Digital Forensics Investigation of the Tesla Autopilot File System

Kevin Gomez Buquerin
Technische Hochschule Ingolstadt and
Friedrich Alexander University Erlangen Nürnberg
CARISSMA Institute of Electric, Connected, and
Secure Mobility (C-ECOS)
Germany
email: extern.kevinklaus.gomezbuquerin@thi.de

Hans-Joachim Hof
Technische Hochschule Ingolstadt
CARISSMA Institute of Electric, Connected, and
Secure Mobility (C-ECOS)
Germany
email: hans-joachim.hof@thi.de

***Abstract*—Tesla vehicles offer a wide range of services, including an autopilot. As a central vehicle component, the autopilot has been the focus of much media and research attention. Several articles have highlighted flaws in the autopilot service. These flaws make the autopilot service relevant for Automotive Digital Forensics (ADF) investigations since vehicle automation is likely to cause accidents. This paper presents an ADF investigation of the file system of a Tesla autopilot hardware version 2.0. We identified metadata characteristics, including general information (such as Linux user accounts, extensions, and timestamps) and vehicle-specific characteristics (including surveillance and safety-related information that is of great use in investigations of modern vehicles). The paper evaluates the forensic reliability of memory acquisition and the usability of the identified features.**

Index Terms*—*automotive, vehicle, digital forensics, automotive digital forensics, tesla, autopilot, metadata, vehicle forensics

I. Introduction

The total number of Tesla deliveries has steadily increased in recent years. In the first quarter of 2021, Tesla delivered 184,800 vehicles [21], in the second quarter of 2021, 201,250 [22], in the third quarter, 241,300 [23] and in the fourth quarter of 2021, 308,840 [24]. These figures show an increase of 66,99% in one year. The company's electric vehicles offer various services, including the autopilot. According to an investigation by Isidore and Valdes-Dapena [25], bugs regularly appear in Tesla's autopilot. As a result, its vehicles and autopilot are likely to be part of ADF investigations. Understanding the Tesla car and its features, including the autopilot and file system, is key to a successful ADF investigation. Buchholz and Spafford show that the file system is essential in Digital Forensics (DF) and ADF investigations [26]. This leads to the following research question, "*What are DF- and ADF-specific characteristics that can be captured in the file system of a modern vehicle?*" with the hypothesis "*The file system of the Tesla autopilot contains metadata relevant to answer forensic questions in ADF investigations.*" Our contributions are:

- Identification of metadata characteristics of a Tesla autopilot hardware version 2.0.
- Identification of general DF characteristics of a vehicle-specific file system.
- Identification of vehicle-specific characteristics from a Tesla autopilot snapshot.
- Evaluation of the forensic soundness of the data acquisition method from the Tesla autopilot Electronic Control Unit (ECU).

This paper is structured as follows – Section II highlights related work in Tesla analysis and ADF investigations. The research question is further analyzed in Section III by considering the characteristics and metadata of the Tesla autopilot and their relevance to ADF. The implementation of a forensic analysis of the Tesla autopilot is presented in Section IV. Section V summarizes the results of the investigation. The evaluation in terms of forensic soundness, usability, limitations, and assumptions is presented in Section VI. Section VII concludes the paper and gives an outlook on future work.

II. Related work

We are not the first to look at Tesla vehicles. In this Section, we highlight different research focusing on security analysis of Tesla vehicles, its components, and services. Such investigations hold valuable information that can be used in DF investigations. Furthermore, we highlight ADF investigations on Tesla vehicles in existing research and how our approach and research goals differ.

In [17], Tencent's Keen Security Labs present a security analysis of a Tesla vehicle. They reverse-engineered the in-vehicle Controller Area Network (CAN) bus and show problems that lead to wireless exploitation of such vehicles. A similar problem was presented in [16], where the authors remotely compromised the gateway of the Body Control Module (BCM) of Tesla vehicles. ADF investigations can benefit from such security analysis. Such information helps determine where logs and other valuable information are stored to answer forensic questions.

Tristan Rice published a multi-part blog post about a security analysis of a Tesla Model 3, starting with [20]. The author reverse-engineered various services (e.g., the autopilot and software update system), the internal structure, security configurations (e.g., firewalls and iptables), and the internal API. Such descriptions enable forensic scientists to identify

 ISBN: 978-1-68558-007-0

locations with characteristics relevant to DF investigations. This knowledge is valuable for security analysis and benefits ADF investigations.

In [19], Gomez et al. focus on the architecture, communication data, and snapshot capabilities of a Tesla autopilot hardware version 2.0, and the authors evaluate how these features affect the handling of personal data. Our work analyzes the same autopilot version but focuses on the relevance of the file system for ADF investigations.

Ebbers et al. published an article analyzing several IOS and Android apps for different vehicles [18]. They sent Subject Access Requests (SARs) to Original Equipment Manufacturers (OEMs) to get all the information OEMs have about each user. The authors found that data for smartphone apps may be encrypted or stored in plain text on smartphones. Some OEMs - such as Tesla - can transmit various vehicle data that could be relevant to DF investigations. Others OEMs - such as Ford and Mercedes [18] - are pretty limited in data availability.

The highlighted articles focus on security issues and data handling in Tesla vehicles. To the best of our knowledge, no article has been published on the Tesla autopilot file system and its relevance of DF investigations.

III. Investigation of the characteristics of the Tesla autopilot

Carrier defines digital investigations as "*a process by which we develop and test hypotheses that answer questions about digital events*" [15]. Thus, DF investigators need to reconstruct digital events based on the data they collect and analyze. As highlighted by Gomez et al. in [14], this is also true for ADF, but with a focus on automotive systems. In addition, the authors mention the importance of forensic questions of interest. The questions are in focus throughout this article and are:

- *Who* performed or is responsible for a digital event?
- *What* digital event was performed?
- *When* did the digital event take place?
- *Where* did the digital event take place?
- *How* did the digital event take place?
- *Why* did the digital event take place?

A. Tesla's autopilot from the perspective of digital forensics

The Tesla autopilot is an advanced driver assistance system. It supports the driver with various services such as cruise control, lane assistant, navigation, and automatic distance assistant. Tesla introduced autopilot in hardware version 1 in 2014, followed by hardware version 2.0 and 2.5 in 2016 [12]. The latest version is 3, which was introduced in 2019 and installed in all new Tesla vehicles since then [11]. We will focus on hardware version 2.0 due to its availability in the investigated vehicle. In addition, snapshots of the Tesla autopilot in hardware version 3 are usually encrypted. Based on a study by MIT, hardware version 2.0 is still installed in Tesla vehicles on the road [1] [2].

As mentioned by Rice in [20], the autopilot introduces several services and features. Examples include the service itself and the *Hermes* service, enabling communication between the OEM backend and Tesla vehicles. Hermes is also used to provide updates to features and components in the vehicle. Tesla vehicles store the files of the autopilot in encrypted form [10]. This causes problems with extracting the autopilot from in-vehicle systems during ADF investigations. Older versions of the autopilot were not encrypted, as described in an article by Keen Security Labs [9]. During the ADF investigation, the analyst must decrypt any encrypted autopilot. To do so, the analyst needs either the corresponding decryption key or an exploit for the autopilot.

B. Metadata in digital forensic investigations of file systems

Buchholz and Spafford define characteristics related to metadata based on the forensic questions *who*, *where*, *when*, *what*, *why*, and *how* [26]. They emphasize the importance of metadata in file systems to answer these forensic questions. As described by Carrier in [15], metadata is directly linked to the describing object. Thus, its metadata also changes when the object is modified, deleted, or otherwise changed. This fact makes metadata an important consideration in DF studies. Compared to deleting files (e.g., log files) or modifying text files, manipulating metadata is more challenging for an attacker.

As a result, DF investigators must validate the *trustworthiness* of the collected information to trust the metadata. In DF, trustworthiness is referred to as *forensic soundness* [8], which corresponds to the degree of the following attributes, as shown by [7]:

- Correctness: information that was actually stored in memory when the snapshot was taken.
- Atomicity: There should be no signs of concurrent system activity.
- Integrity: Captured memory areas will not be modified after the capture timestamp t.

The goal of DF investigations is to achieve a high level of forensic soundness to ensure the trustworthiness of the captured metadata.

IV. Digital forensic features of a Tesla autopilot hardware version 2.0

This paper focuses on the Tesla autopilot, i.e., hardware version 2.0. We analyzed the collected data using two approaches to enable comparability and minimize analysis errors by forensic tools: (1) developing a Python tool for analysis and (2) using Magnet AXIOM, a sophisticated DF tool. This approach also allows us to determine general characteristics of the Tesla autopilot relevant to future studies.

We conducted the ADF investigation following the process model proposed by [14]. The authors highlight four steps:

1) Forensic readiness: Determine if relevant data sources and tools are available to conduct an investigation.
2) Data collection: Obtain necessary information.
3) Data analysis: Analyze the data collected.
4) Documentation: Prepare a report presenting the results.

 ISBN: 978-1-68558-007-0

Forensic readiness is given for Tesla autopilot analyses. Snapshots can be created using various methods, e.g., chip-off or live acquisition. Tools for analysis are available with a custom Python tool and Magnet AXIOM. We discuss data acquisition and analysis in the following. This paper is the documentation of the results of the ADF investigation.

A. Acquisition of the Tesla autopilot

We acquired a Tesla autopilot (hardware version 2.0) from a 2017 Tesla Model S. We performed a chip-off of the installed memory device on the autopilot ECU. Chip-offs are a DF technique that has proven successful in ADF investigations, as [6] demonstrated in the analysis of a Volkswagen infotainment system.

Data on the extracted chip was acquired using a memory adapter that translates the pin-out to Universal Serial Bus (USB). Using a write blocker, we could ensure the data's integrity during the acquisition process. Write blockers are used in investigations to prevent changes to the data on the target evidence.

The result of the acquisition process was a snapshot of the Tesla autopilot. We created a duplicate and continued working on the duplicate only.

B. Python tool for Tesla autopilot analysis

The next step is to analyze the collected data. As suggested by [14], the data should be initially reviewed. We expected the snapshot to be encrypted. However, we were able to read the contents of the snapshot. In addition, we found that the snapshot was stored as *SquashFS* (a common read-only file system for Linux). This confirmed the security analysis results presented in [9].

We mounted the file system and identified several folders, all related to the classic Linux file system structure. Examples include *bin*, *etc*, *home*, and *lib*. We have also identified vehicle-specific folders such as the *opt* folder. It contains binaries for the autopilot and the *Hermes* service used for communication between the Tesla backend and Tesla vehicles. Another interesting folder for ADF investigations is the *lib* folder that stores all libraries used. Those can be valuable during penetration testing and identification of vulnerable libraries.

To automate the analysis process, we implemented a custom Python tool - in form of a Jupyter Notebook - to collect various metadata from the mounted file system. The tool uses "*os.walk()*" to recursively collect all directories and files. In addition, the implementation determines the timestamp of the last modification and the extension of each file. Finally, we create graphs to present the results.

The tool collected 4216 unique files and 447 directories from the mounted file system. We used the framework *python-magic* [5] to determine the file type. For 291 files (6.91%), the framework was unable to determine the type. We assume that the reason are corrupted magic bytes of the files (e.g., from custom file-types) and dot files from Linux. However, we were not able to confirm our assumption. The same is true for timestamps. The timestamp for 275 files and folders (6.52%) could not be determined for the same reasons.

As shown in Figure 1 and Table I, the most commonly used extension is *.so*, followed by *.0* (linked file on a Linux system), *.crt*, *.pem* and *.conf*. The extensions with numbers (e.g., *.1* or *.2*) are user-defined extensions probably used to arrange files within a directory.

TABLE I
NUMBER OF FILE EXTENSIONS WITHIN A TESLA AUTOPILOT

Extension	Count	Extension	Count
.so	356	.4	19
.0	221	.rules	18
.crt	140	.56	15
.pem	133	.hwdb	14
.conf	103	.6	14
.mo	100	.5	11
.sl	46	.10	9
.1	41	.wav	9
.2	33	.pdf	8
.img	32	.3	7
.sh	28	.profile	7
.txt	26	.00	7
.map	26	.13	6
.hlp	25	.16	6
.bin	24		

We created the line graph shown in Figure 2 from the collected timestamps. Several peaks in the timestamps are clearly visible. Table II lists the ten most frequently timestamps.

TABLE II
THE TIMESTAMP RESULTS WERE USED TO CREATE A LINE GRAPH.

Timestamp	Occurrences
Fri Jul 19 05:16:47 2019	1234
Fri Jul 19 05:51:13 2019	587
Fri Jul 19 05:51:12 2019	332
Fri Jul 19 05:28:04 2019	208
Fri Jul 19 05:28:03 2019	192
Fri Jul 19 05:51:06 2019	158
Fri Jul 19 05:23:04 2019	112
Fri Jul 19 05:51:18 2019	108
Fri Jul 19 05:29:59 2019	105
Fri Jul 19 04:22:50 2019	74

C. Analysis of the Tesla autopilot using Magnet AXIOM

To validate our results from Section IV-B and compare the findings of another tool, we analyzed SquashFS using Magnet AXIOM. The forensics tool identifies various indicators and presents them in a final report. Magnet AXIOM identified so-called *people*. In the case of a Tesla autopilot, these relate to Linux user accounts. Magnet AXIM identified a total of 103 accounts that contain usernames and IDs. These include common user accounts such as *root*, *daemon*, and *bin*. In addition, automotive and autopilot-specific usernames were also identified, including *temperature_monitor*, *visualizer*, *legacyvehicle*, *drivermonitor*, *gps*, and *hermes*.

The autopilot contains various media files. In particular, these are audio files used in the infotainment system. Examples

 ISBN: 978-1-68558-007-0

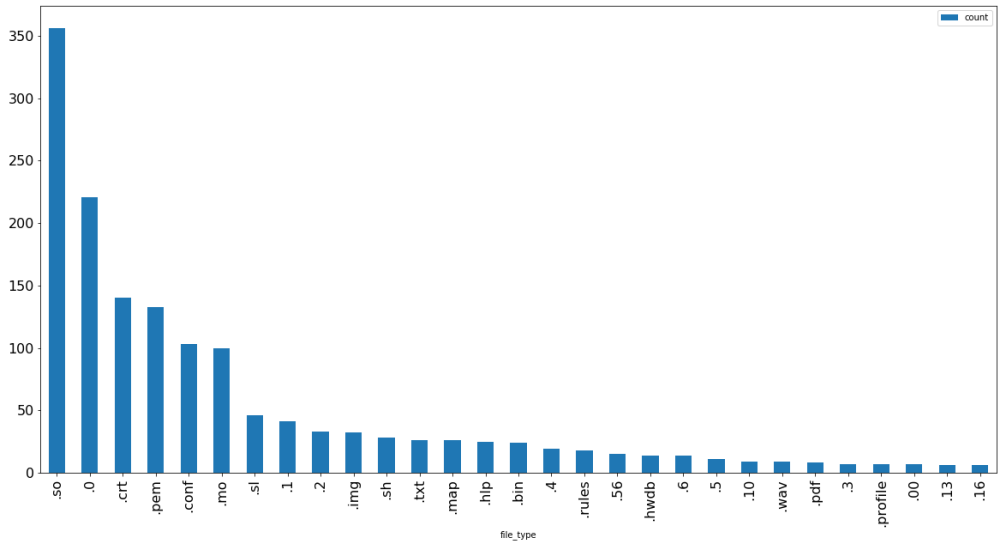

Figure 1. File types in the Tesla autopilot

are *.wav* files for steering wheel warnings or forward collision warnings.

Another category highlighted by Magnet AXIOM is *documents*. For the autopilot, these include a *.csv* sample file, 8 *.pdf* user manuals, and 26 *.txt* files, i.e., READMEs.

Magnet AXIOM has identified 32 *.img* files. These files are the firmware images of the various services implemented in the Tesla autopilot hardware version 2.0. All the *.img* files contain the string "*HW2*", indicating that these files refer to hardware version 2.0.

For the operating system information, Magnet AXIOM correctly detected the use of buildroot. The operating system version is specified as "*2016.05-g977a322*". This is the string that is included in the buildroot configuration.

V. Results of the Forensic Analysis

We implemented an ADF investigation on the Tesla autopilot file system and performed two analyses using a custom Python tool and Magnet AXIOM.

A. Answering forensic questions using the collected metadata

The metadata found is able to answer most of the forensic questions highlighted in Section III. Table III summarizes the results related to the forensic questions. The questions about "*Who performed or is responsible for a digital event?*" can be traced to the user accounts highlighted by Magnet AXIOM. In addition, "*who*" can be answered cron-jobs too. The next question relates to "*Where did the digital event take place?*" and is to be answered with the file and folder structure within the file system. "*When did the digital event take place?*" uses the timestamp collected by the custom Python tool as well as logs located in different location within the file-system. Some log files are located in the *etc* folder. However, these are general system logs and not application logs. Together with the configuration files (i.e., the *.conf* and *.profile* extensions), we can partially answer the question "*How did a digital event take place?*". The collected metadata cannot answer the question "*Why did a digital event take place?*".

If different log-files or other event management systems store information such as the user accounts, cron-jobs, and time-stamps, such data can be correlated with the results we highlighted. Hence, this information can be used to prove who or what is responsible for a digital event.

TABLE III
Results of the Analysis in Relation to the Forensic Questions

Forensic questions	Corresponding identified metadata
Who	User accounts and cron-jobs
Where	Files and folders structure
When	Timestamps of the files and log-files
What	Log files within the *etc* folder
How	Configuration files (*.conf* and *.profile* extension
Why	Can not be answered using the collected metadata

B. Specific characteristics of digital forensics for the automotive sector

In Section IV, several general metadata characteristics were identified. Some of which are specific to the automotive sector. These were also listed but not elaborated on.

The analysis revealed several metadata features that are specific to ADF. One example is the distribution of timestamps. Vehicles, unlike smartphones or personal computers, are cyber-physical systems. Therefore, they interact with the physical outside world. This leads to safety requirements and regulations. Consequently, updates must undergo in-depths testing

 ISBN: 978-1-68558-007-0

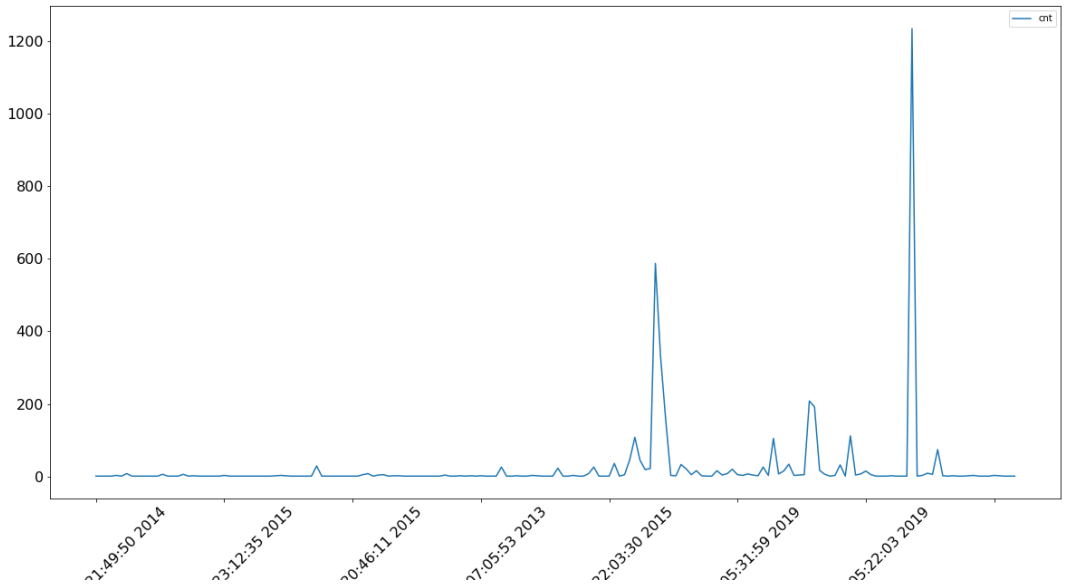

Figure 2. Timestamp of the files within the Tesla autopilot

and certification prior to roll-out. An update must ensure that it does not affect safety-critical systems such as brakes and airbags. This could be a reason for the distribution of timestamps. Tesla could update its autopilot in larger releases compared to small update cycles as known from common IT systems. This allows the manufacturer to verify and certify the update for use in vehicles in the field. Unfortunately, we cannot verify this assumption based on the available information.

As can be seen in Table I, *.so* is the most common extension. Thus, the Tesla autopilot uses a lot of shared libraries. With the use of shared libraries, the behavior of different services becomes comparable. Shared libraries store similar logs and perform related digital events. Hence, using shared libraries is a valuable autopilot feature for DF and penetration testing. In penetration testing, a vulnerability in a shared library can be used to exploit multiple services that use the *.so* file.

Magnet AXIOM identified several user accounts. Most are common to Linux Operating System (OS). However, some are specific to automotive. Two user accounts are named *cantx* and *canrx*. Both refer to the onboard CAN bus protocol. In addition, several user accounts in the file system snapshot refer to cyber-physical systems, e.g., *temperature_monitor*, *roadestimator*, *drivermonitor*, and *rainlightsensing*. Monitoring and safety-related user accounts are also part of the autopilot. The *dash_cam*, *camera*, *backup_camera*, *vision*, and *gps* are examples. Further research on these services for ADF-specific data classes [4] could be valuable.

As a result, several vehicle-specific DF features could be identified within the metadata of the file system of a Tesla autopilot snapshot. Therefore, we can confirm our hypothesis that the file system of the Tesla autopilot contains metadata relevant to answering forensic questions in ADF investigations.

VI. Evaluation

This Section discusses the forensic soundness of the data acquisition, the usability of the identified characteristics, as well as limits and assumptions of the investigation.

A. Forensic soundness

Forensic soundness is the degree of correctness, atomicity, and integrity in memory acquisitions [7]. The definitions of these three attributes were revised by Ottmann et al. in [8] to allow for literal usability. Snapshots that satisfy integrity also satisfy atomicity and correctness [8]. SquashFS is a read-only file system, and we used a write blocker during collection. Since we performed a chip-off, the memory is *frozen* at time t when we removed the chip from the ECU. Thus, the integrity of the acquired snapshot is guaranteed.

B. Usability in automotive digital forensic investigations

We have published our custom Python tool on GitHub [3]. Therefore, the results can be replicated on other Tesla autopilot snapshots. The identified metadata characteristics are valuable for future research. This is especially true for the vehicle-specific characteristics mentioned in Section V-B. Future studies and research can use the information obtained in this article.

C. Limits and assumptions

We assume that the timestamps were not tampered while the autopilot was running. Furthermore, we assume that the system clock is correct. Otherwise, the timestamp analysis could not be conducted in the presented way [26]. The highlighted ADF-specific characteristics are specific to the analyzed Tesla autopilot. However, due to the reuse of hardware and software

in modern vehicles, those characteristics will be helpful in future investigations.

VII. Conclusion and future work

In this article, we investigated the properties of metadata in modern vehicles. We focused on a Tesla autopilot hardware version 2.0 ADF investigation included the collection of data within the autopilot ECU using a chip-off. Analysis of the collected data was performed using two approaches. First, with a self-written Python tool. Second, with Magnet AXIOM, a sophisticated DF tool.

The analysis captured files and directories, file extensions, timestamps, user accounts, media data (e.g., audio), documents in the form of *.cvs*, *.txt*, and *.pdf* files, image files, and general file system information, e.g., that the image was created with buildroot. The most popular extensions were *.so*, *.0*, and *.crt*. We found that the most commonly used timestamp was July 19, 2019.

Vehicle-specific metadata was also identified during the investigation. This includes cyber-physical system-specific user accounts such as *temperature_monitor*, *visualizer*, *legacyvehicle*, *drivermonitor*, *gps*, and *hermes*. In addition, security-related user accounts were captured. Examples include *dash_cam*, *camera*, *backup_camera*, *vision*, and *gps*.

The investigation revealed several DF features that allow answering forensic questions in ADF: *who*, *where*, *when*, *what*, and *how*. Questions regarding "*why*" cannot be answered with the collected metadata.

The results highlighted in this paper are valuable for future studies of the Tesla autopilot ECU and modern vehicles in general. Future work will focus on the file system of other components of the vehicle ecosystem and on refining the analysis methods. In addition, future work will focus on newer hardware versions of the Tesla autopilot.

References

[1] Massachusetts Institute of Technology, "*Advanced Vehicle Technology (AVT) Consortium*,", online, https://agelab.mit.edu/avt, (accessed: 20.09.2022)

[2] L. Fridman, "*Tesla Vehicle Deliveries and Autopilot Mileage Statistics*," online, https://lexfridman.com/tesla-autopilot-miles-and-vehicles/, (accessed: 20.09.2022)

[3] K. Gomez Buquerin, "*Tesla autopilot Jupyter Notebook GitHub repository*," online https://github.com/k-gomez/telsa-ap-analysis, (accessed: 20.09.2022)

[4] K. Gomez Buquerin, C. Corbett, and H.-J. Hof, "*Structured methodology and survey to evaluate data completeness in automotive digital forensics*," 19^{th} escar Europe : The World's Leading Automotive Cyber Security Conference (Conferencepublication), pp. 52-67, 2021

[5] A. Hupp, "*Python-magic GitHub repository*," online, https://github.com/ahupp/python-magic, (accessed: 20.09.2022)

[6] D. Jacobs, K.-K. Raymond Choo, M.-T. Kechadi, and N.-A. Le-Khac, "*Volkswagen Car Entertainment System Forensics*," 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 699-705, 2017

[7] S. Vömel and F. Freiling, "*Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisition*," Digital Investigation, Vol. 9, No. 2, Elsevier BV, pp. 125-137, 2012

[8] J. Ottmann, F. Breitinger, and F. Freiling, "*Defining Atomicity (and Integrity) for Snapshots of Storage in ForensicComputing*," Proceedings of the Digital Forensics Research Conference Europe (DFRWS EU), 2022

[9] Keen Security Labs, "*Experimental Security Research of Tesla Autopilot*," online, https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf, (accessed: 20.09.2022)

[10] S. Dent, "*The Dutch government claims it can decrypt Tesla's hidden driving data*," engadget, online, https://www.engadget.com/a-dutch-government-lab-has-decoded-teslas-driving-data-for-the-first-time-085709633.html, (accessed: 20.09.2022)

[11] T. Simonite, "*Tesla's New Chip Holds the Key to 'Full Self-Driving'*," Wired, online, https://www.wired.com/story/teslas-new-chip-holds-key-full-self-driving/, (accessed: 20.09.2022)

[12] V. Tabora, "*Tesla Enhanced Autopilot Overview — L2 Self Driving HW2*," Medium, online, https://medium.com/self-driving-cars/tesla-enhanced-autopilot-overview-l2-self-driving-hw2-54f09fed11f1, (accessed: 20.09.2022)

[13] B. Erwin, "*The Ultimate Guide to Tesla Autopilot*," Current Automotive, online, https://www.currentautomotive.com/the-ultimate-guide-to-tesla-autopilot/, (accessed: 20.09.2022)

[14] K. Gomez Buquerin, C. Corbett, and H.-J. Hof, "*A generalized approach to automotive forensics*," Forensic Science International: Digital Investigation, Vol. 36, p. 301111, 2021

[15] B. D. Carrier, "*File System Forensic Analysis*," Addison-Wesley, 2005

[16] Keen Security Labs, "*Over-the-air: How we remotely compromised the Gateway, BCM, and Autopilot ECUs of Tesla Cars*," Black Hat Security Conference, 2018

[17] Keen Security Labs, "*Free-fall: Hacking Tesla from Wireless to CAN Bus*," Black Hat Security Conference, 2017

[18] S. Ebbers, F. Ising, C. Saatjohann, and S. Schinzel, "*Grand Theft App: Digital Forensics of Vehicle Assistant Apps*," CoRR, 2021

[19] K. Gomez Buquerin, D. Bayerl, and H.-J. Hof, "*Überwachung in modernen Fahrzeugen*," Datenschutz und Datensicherheit - DuD , Vol. 45, No. 6, Springer Science and Business Media LLC, pp. 399-403, 2021

[20] T. Rice, "*Hacking my Tesla Model 3 - Security Overview*," online, https://fn.lc/post/tesla-model-3/, (accessed: 20.09.2022)

[21] Tesla, "*Tesla Q1 2021 Vehicle Production & Deliveries*," online, https://ir.tesla.com/press-release/tesla-q1-2021-vehicle-production-deliveries, (accessed: 20.09.2022)

[22] Tesla, "*Tesla Q2 2021 Vehicle Production & Deliveries*," online, https://ir.tesla.com/press-release/tesla-q2-2021-vehicle-production-deliveries, (accessed: 20.09.2022)

[23] Tesla, "*Tesla Q3 2021 Vehicle Production & Deliveries*," online, https://ir.tesla.com/press-release/tesla-q3-2021-vehicle-production-deliveries, (accessed: 20.09.2022)

[24] Tesla, "*Tesla Q4 2021 Vehicle Production & Deliveries*," online, https://ir.tesla.com/press-release/tesla-q4-2021-vehicle-production-deliveries, (accessed: 20.09.2022)

[25] C. Isidore and P. Valdes-Dapena, "*Tesla is under investigation because its cars keep hitting emergency vehicles*," online, https://edition.cnn.com/2021/08/16/business/tesla-autopilot-federal-safety-probe/index.html, (accessed: 20.09.2022)

[26] F. Buchholz and E. Spafford, "*On the role of file system metadata in digital forensics*," Digital Investigation, Vol. 1, No. 4, Elsevier BV, pp. 298-309, 2004

 ISBN: 978-1-68558-007-0