, all tested apps left forensic data traces of some variation.

Almost all of these data traces could aid in criminal investigations, e.g., to prove that a suspect used the vehicle during the time of the suspected wrongdoing. Location data is even more helpful.

The scope of the data on the smartphone depends on the equipment of the vehicle. In the case of the Mercedes and Volkswagen vehicles examined, additional hardware was required for data transmission. However, the vehicles which communicated with the smartphone via Bluetooth provided the most extensive data through the digital forensic analysis. Here the smartphone acts as a repository for the data collected. For vehicles using a GSM interface, only data retrieved in the app was cached on the smartphone. In this case, the data is not stored completely on the smartphone but on the manufacturer's server or the vehicle.

Table 3: Overview of data included in GDPR SAR responses.

Manufacturer	**Customer Data**	**Vehicle Data**	**Infotainment Usage**	**Correspondence**	**Order History**	**Position Data**	**Additional Data**
Audi	●	●	●	○	◐	–	–
BMW	●	●	–	○	–	–	–
Ford	●	–	–	–	–	–	–
Mercedes	●	–	–	–	–	–	–
Opel	●	●	–	–	–	–	–
OnStar	●	✚	●	○	●	◐	✚
Seat	●	●	●	–	–	–	–
Tesla	●	●	–	–	●	●	✚
Volkswagen	●	●	–	–	●	●	✚

● full data ◐ partial data ○ metadata
– no data ✚ extensive data (see text)

Interestingly, the analysis of iOS and Android apps shows that the data storage differs significantly. For example, stored data from the Mercedes app is encrypted in Android but not in iOS.

The data manufacturers provided in responses to the SARs also differed significantly. Except for Mercedes – which only provided the customer data – all manufacturers provided customer and vehicle data. Vehicle information ranged from basic information to a detailed list of the vehicle's equipment. Audi and Volkswagen only stated what data they collect but not the actual – seemingly extensive – data. OnStar Europe communicated when and from which location communication to the OnStar service was established. The data even includes a period when the applicant did not own the vehicle – which is a serious privacy violation.

Tesla's extensive data shows the potential benefit law enforcement could reap from requesting customer data from the manufacturer. Since Tesla includes detailed metrics with high resolution, almost any vehicle actions can be reconstructed. In combination with other evidence, this data could aid in reconstructing criminal cases, including checking alibis and even convicting or exonerating the driver of a crime involving the vehicle. While only Tesla provided such extensive data, the data we received in response from other manufacturers might be limited by the tested vehicles' features and equipment. We expect that more modern vehicles will provide even more data to the manufacturer and the assistant application, providing useful information for criminal investigations.

6 CONCLUSION

This work shows that the extensive data generated by modern vehicles is transmitted to car manufacturers and transferred and stored on drivers' smartphones through vehicle assistant apps.

The digital forensic examination of the apps shows that this data is a useful addition to vehicle forensics. Using digital forensic methodology, we retrieved data from the tested apps in order to contribute to clarifying the key digital forensic questions.

The information provided by car manufacturers in response to the SARs shows that often only data on the vehicle's owner, designation, and the VIN are present. Extensive data was only provided by Tesla. Thus, it can be concluded that this personal data is not within the direct access of the car manufacturers and is stored in the vehicles' storage. The volume and diversity of the vehicle data provided by Tesla show the possibilities of data collection available in modern vehicles. This data collected on a millisecond basis considerably supports analyzing and reconstructing incidents.

Our research results provide a positive result to our research question about the usefulness of forensically acquired data from vehicle assistant apps and data requested from manufacturers in investigating criminal offenses. Such extensive data as acquired from Tesla and the forensic analysis of various apps could be a crucial aid in solving criminal offenses. While not all tested apps and contacted manufacturers provide such extensive data, the trend shows that the amount of data collected by future vehicle assistant systems will increase, providing even more data to investigators.

In summary, this work provides insights to be considered for future digital forensic investigations involving smart vehicles. In particular, we recommend that law enforcement considers the data generated by vehicle assistant applications to aid in investigations.

Future Work. In some cases, the encryption of databases in Android applications prevented access to information. Further forensic research should look into the encryption's strength and key management. Another interesting research avenue is the caching of data. While we could reconstruct cached data in apps after usage, we did not analyze the actual caching behavior. It would be interesting to learn how long data remains available for forensic analysis.

REFERENCES

[1] Council of European Union. 2015. Regulation (EU) 2015/758 of the European Parliament and of the Council.

[2] Council of European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council.

[3] Bundesamt für Sicherheit in der Informationstechnik. 2011. Leitfaden "IT-Forensik".

[4] Binary Hick. 2019. Ridin' With Apple CarPlay. https://thebinaryhick.blog/2019/05/08/ridin-with-apple-carplay/

[5] Joshua Hickman. 2019. Ka-Chow!!! Driving Android Auto. https://dfir.pubpub.org/pub/716tlra7/release/2

[6] Thomas Käfer. 2015. *Car-Forensics : Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung.* Books on Demand.

[7] Nhien-An Le-Khac, Daniel Jacobs, John Nijhoff, Karsten Bertens, and Kim-Kwang Raymond Choo. 2020. Smart vehicle forensics: Challenges and case study. *Future Generation Computer Systems* 109 (2020), 500–510. https://doi.org/10.1016/j.future.2018.05.081

[8] Edmond Locard. 1930. *Die Kriminaluntersuchung und ihre wissenschaftlichen Methoden.* Berliner Kameradschaft.

[9] Sarah Edwards; Heather Mahalik. 2019. They See us Rollin'; They Hatin': Forensics of iOS CarPlay and Android Auto. SANS DIFR Summit 2019.

[10] George Mohay, Alison Anderson, Byron Collie, Olivier De Vel, and Rodney McKemmish. 2003. *Computer and Intrusion Forensics.* Artech House.

[11] Euro NCAP. 2020. System Grading. https://www.euroncap.com/en/vehicle-safety/safety-campaigns/2020-assisted-driving-tests/gradings-explained

[12] Netscribes Inc. 2020. Projected global ADAS market size between 2015 and 2023. https://www.statista.com/statistics/591579/adas-and-ad-systems-in-light-vehicles-global-market-size/

[13] Olivia Solon. 2020. Insecure wheels: Police turn to car data to destroy suspects' alibis. https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939

[14] R. Tamma, O. Skulkin, H. Mahalik, and S. Bommisetty. 2020. *Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices, 4th Edition.* Packt Publishing.