Lehrstuhl für Informatik 1
Friedrich-Alexander-
Universität
Erlangen-Nürnberg

MASTER THESIS

Analyzing the Relevance of Forensic Techniques in Comfort Electronics within the Automotive Sector: A Case Study Exploration

Christian Körber

Erlangen, September 10, 2024

Examiner: Prof. Dr.-Ing. Felix Freiling
Advisor: Kevin Mayer

Abstract

This thesis investigates the impact of digital forensics on comfort electronics in the automotive environment. Previously, this kind of research was only performed on the automotive environment in general or other areas of automotive electronics, but not specifically in the field of comfort electronics. This gap is filled by performing first a general analysis of the forensic readiness in comfort electronics, followed by a case study, where the theoretical approach is tested on a real world project. This leads to the conclusion, that digital forensics is relevant for multiple stakeholder for different reasons and that this topic will even get more relevant in the future.

Zusammenfassung

Diese Arbeit untersucht die Auswirkungen der digitalen Forensik auf die Komfortelektronik im Automobilbereich. Bisher wurde diese Art von Forschung nur im Automobilbereich im Allgemeinen oder in anderen Bereichen der Automobilelektronik durchgeführt, aber nicht speziell im Bereich der Komfortelektronik. Diese Lücke wird geschlossen, indem zunächst eine allgemeine Analyse der forensischen Bereitschaft in der Komfortelektronik durchgeführt wird, gefolgt von einer Fallstudie, in der der theoretische Ansatz an einem realen Projekt getestet wird. Dies führt zu der Schlussfolgerung, dass digitale Forensik aus verschiedenen Gründen für eine Vielzahl von Stakeholdern relevant ist und dass dieses Thema in Zukunft noch an Bedeutung gewinnen wird.

Contents

1 INTRODUCTION

The introduction of this thesis is structured to provide a comprehensive foundation for understanding the scope and objectives, of the research presented. Firstly, the motivation outlines the incentive behind the research, highlighting the relevance and importance of the topic. This section explains why the study is significant, setting the stage for further investigation. Secondly, the task section describes the specific challenges and questions the research aims to address. It sets the scope of the study and presents the research questions as well as the corresponding evaluation criteria. Following this, the research goals are shown. Afterwards, the structure of the thesis is outlined, giving an overview how the work is organized, and summarizing the content of each chapter to help the reader understand the flow of the research and the key areas covered.

1.1. Motivation

In our fast moving world today, the automotive industry must build vehicles that not only are functional, but also comfortable and safe. Adding comfort electronics has changed the way we experience cars. However, these complex systems require new approaches to ensure their reliability and safety. This is where cyber security technologies come into play. At first, digital forensics focused on computer related investigations but has since

expanded to include all devices that can store, handle, and send digital data [19]. This broader scope includes a range of technologies and methods designed to uncover and analyze digital evidence. Comfort electronics refer to the various systems and functions in modern vehicles aimed at enhancing comfort and convenience. These systems are unnecessary for the vehicle to drive. They highly improve passenger experience and satisfaction [26]. They are designed to work in addition to the primary vehicle functions, ensuring that the vehicle remains operational even if these comfort features are temporarily unavailable. The intersection of digital forensics and comfort electronics involves examining how these advanced systems can be investigated to provide insights into vehicle usage, connectivity, and user interactions. Comfort systems generate a wealth of data that can reveal detailed information about how they were used and, by extension, about the individuals using them. Understanding these systems from a forensic perspective is essential for ensuring their security and reliability, especially as they become increasingly integral to modern vehicles.

The primary objective of this thesis is to fill a gap in existing research about digital forensics in automotive comfort electronics. While some papers investigate digital forensic in the automotive industry in general, there is a lack of publications about comfort electronics specifically. So, this master's thesis aims to thoroughly analyze the relevance and application of forensic techniques in context of automotive comfort systems. To achieve this, the thesis will start with a general analysis of digital forensics in comfort electronics to provide insights into how forensic principles and methods relate to and can be used in this specialized field. After this theoretical exploration, the thesis will include a practical case study to apply these forensic concepts to a real world scenario. By integrating both theoretical and practical perspectives, this thesis aims to offer a comprehensive overview of the importance and implementation of digital forensics in this emerging field.

1.2. Research Questions

The research questions guiding this thesis are chosen to explore the role and impact of digital forensics within the field of automotive comfort electronics. These questions aim to address the key aspects of forensic relevance, current practices and potential benefits for stakeholders, especially suppliers.

1. Hold automotive comfort systems relevant data for digital forensics investigations?

This question seeks to determine whether digital forensics has a role in the scope of automotive comfort electronics. It will investigate, if these systems store or process data in a way that forensic analysis provides relevant new insights.

2. What is the current state of support for digital forensic activities in the automotive comfort electronic environment?

The goal is to investigate the existing support for forensic activities in the automotive comfort electronics sector by exploring whether there are established standards, norms, and practices related to forensic analysis and whether relevant expertise is available.

3. Which processes and tools can be used in automotive comfort digital forensics to acquire and analyze relevant data?

This question focuses on identifying the specific processes and tools that are effective for data acquisition and analysis in automotive comfort electronics. It will involve comparing various methodologies and technologies to determine their applicability and effectiveness in forensic investigations.

4. How can a comfort electronics supplier benefit from automotive digital forensics?

The aim is to explore the potential advantages that automotive comfort electronics suppliers can gain from using digital forensics in their development and operational processes. It will examine how forensic practices can improve product development, security, and overall business benefits.

1.3. Goals

The goals of the thesis are directly related to the research questions, with each question targeting a specific objective within the broader investigation. (i) The first goal is to asses whether and how digital forensic is relevant in the context of automotive comfort electronics. This includes identifying the types of data stored and processed within comfort electronics that could be relevant for a forensic analysis. The research will also explore whether comfort electronic systems have issues that can be effectively addressed through digital forensic techniques. The expected outcome is confirmation that digital forensics is generally applicable, although its relevance depends on the specific application. (ii) The second goal is to examine if there are existing standards, norms or guidelines that support forensic activities in automotive comfort electronics. This includes evaluating how development and technologies consider forensic and analyzing the availability of professionals with expertise. The research is expected to showcase the growing presence of forensic considerations, supported by emerging regulations like United Nations Economic Commission for Europe (UNECE) R155 and an increasing availability of forensic experts. (iii) The third goal is to identify and evaluate the processes and tools currently available for extracting and analyzing forensic data in automotive comfort electronics. By comparing the effectiveness of different methods and tools, best practices are shown. The anticipated result is the identification of adaptable process models for automotive forensics that can be applied to comfort electronics as well. (iv) The final goal is to explore the potential benefits that comfort electronic suppliers can gain from implementing forensic techniques and processes. This is done by evaluating how forensic analysis enhance

product development, quality assurance and security standards. It will also be determined whether forensic insights can be used to gain a competitive advantage and improve customer satisfaction. Supposedly, forensic considerations will help suppliers to protect their firmware, support investigations if needed and potentially provide a medium-term competitive edge as this field emerges.

1.4. Outline

This thesis is structured into five main chapters to answer the research questions defined in the introduction.

Chapter1 provides an introduction to the topic, outlining the motivation behind the study, the research questions, the goals, the methods used, and the criteria for evaluating the thesis.

Chapter 2 gives the background and related work. This chapter discusses the fundamentals of comfort electronics, digital forensics, and automotive protocols, providing a theoretical foundation for the study. Additionally, it reviews existing literature to position the research within the broader academic and industry context.

Chapter 3 presents a detailed analysis of comfort electronics, focusing on the structure, software, hardware, and communication requirements. This chapter also examines the relevance of digital forensics in this domain, highlighting its necessity and the potential impacts on both users and manufacturers. The analysis concludes with a market overview that assesses forensic readiness, data acquisition, and data analysis capabilities within the automotive industry.

Chapter 4 introduces a case study conducted on a project at APAG CoSyst, which serves as a practical application of the concepts discussed in previous chapters. This chapter details the setup, implementation, and results of the case study, providing concrete examples of how digital forensics can be applied in comfort electronics.

Chapter 5 concludes the thesis by discussing the findings, verifying the evaluation criteria, and offering contributions and insights for future work. This chapter also outlines potential areas for further research and suggests ways in which the industry can advance in the integration of digital forensics within automotive comfort electronics.

2 Background and Related Work

2.1. Comfort Electronics

While there are different domains in the vehicle, like body electronics, chassis electronics, infotainment and others, with different goals, comfort electronics aims to enhance the comfort experience of the driver and other passengers in the car [22]. The collection of Figure 2.9 showcases various examples of comfort electronics used in modern automotive systems, highlighting the diversity and complexity of these components. Figure 2.1 shows the steering wheel adjustment module, an essential element for enhancing driver comfort by allowing precise adjustments of the steering wheel position. Figure 2.2 displays the door control panel, which is responsible for managing functions such as window operations and mirror adjustments. The overhead console, shown in Figure 2.3, typically integrates various controls and displays, contributing to the overall user experience within the vehicle. The motor control unit in Figure 2.4, plays a critical role in managing the various electronic systems by ensuring their efficient operation. Figure 2.5 highlights the screen control unit, which controls the display systems within the vehicle, offering a user friendly interface for infotainment and navigation features. The multi functional gateway, as shown in Figure 2.6, serves as a communication hub, linking different electronic systems within the vehicle to ensure seamless operation. In Figure 2.7, the electronic air

vents are depicted, showing a component that enhances climate control within the vehicle, allowing for precise adjustment of airflow and temperature. Finally, Figure 2.8 presents the logo illumination, that adds to the aesthetic appeal of the vehicle and also serves as a branding element, often illuminated for enhanced visibility and style.

Figure 2.1.: Steering wheel adjustment

Figure 2.2.: Door control panel

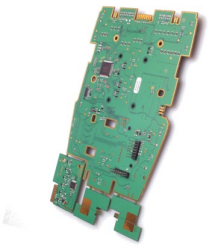

Figure 2.3.: Overhead console

Figure 2.4.: motor control unit

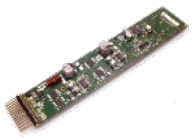

Figure 2.5.: Screen control unit

Figure 2.6.: Multi functional gateway

Figure 2.7.: Electronic air vents

Figure 2.8.: Logo illumination

Figure 2.9.: Examples of comfort electronics

2.2. Digital Forensics

This section introduces the basic concepts of digital forensics. First the general concepts and uses of digital forensics will be presented. Afterwards, the use case of digital forensics specifically in the automotive environment will be presented. For the structure in this subsection, the literature review by Strandberg et al. [30] was used, which also served as

main reference to find relevant sources for this topic released between 2006 and 2021. Finally, some basic forensic concepts, which get used later on, are introduced.

2.2.1. Digital Forensics in general

Historically starting with computer forensic, digital forensic was derived to not only focus on computer systems but rather all digital devices [27]. Digital forensic activities today include not only computers, but also any digital device that processes, transmits, or stores data [30]. The goal of forensics in general is to answer the following questions [5]:

- What happened?
- Where did it happen?
- When did it happen?
- How did it happen?
- Who did it?
- What can be done to prevent it from happening again?

To answer these questions, the task of a forensic investigation includes collecting data, analyzing it and finally reporting the findings [16]. To properly answer these questions, several standard forensic requirements must be followed in the investigation process [5]:

- Acceptance: Use of generally accepted methodologies by experts
- Credibility: Demonstrating the correctness and robustness of new methods
- Repeatability: Third parties must obtain the same results when using the same tools and methods
- Integrity: Traces must not be altered during the investigation
- Cause and effect: There must be a logical link between the trace and the inferred events
- Documentation: Each step must be adequately documented

Although these specifications help perform a forensic investigation, for an extensive result, it is still necessary to follow a structured process model [27]. There are multiple proposed process models, but they are usually composed similarly, only varying in details. For example, the following phases were identified in a literature review: identification, preparation, analysis, documentation, and presentation [3]. The identification phase involves recognizing and defining the scope of the forensic investigation, including the relevant data sources and potential evidence. In the preparation phase, the necessary tools, resources and environment are prepared, to ensure that the investigation can proceed without contamination or loss of data. During the analysis phase, the collected data

are carefully examined to uncover relevant information and potential evidence. The documentation then records all findings and methodologies used, providing a clear trail for review or legal purposes. Finally, the presentation phase involves compiling and presenting the results in a way that is understandable and useful to stakeholders, such as legal teams or other investigators.

2.2.2. Automotive Digital Forensics

Modern vehicles, like other smart devices, store extensive data and can connect to the internet, often revealing more about their owners than smartphones. As a newer branch of digital forensics, car forensics is gaining importance in criminal investigations, shifting the focus from traditional physical evidence to valuable digital data now stored in vehicles [29].

Challenges

These new tasks come with some unique challenges that computer forensics does not address. Those include low storage capacity in the Electronic Control Unit (ECU), no supervision in certain bus systems, mass storage, and memory often part of the micro controller and difficult to access, and lack of standardization of components [1]. Those are explained in detail in the following paragraphs.

An important challenge is the limited storage capacity in ECUs. ECUs, which are designed to manage specific vehicle functions such as engine control or brake systems, often have limited memory space. This limitation can create problems during forensic investigations, as important data, such as event logs or diagnostic trouble codes, may be overwritten or lost due to restricted storage. For example, in the case of a collision investigation, crucial evidence could be irretrievably lost if relevant data has already been overwritten due to the limited capacity of the ECU.

Another challenge is the lack of supervision in certain bus systems within vehicles. These bus systems, such as the Controller Area Network (CAN) bus, allow communication between different ECUs. However, not all of these systems are supervised or monitored, making it difficult to track data flow or detect unauthorized access. For example, an attacker could exploit this lack of supervision in the CAN bus to inject malicious messages, altering the vehicle's behaviour without leaving clear traces for forensic analysis. This vulnerability presents a significant obstacle for investigators trying to piece together the events that led to an incident.

Another key challenge in vehicle forensics is the fact that mass storage and memory are often integrated into the micro controller, making them difficult to access. Unlike traditional computing devices where storage components like hard drives or SSDs are separate

and more easily accessible, in vehicles, critical data is often embedded directly into the micro controller. This integration complicates the forensic process because specialized tools and techniques are required to extract data without damaging the micro controller or altering the data. For example, accessing crash data stored in an airbag control module may require special handling and specific hardware interfaces, which not all forensic investigators can access.

Finally, the lack of standardization of vehicle components is a great challenge. Different manufacturers and even different models from the same manufacturer may use varying types of ECUs, communication protocols, and storage systems. This diversity means that forensic investigators must be familiar with a wide range of technologies and have access to specialized tools for each type of vehicle. For example, a forensic method that works on one brand of vehicles may be completely ineffective on another due to differences in how data is stored or transmitted. This lack of standardization complicates the forensic process and increases the time and resources needed to perform investigations.

Stakeholder

Understanding the roles and scenarios associated with various stakeholders is crucial in the field of automotive forensics. Table 2.1 shows the key stakeholders and outlines typical scenarios they might face.

Insurance Companies have to assess if any modifications to the hardware or software of a vehicle, such as performance tuning, have been performed and if they could potentially influence an incident. Additionally, they investigate if third party alterations or tampering may have played a role in the event. Their involvement is essential for determining liability and ensuring that claims are handled appropriately.

Legal Authorities include entities such as law enforcement agencies, legislators, and courts. Their primary concern is to verify whether vehicles and their manufacturers comply with current legal and regulatory standards. They also assess whether manufacturers have implemented up to date technologies and practices to prevent, monitor, and address potential security threats. This role is critical in ensuring that legal and safety standards are maintained.

Original Equipment Manufacturers (OEMs) are responsible for investigating potential security breaches or misuse of their components. They must also ensure that their products meet regulatory requirements, including data protection and privacy standards. This involves examining if their vehicles contain specific types of data and they adhere to the necessary regulations.

Component Suppliers play a vital role in analyzing and demonstrating issues related to their supplied parts. This includes investigating malfunctions, unauthorized modifications, or misuse of their components. Furthermore, suppliers need to ensure that their

intellectual property is protected from forensic investigations, safeguarding their proprietary technologies and designs.

Vehicle Owners and Customers are directly affected by vehicle malfunctions or issues with related services. They need to determine liability in cases of malfunction and provide evidence of any unusual behavior observed in their vehicles. This group's perspective is crucial for understanding the practical impacts of forensics on end-users.

Stakeholder	Scenario Examples
Insurance Company	Verify whether any modifications have been made to the vehicle's hardware or software (e.g., performance enhancements).
	Investigate whether third party alterations or tampering could have influenced the incident.
Legal Authorities	Check if the vehicle and its manufacturer comply with existing legal and regulatory requirements.
	Evaluate whether the manufacturer has incorporated up to date technologies and practices to address and monitor potential security threats.
OEM	Examine and reproduce potential security issues or misuse related to vehicle components.
	Verify if the vehicle includes certain types of data and adheres to regulatory requirements (e.g., data protection).
Component Supplier	Investigate and demonstrate issues like malfunctions or unauthorized changes in their components.
	Ensure that their intellectual property is protected from forensic investigations.
Vehicle Owner/Customer	Determine who is responsible in case of vehicle malfunctions or issues with related services.
	Provide evidence of any unusual behavior observed in the vehicle or its services.

Table 2.1.: Different stakeholders in a forensic investigation. Adapted from [15]

2.2.3. Concepts

In this section, some basic cyber security concepts are explained, which are then used during the analysis. This includes sniffing where data is extracted by listening to a bus network and brute force attacks, a trial and error approach to extract data where insight knowledge is required.

Sniffing

Sniffing describes the act of monitoring and capturing data from a network [14]. This is done without interacting with the participants of the communication itself but rather just listening to the network as shown in Figure 2.10. This can be done with pretty much any bus or switch network, as the attack is applied on the data link layer of the ISO/OSI reference model [2]. Therefore, this attack affects all the upper layer as well.

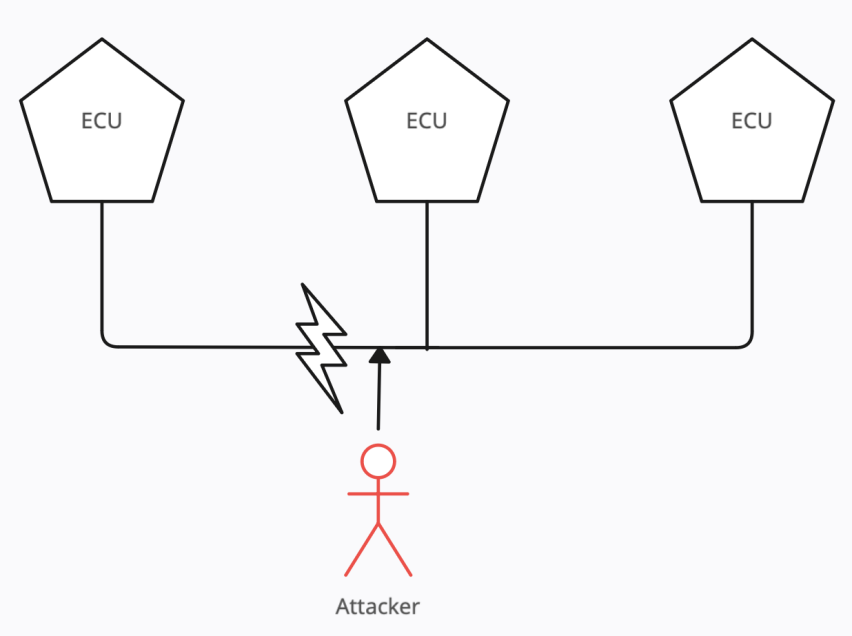

Figure 2.10.: Visualization of a sniffing attack

Brute Force Attack

Brute force attacks are most known for the attempt to hack a password, which is done by just trying out all possible combinations [8]. This strategy can be adapted to all circumstances where multiple inputs are possible, and the correct one is unknown. This trial and error method works well with only a small number of possibilities but scales exponentially.

2.3. Automotive Protocols

In this section, the two most important automotive protocols which are used in this analysis are introduced. Local Interconnect Network (LIN) is a bus network protocol and Unified Diagnostic Services (UDS) provides diagnostic services.

2.3.1. LIN

LIN is a transmission protocol used in the automotive environment with the goal of reducing the cost of transmitting data between multiple nodes [7]. This is achieved by using only a one wire connection where the data is sent and the vehicle's chassis as the ground wire [12]. Another cost saving aspect is the structure of a LIN setup. As shown in Figure 2.11, is there only one master ECU on each LIN network. Only this master is responsible for any timing and schedules on the network, compared to CAN, where every ECU needs their own clock [12].

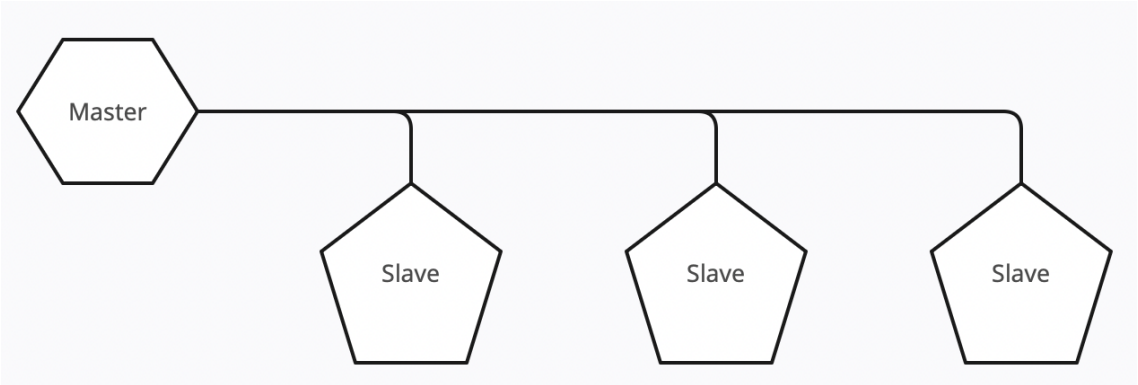

Figure 2.11.: Visualization of the master slave principle of LIN

A message on the LIN bus network is called a LIN frame, which structure is displayed in Figure 2.12. The header is always sent by the master, with either a response by the master itself, if any instructions have to be communicated or a response by the slave. The according case is transmitted through the protected identifier field. This ID indicates the content of the message and thereby only implicitly addresses certain slaves. The break field and sync byte field are only relevant for synchronizing, so they will not be explained in detail here.

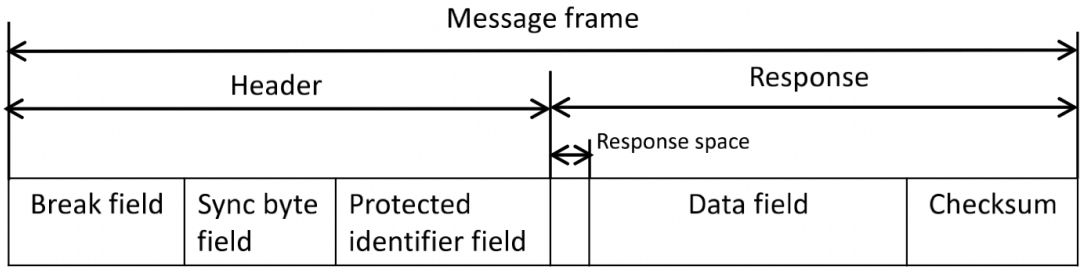

Figure 2.12.: Structure of a LIN message frame. Figure taken from [32]

2.3.2. UDS

Integrated into the bus network, UDS was created to standardize diagnostics. Though originally designed for CAN, UDS is now implemented on various other bus systems, including LIN [9]. In LIN, the standardized header ID is 0x3C for a diagnostic request and 0x3D for a diagnostic response. The data section of the LIN frame is subsequently utilized to relay the UDS message. If needed, the LIN protocol manages cases where the UDS message exceeds the data field of the LIN frame [31]. ISO 14229–1 specifies 27 UDS Service Identifiers (SIDs), each representing a unique diagnostic service [9]. These are all displayed in Figure 2.13 on the left side in orange. They fall into various categories such as communication management, data transmission, and diagnostic troubleshooting. The positive response SID is shown in green beside it, and 0x7F indicates a negative response code.

UDS service identifiers (SIDs)

	UDS SID (request)	UDS SID (response)	Service	Details
Diagnostic and Communications Management	0x10	0x50	Diagnostic Session Control	Control which UDS services are available
	0x11	0x51	ECU Reset	Reset the ECU (“hard reset”, “key off”, “soft reset”)
	0x27	0x67	Security Access	Enable use of security-critical services via authentication
	0x28	0x68	Communication Control	Turn sending/receiving of messages on/off in the ECU
	0x29	0x69	Authentication	Enable more advanced authentication vs. 0x27 (PKI based exchange)
	0x3E	0x7E	Tester Present	Send a “heartbeat” periodically to remain in the current session
	0x83	0xC3	Access Timing Parameters	View/modify timing parameters used in client/server communication
	0x84	0xC4	Secured Data Transmission	Send encrypted data via ISO 15764 (Extended Data Link Security)
	0x85	0xC5	Control DTC Settings	Enable/disable detection of errors (e.g. used during diagnostics)
	0x86	0xC6	Response On Event	Request that an ECU processes a service request if an event happens
	0x87	0xC7	Link Control	Set the baud rate for diagnostic access
Data Transmission	0x22	0x62	Read Data By Identifier	Read data from targeted ECU - e.g. VIN, sensor data values etc.
	0x23	0x63	Read Memory By Address	Read data from physical memory (e.g. to understand software behavior)
	0x24	0x64	Read Scaling Data By Identifier	Read information about how to scale data identifiers
	0x2A	0x6A	Read Data By Identifier Periodic	Request ECU to broadcast sensor data at slow/medium/fast/stop rate
	0x2C	0x6C	Dynamically Define Data Identifier	Define data parameter for use in 0x22 or 0x2A dynamically
	0x2E	0x6E	Write Data By Identifier	Program specific variables determined by data parameters
	0x3D	0x7D	Write Memory By Address	Write information to the ECU’s memory
DTCs	0x14	0x54	Clear Diagnostic Information	Delete stored DTCs
	0x19	0x59	Read DTC Information	Read stored DTCs, as well as related information
	0x2F	0x6F	Input Output Control By Identifier	Gain control over ECU analog/digital inputs/outputs
	0x31	0x71	Routine Control	Initiate/stop routines (e.g. self-testing, erasing of flash memory)
Upload/ Download	0x34	0x74	Request Download	Start request to add software/data to ECU (incl. location/size)
	0x35	0x75	Request Upload	Start request to read software/data from ECU (incl. location/size)
	0x36	0x76	Transfer Data	Perform actual transfer of data following use of 0x74/0x75
	0x37	0x77	Request Transfer Exit	Stop the transfer of data
	0x38	0x78	Request File Transfer	Perform a file download/upload to/from the ECU
		0x7F	Negative Response	Sent with a Negative Response Code when a request cannot be handled

Figure 2.13.: List of all SIDs in UDS. Figure taken from [11]

The transmission is illustrated in Figure 2.14. The tester sends a request containing a SID and some data. For instance, the SID code 0x22 is selected, representing Read Data by Identifier (RDbID), along with additional data of 0x01. This indicates the intent to retrieve some data from ECU, which is internally stored as ID 0x01. If the ECU contains a value with this ID, 0x62 plus the value of ID 0x01 will be returned, resulting in a message like 0x62 12 34. If no data is stored or the security requirements for a response

are not met, the ECU will return a negative response, such as 0x7F 0x22 09, where 0x7F is the negative response indicator, 0x22 is the SID, and 0x09 explains why the request was denied. Alternatively, the ECU might not respond at all, depending on its programming.

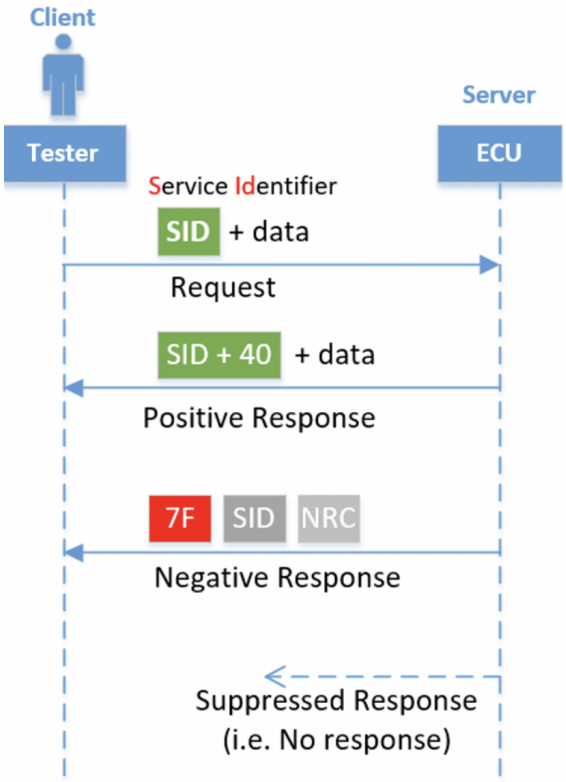

Figure 2.14.: Example communication in UDS. Figure taken from [10]

2.4. Related Work

Since no actual publications on the topic of digital forensics in automotive comfort electronics were found, some related topics will be listed in this section, grouped by the main problem they are addressing. The categories are (i) introduction and basics of automotive digital forensics, (ii) technical solutions and tools (iii) specific challenges and case studies (iv) forensic readiness and company strategies.

Introduction and Basics of automotive Digital Forensics

The paper "A Generalized Approach to Automotive Forensics" investigates the viability of implementing digital forensics in modern vehicles [15]. It emphasizes the issues

arising from the complexity of current automotive systems and assesses existing forensic methodologies. The study suggests a generalized forensic process including forensic readiness, data acquisition, analysis, and documentation, and illustrates its use with common diagnostic tools. Although the research indicates that forensic analysis is achievable, it points out limitations such as the absence of tamper resistant data storage and the diversity of technologies among vehicles, recommending that future research should aim at improving forensic tools and creating secure data storage systems. The paper "Vehicle Forensics" discusses how modern vehicles, equipped with advanced technologies like GPS, Bluetooth, Wi-Fi, and infotainment systems, have become significant sources of digital evidence in criminal investigations [4]. It highlights how these embedded systems store data such as location history, call logs, and media, which investigators can use to solve cases involving vehicles. The paper emphasizes the growing field of vehicular forensics, focusing on both automotive and drone forensics, and explores the tools and techniques used for analyzing digital evidence from these systems. It also addresses the challenges investigators face due to the increasing complexity of vehicle technology and the need for more advanced forensic tools to stay ahead of evolving criminal methods. The paper "Actual Issues of Modern Digital Vehicle Forensic" addresses the growing importance of digital forensics in the automotive industry due to the integration of electronic control units, digitization, and telematics in modern vehicles [25]. With vehicles now processing and storing large amounts of operational and driver data, they have become valuable sources of digital evidence. The paper highlights the main challenges in this emerging field, such as the lack of standardization in data interfaces and storage systems, and the need for advanced, user-friendly forensic tools. It also emphasizes the need for specialized forensic engineers and methodologies to handle the complexity of digital vehicle forensics as technology continues to advance, especially with the rise of autonomous and electric vehicles.

Technical Solutions and Tools

The paper "READ: Reverse Engineering of Automotive Data Frames" introduces a new algorithm called READ, designed to automatically reverse engineer and classify signals from unknown CAN bus messages in vehicles [21]. The challenge addressed by READ is the lack of public specifications for CAN messages, which complicates security analysis and forensics in modern vehicles. The proposed algorithm improves previous methods by extracting and labeling more signals with greater accuracy and faster execution. Experimental results demonstrate READ's effectiveness in analyzing real vehicle CAN traffic, providing a valuable tool for researchers and forensic experts to better understand and secure in vehicle networks against cyber threats. The paper "Log your car: The non invasive vehicle forensics" addresses the growing importance of digital forensics in automotive systems, which use multiple ECUs to support modern connected and intelligent vehicle technologies [20]. It highlights the potential of digital evidence from these

ECUs for crash investigations, insurance claims, and crime analysis. The paper introduces DiaLOG, a diagnostic application for smartphones that utilizes a secure protocol to communicate forensic data to a secure cloud storage. The proposed system ensures data integrity, security, and privacy, with performance measured using formal analysis tools like Scyther and CasperFDR. The paper concludes that the DiaLOG application enhances forensic investigations by providing a secure, reliable, and privacy preserving framework for collecting and storing vehicle data. Future work aims to expand the logging features of the DiaLOG application to improve forensic analysis. In their paper, Sladović et al.. delve into the growing field of car forensics, which has become increasingly significant as modern vehicles become more advanced and digitally integrated [29]. The authors discuss the array of data that new vehicles can store, including details on vehicle operation, driver behavior, and interactions with onboard and external systems. They explain the forensic extraction process, highlighting the software and tools used to retrieve data from a car's systems, such as its infotainment and security features. The paper emphasizes the challenges forensic investigators face during data extraction and the potential of car forensics to resolve various types of crimes by analyzing digital evidence from vehicles. The study illustrates how modern cars, equipped with sophisticated systems and connectivity features, serve as crucial sources of evidence in forensic investigations, underscoring the importance of specialized knowledge and tools in this evolving field.

Specific Challenges and Case Studies

In their study, Urquhart et al. conduct a detailed examination of the 2017 Skoda Octavia vRS to explore its cybersecurity vulnerabilities [33]. They highlight how the integration of modern technologies, such as CAN networks and 3G/4G connectivity, has expanded the potential attack surface of vehicles. The research reveals multiple security flaws, including the successful compromise of the key fob rolling code, vulnerabilities within the infotainment system, and weaknesses in the VW Transport Protocol 2.0, which can lead to unauthorized access and modifications of ECU parameters. The paper also discusses the implications of these vulnerabilities for both vehicle security and digital forensics, emphasizing the need for improved protective measures and forensic capabilities in modern vehicles. In their paper, Le-Khac et al. explore the emerging field of smart vehicle forensics, which is increasingly relevant as vehicles become more digitized and integrated with various electronic systems [18]. The authors highlight the shift from traditional forensic methods, which focus on physical evidence, to a more comprehensive approach that includes the analysis of digital data stored in modern vehicles. They discuss the forensic challenges associated with acquiring and analyzing data from different vehicle systems, such as entertainment systems and mobile traffic. Through case studies of Volkswagen, Audi, and BMW vehicles, the paper identifies key sources of forensic artifacts and examines potential tools and methods for data acquisition. The study underscores the need for adaptable forensic strategies and tools to handle the complex and varied data found in con-

temporary vehicles, and suggests future research directions to improve forensic readiness and real time data acquisition capabilities. Shin et al. examine the growing importance of digital forensics in in vehicle infotainment systems, particularly focusing on Android Auto and Apple CarPlay [28]. With vehicles increasingly connected to mobile devices, these systems exchange valuable data that can assist forensic investigations. The authors propose a comprehensive forensic methodology that analyzes four key areas: wireless communication between the cloud and mobile devices, communication between the IVI system and mobile devices, and the internal storage of both the IVI system and the connected mobile device. Through case studies on various IVI systems, they demonstrate how their methodology uncovers useful forensic artifacts, and they develop a tool to automate data collection. The paper highlights the need for future research on more advanced methods, such as analyzing wireless communication structures and retrieving data from chip-off resistant systems, as IVI systems become a key source of digital evidence. Another paper explores the role of modern vehicle infotainment systems in vehicular digital forensics, particularly in the context of crime investigations [17]. Infotainment systems, which interact with drivers and passengers via Bluetooth and WiFi, store data from external devices such as phones and laptops. Extracting information from these systems could provide valuable insights for forensic analysts to determine which data is relevant to law enforcement. The ability to analyze this data could enhance the broader infrastructure of Intelligent Transport System and Vehicular Ad Hoc Networks, making it easier to combat vehicle related crimes. The study also emphasizes the potential of infotainment systems to offer indirect or direct information about the vehicle's end user. Further, it highlights the need for a more developed forensic framework for analyzing data from infotainment systems to enhance law enforcement's ability to reconstruct events, particularly in criminal or accident investigations. The research suggests future work is necessary to create standardized forensic methodologies for different infotainment platforms, especially as vehicle technology continues to evolve. The paper "A Survey on Open Automotive Forensics" addresses the complexities and challenges of conducting forensic investigations within modern automotive systems, which integrate numerous ECUs and sensors. With vehicles increasingly connected through external communication channels, such as Car to X communication, new security vulnerabilities have emerged, making it crucial to have effective forensic processes in place. The study highlights the need to adapt traditional forensic methods from desktop IT to the automotive environment, identifying requirements for tools that can reliably support such investigations. This involves ensuring that data is collected, preserved, and analyzed with integrity, regardless of whether the incident was caused by an error or a malicious attack. The paper underscores the necessity for dedicated forensic tools and methodologies tailored to automotive systems to enhance safety and security in this rapidly evolving field.

Forensic Readiness and Company Strategies

The paper "The Importance of Corporate Forensic Readiness in the Information Security Framework" emphasizes the growing role of forensic readiness as a vital part of corporate information security, extending beyond traditional law enforcement use [24]. It argues that organizations should integrate digital forensic principles into all monitoring and investigation activities, as security incidents and policy breaches can lead to legal challenges at any time. Forensic readiness enhances a company's ability to investigate incidents, assess policy violations, and respond effectively, while also demonstrating that management is taking responsibility for protecting information assets. By embedding forensic practices into the broader security framework, businesses can reduce the impact of security breaches and ensure compliance with regulations. The paper also highlights the need to expand the scope of digital forensics across the entire security domain, posing new challenges for security professionals.

3 ANALYSIS

In this chapter a generic analysis of digital forensic in the automotive comfort electronic environment gets performed. To do this, the relevance of digital forensics in the automotive environment in general is first evaluated and transferred to the comfort electronic sector. Afterwards, a market analysis gets done to evaluate, with the use of different criteria, if and how the comfort electronic sector can support the forensic process. Instead of giving a completely generic view on the basics of automotive digital forensics, this analysis mainly focuses on the aspects of a supplier. As there is only a limited amount of publications about comfort electronics, a short list of questions got put together and different persons of various working time in this field answered them. As the questions were quite simple and simply served to show the basic principles and requirements of comfort electronics, the answers usually were so similar that it is unnecessary to separate them, but rather use them as one answer.

3.1. Structure of Comfort Electronics

The responsibilities of a driver can be divided into three categories [26]. Primary tasks include fundamental activities directly impacting the vehicle control and safe navigation

on the road. This includes navigation, such as selecting the route and planning the timing of the trip, guidance which involves maintaining distance from the vehicle ahead, also managing acceleration, deceleration, and stabilization, which means steering, braking and accelerating. Secondary tasks are related to the operation of the vehicle that do not directly affect the driving itself but are necessary for the functionality of the vehicle. Examples include shifting gears, operating indicators and lights or activating the windshield wipers. Tertiary tasks involve activities related to comfort and the environment inside of the car, which do not directly impact the safety of the driving. These include adjusting the cabin temperature or operating the infotainment system such as the radio or the phone. These categories highlight different level of attention and action a driver must manage simultaneously during a trip. It emphasizes that other than direct controlling the vehicle, other activities are necessary which can burden the driver. While modern assistance systems and driving automation try to minimize primary and secondary tasks, comfort electronics tackles the remaining tertiary tasks. By enhancing those unnecessary but nice to have features, the attention of drivers can focus on more important tasks.

Task	Activity	Examples
Primary Tasks	Navigation	Choosing the route and planning the timing of the trip.
	Guidance	Selecting the driving lane, maintaining safe distance from other vehicles.
	Stabilization	Steering, braking, accelerating.
Secondary Tasks	Operational Controls	Shifting gears, using turn signals, headlights, and windshield wipers.
Tertiary Tasks	Environmental Controls	Adjusting temperature, operating the infotainment system (music, phone calls).

Table 3.1.: Driving tasks while operating a vehicle [26]

3.1.1. General Requirements

Comfort electronics in automobiles have evolved significantly over the years, transitioning from purely mechanical systems to advanced electronic solutions. Historically, features such as power windows, seat adjusters, and steering column adjustments were mechanically operated. Today, these have become electronically controlled, offering enhanced functionalities like seat massage, specialized ventilation, seat heating, climate control, interior lighting or sunroof operations.

While comfort electronics traditionally included infotainment systems, this area has since grown into its own domain due to its complexity and scope. As a result, infotainment is

now often considered separate from comfort electronics.

Another distinction must be made between comfort electronics and safety electronics. For instance, a door control unit might initially be classified as comfort electronics. However, if it becomes responsible for controlling safety critical functions, such as airbag deployment or acting as a gateway for other safety systems, it transitions into the realm of safety electronics [26]. This reclassification brings stricter documentation requirements, more rigorous approvals, and more severe consequences in the event of a failure.

Examples of comfort electronics include window control units, door control units, seat control units, and climate control systems. The advantage of comfort electronics lies in the relatively lower risk associated with their failure. If a comfort feature is difficult to access or repair, the risk is often considered acceptable because the impact of its failure is generally minor compared to other systems in the vehicle.

3.1.2. Software Requirements

Developing software for comfort electronics in automobiles sticks to the V-model for efficient and high-quality development, often following the Automotive Software Process Improvement and Capability Determination (ASPICE) framework. This model breaks down the development process into clear phases, starting with system requirements and progressing through software and mechanical design, analysis, and testing.

To support these processes, various tools are employed for change management, simulation/modeling, automatic code generation, and testing. Standard coding guidelines must always be followed, regardless of the specific tools or processes used.

Security considerations such as encryption, digital signatures, and secure boot mechanisms may be necessary, particularly if the Threat Assessment and Remediation Analysis (TARA) determines the impact of a potential attack to be high. Secure access and secure update processes are also important to ensure that the system remains protected against unauthorized modifications.

Many norms and standards influence automotive software development, with each OEM often adapting these to create their own specific requirements. This means that different OEMs may have unique documentation requirements, such as test reports and other verification documents, that must be completed.

Logging within the software typically does not track every change or setting adjustment. Instead, only error cases are logged, sometimes with timestamps depending on the system, due to limited memory space. For example, firmware security measures may include disabling JTAG access, preventing memory readouts over the bus, and restricting the read data by address service with the On-Demand System (ODS).

While rare, if firmware is stored on external memory, encryption may be necessary to

prevent unauthorized access. Internal memory, on the other hand, requires significant effort to extract data, reducing the likelihood of unauthorized access.

Finally, proving the software's correct functionality typically does not involve logging, but may include preventative measures. These could include restricting certain use cases or blocking operations under specific conditions, such as extreme temperatures, to ensure the system behaves as expected under all circumstances.

3.1.3. Hardware Requirements

For simple tasks in automotive comfort electronics, microcontrollers may not always be necessary. However, when bus communication or other interfaces are required, using a microcontroller becomes essential. Hardware components such as motors often rely on bridge drivers, which can be implemented simply with Field-effect transistors (FETs) or as part of integrated ECUs. Similarly, light-emitting diodes (LEDs) require dedicated LED drivers to function effectively.

The operating voltage for these systems typically ranges between 9-16V, with reverse polarity protection to prevent damage from incorrect power connections. Inputs and outputs must be short circuit proof against both Klemme 30 (battery voltage) (KL30) and Klemme 31 (vehicle mass) (KL31).

To ensure electromagnetic compatibility, filters such as capacitors are used to protect the input voltage from surges, particularly during power on events. For systems supporting Over-The-Air (OTA) updates, sufficient memory is required to store the update, verify it using Cyclic Redundancy Check (CRC) or hash functions, and then apply the update. While smaller updates may be handled within the internal memory of the microcontroller, external memory is often used for larger updates.

Typically, the maximum quiescent current allowed for these systems is around 100 μA. When the vehicle is turned off, the control unit may continue operating briefly to save data from Random Access Memory (RAM) to Electrically Erasable Programmable Read-Only Memory (EEPROM) before entering sleep mode. Due to the need for short development cycles, it is common to use flash memory instead of Read-Only Memory (ROM), allowing for reprogramming with a bus system.

Mechanically, the hardware must be resistant to vibrations and mechanical shocks, which are typically validated through vibration tests. Additionally, environmental testing is crucial, particularly for temperature resistance.

For security, the Joint Test Action Group (JTAG) interface should be disabled to prevent unauthorized access. The method of disabling JTAG depends on the microcontroller manufacturer and can involve various techniques, such as burning fuses, setting certain registers, or using keycodes. In some cases, it may not be possible to disable JTAG in an obvious way, making it a less straightforward task.

3.1.4. Communication Requirements

In automotive comfort electronics, communication is a critical aspect, primarily involving the exchange of control signals or measurement data, typically via various bus systems. Commonly used communication protocols include CAN, LIN, FlexRay, and Ethernet. Ethernet is more frequently associated with the infotainment systems though. Internal communication within devices may utilize protocols like Serial Peripheral Interface (SPI), Universal Asynchronous Receiver-Transmitter (UART), or Inter-Integrated Circuit (I²C).

Other communication interfaces such as Near Field Communication (NFC) and USB may also be used, with USB commonly used for tasks such as charging mobile devices. JTAG and other debug interfaces play a role during the development and testing phases.

The specific communication systems used in a vehicle are given by the overall architecture of the vehicle, which is determined by the OEM. In a LIN bus system, for example, there is often only one master node, meaning that Denial of Service (DoS) attacks might be possible, but a more severe compromise would require the master node itself to be taken over.

Wireless interfaces, such as WiFi, tend to be integrated in higher right applications, particularly in systems where remote connectivity or OTA updates are relevant.

3.2. Relevance of digital Forensics in the automotive Comfort Electronics Environment

This section explores the importance of digital forensics in the scope of automotive comfort electronics, highlighting the necessity, specific aspects, and the implications for users and manufacturers.

3.2.1. The Necessity of Digital Forensics in Comfort Electronics

The continuous release of new comfort systems in vehicles introduces additional features, which bring new requirements and greater relevance for digital forensics. As these systems become more complex, the need to ensure their security and integrity grows.

Increasing security concerns, fueled by frequent reports of cyberattacks in the news and popular media, highlight the risks of unauthorized access and system malfunctions. These concerns make it essential to have the capability to analyze and reconstruct incidents, especially in the event of accidents, system failures, or data breaches.

Moreover, increasing compliance requirements, such as those outlined in UNECE Regulation 155 [13], are pushing the automotive industry towards enhanced forensic capabilities. It is likely that future regulations will further emphasize the need for robust forensic measures to ensure the safety, security, and reliability of automotive comfort systems.

3.2.2. Impacts on Users and Manufacturers

For users, integrating digital forensics in comfort electronics may initially raise privacy concerns, particularly when personal data might be processed during forensic investigations. However, manufacturers who incorporate forensic considerations early in the development process can carefully determine which data will be accessible and under what conditions, thereby cautiously having a trade off between privacy and security needs.

For manufacturers, there is a risk that their devices could be blamed for certain errors or vulnerabilities. Digital forensics can play an important role in disproving these accusations by providing evidence to clarify the true cause of issues. Additionally, the reputation of a manufacturer can be significantly affected by forensic findings. A random forensic investigation that uncovers security flaws could damage the reputation of a manufacturer. The other way around, if a control unit helps to solve a critical issue during an investigation, it can enhance the manufacturer standing.

As with any technology that is expected to play a larger role in the future, manufacturers who engage with digital forensics early on can secure at least a medium-term competitive advantage, positioning themselves ahead of the curve in a rapidly evolving industry.

3.3. Market Analysis

Buquerin proposed a generalized process approach to automotive forensics. The process is shown in Figure 3.1. This model will be the foundation for the following analysis. There the current support of the different steps will be evaluated.

3.3.1. Forensic Readiness

Forensic readiness in the context of automotive comfort electronics requires a unique set of challenges that are significantly different from other areas of digital forensics. The way comfort systems are designed with user convenience in mind, rather than with security or forensic capabilities as a priority, present different challenges when assessing how prepared these systems are to support forensic investigations.

One of the most unique aspects of forensic readiness in automotive comfort electronics is the diversity and complexity of the data sources involved. Unlike traditional computing

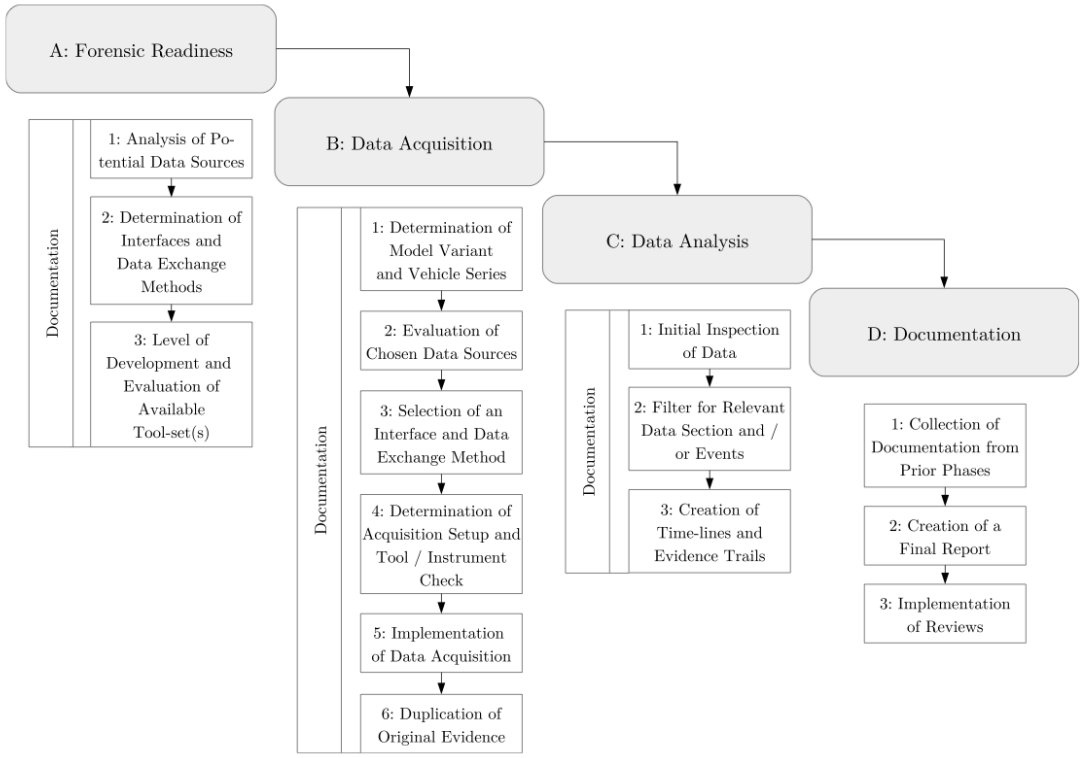

Figure 3.1.: Automotive process model of a forensic investigation. Figure taken from [6]

systems, where data might be centralized, comfort electronics data may be stored across various ECUs. Each of these ECUs may handle different comfort functions, but they often interact with each other or with other vehicle systems. Forensic readiness here means ensuring that data from these separate systems can be reliably accessed, correlated, and analyzed.

Furthermore, the data generated by comfort electronics is typically not as tightly controlled or logged as data from critical systems like engine management or braking. This can make it more difficult to track events or detect anomalies that might indicate a security breach or malfunction. For example, while a seat adjustment might seem trivial, in the context of an investigation, it could be crucial to determine whether a vehicle was tampered with or whether a specific user was present in the vehicle at a certain time.

Another critical factor is the real time capability of many comfort electronics systems. Unlike traditional digital forensics, which often deals with static data, comfort systems are designed to react instantly to user input. This means that forensic tools must be capable of capturing data in real time or reconstructing events afterwards in a way that accurately reflects what happened.

In addition, the proprietary technology used in automotive comfort electronics adds an-

other layer of complexity. Each manufacturer may use different protocols, data formats, and encryption methods, meaning forensic readiness must also include the ability to decode and interpret this information. Tools and methodologies must be adaptable and capable of handling various systems and data types.

3.3.2. Data Acquisition

Data acquisition in the domain of automotive comfort electronics includes challenges and approaches that differ from those in other areas of digital forensics. The focus here is on effectively capturing data from a variety of comfort systems, each with its own unique characteristics, protocols, and operational contexts.

One of the primary challenges in data acquisition for comfort electronics is the variety and distribution of data sources. Comfort systems are sometimes spread across multiple ECUs, each dedicated to a specific function. These ECUs may not only store data in different formats, but also communicate through different protocols. Effective data acquisition must therefore account for this by ensuring that all relevant data can be captured and made accessible for analysis.

Additionally, comfort electronics data are often event driven. Unlike data from core vehicle functions like braking or engine control, which might be logged systematically, comfort systems tend to generate data only in response to specific user actions or environmental conditions. This means that forensic readiness in data acquisition must include the ability to capture data in real time or recover it, which can be especially challenging if the data are not persistently stored.

The proprietary nature of many comfort electronics systems further complicates data acquisition. Manufacturers often use custom protocols and encryption techniques to protect their systems, which can make accessing the data a complex task. This requires the development of specialized tools and techniques that can interact with these proprietary systems to extract the necessary data without compromising its integrity or the help of the manufacturers.

Another unique aspect of data acquisition in this context is considering user privacy and data protection laws. Comfort systems often involve highly personal data. This adds a layer of complexity to the acquisition process, as investigators must ensure that they comply with legal and ethical standards while still obtaining the information required for the forensic process.

In addition, data from comfort systems may need to be correlated with information from other ECUs to provide a complete picture of an event or situation. This requires a comprehensive approach to data acquisition in which multiple data streams are synchronized and analyzed together.

3.3.3. Data Analysis

Data analysis in automotive comfort electronics requires an in depth examination of the data collected during data acquisition. This phase aims to extract relevant information from the often complex and fragmented data.

A particular aspect of data analysis is the need to understand the collected data in the context of the respective comfort function. Comfort systems are highly user centered, which means that the collected data often is closely linked to individual user preferences and behaviors. However, the data can only be useful if it is interpreted correctly, for example to reconstruct the course of an event or to understand how certain systems have interacted with each other.

Another important difference to data collection is the handling of large amounts of data and its preparation for analysis. While the challenge in data acquisition is to extract data from various sources, the focus in analysis is on filtering and structuring this data. Comfort electronics systems may generate a large number of event logs and status messages that need to be carefully evaluated to filter out relevant information and identify possible anomalies or safety-relevant events.

In addition, the analysis requires a deep knowledge of the specific data formats and protocols used in the automotive industry. While the data collection phase focuses on accessing the data, the analysis phase focuses on interpreting this data correctly and putting it into a larger context. This may require the use of specialized software to decipher proprietary formats, as well as an understanding of the functional logic of the comfort systems.

Finally, data analysis also involves the task of testing hypotheses and reconstructing chains of evidence. Here, the collected data is used to create chronological sequences that explain the behavior of the vehicle. This can be particularly important in cases where the aim is to identify human decisions or system errors that led to an incident.

3.3.4. Documentation

In forensic investigations, documentation plays a relevant role in ensuring the credibility and reliability of the entire process. It serves as a formal record that can be referenced to confirm that the investigation was conducted correctly and according to established protocols. This aspect of forensic work is crucial not only for internal consistency but also for the ability to replicate the investigation. Reproducibility is very important in forensics, as it allows others to validate the findings by following the documented steps. Without complete documentation, the integrity of the investigation could be questioned, potentially undermining the results.

Moreover, proper documentation is essential for presenting findings in an organized manner. This is particularly important in legal contexts, where forensic results may be exam-

ined carefully in court. In such cases, clear and precise documentation is necessary for the results being accepted. It provides a structured format that helps judges to understand the investigative process and the conclusions drawn from it. The ability to present evidence in a logical and accessible way is not only crucial for court but also enhances the overall transparency of the forensic investigation.

One of the most effective tools for documentation in forensic investigations is the use of log files. These files offer a detailed trace of all activities and processes that occurred during the investigation, making them invaluable for demonstrating the sequence of events and actions taken. Log files create a verifiable and chronological record that can be used to track the flow of data and the interaction with evidence. This traceability is essential for ensuring that the findings are not only accurate but also reproducible by others who may review the case.

4 Case Study on a project of APAG CoSyst

In order to illustrate these theoretical considerations using a practical example, this thesis got created in cooperation with an industrial partner. In this chapter, we will first give a brief overview of who the company is and which project was used. Then the evaluation criteria and the technologies and tools used are introduced. Afterwards, the same process as described in Chapter 3 is executed on the project. Finally, the results of the execution of the process get discussed and evaluated by the evaluation criteria.

4.1. Introduction

APAG CoSyst is a global player in the automotive supply chain, classified as a Tier 1 and Tier 2 supplier. This implies, that they supply either the OEM or a direct supplier of an OEM respectively. The company specializes in comfort electronics, providing essential components that enhance the driving experience through advanced technological solutions. With approximately 500 employees spread out across Germany, India, Switzerland, Canada, and the Czech Republic, APAG CoSyst can utilize different expertise and innovations of multiple regions. The development operations are strategically located in

Germany, Canada and India.

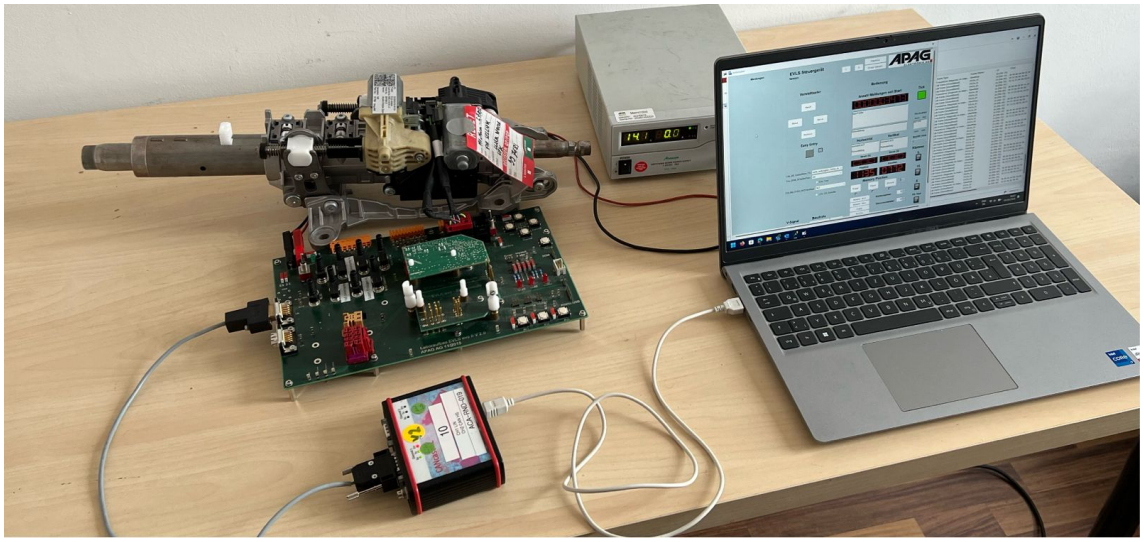

Figure 4.1.: Project Setup of the case study

The project chosen for this case study is an electronically adjustable steering column. The test setup for this is shown in Figure 4.1. The long object in the top left hand side is the steering column. The green board positioned in front of the steering column is the evaluation board. Evaluation boards are used in the embedded development to provide a platform where the ECU can be tested and relevant functionalities of the external system get simulated. The lighter green circuit board mounted on top of the evaluation board is the ECU, which will be evaluated. In front of the evaluation board is the CANcase, which will connect the laptop and the ECU. Its purpose will be explained in detail later on. Behind the laptop is a power supply.

The project aims to achieve several goals while addressing the corresponding challenges. The primary objective is to improve driving comfort by providing an easily adjustable steering column that adapts to the preferences of the driver. A significant challenge is ensuring the integration and communication within the bus-system it is connected with. Additionally, safeguarding the data collected and processed, as well as protecting against unauthorized access and data breaches are relevant as well.

This project is particularly relevant for a forensic investigation for several reasons. Firstly, the ability to adjust the steering column can provide insight into the driver's size and stature, which debatably are personal data. Secondly, the steering column adjustment mechanism interacts with other ECUs within the vehicle, adding another layer of complexity. Thirdly, the adjustments can also reveal about the key used, adding another dimension to the system's forensic analysis. Lastly, the challenge of ensuring the security of the proprietary software that controls the steering column and preventing tampering and unauthorized modifications.

In summary, the electronically adjustable steering column project at APAG Cosyst offers a comprehensive case study to explore the intersection of automotive comfort electronics and digital forensics. By focusing on enhancing driver comfort, ensuring seamless communication within the vehicle's network, and safeguarding sensitive data, this project highlights the most important challenges and opportunities in this specialized field.

4.2. Example Setup

In this section, the project in question gets defined further by first giving an overview about the scope and structure of the project. Afterwards, the evaluation criteria are defined and explained. Finally, the used technologies and tools are introduced.

4.2.1. Definition of the Scope

Figure 4.2 shows the architecture of the electronic adjustable steering column in the vehicle and highlights the most important components and interfaces. The diagram serves as a delimitation of the scope of the system by identifying central elements which are necessary for the functionality of the steering column. The power supply provides the electrical energy for the system especially the ECU, which can forward it to actuators and sensors. This ensures continuous and stable operation. The ECU is the central controller of the electronically adjustable steering column. Receiving the supply voltage of the vehicle, it controls the actuators and sensors. The ECU processes incoming information and data from sensors and the bus system. Then the actuators are navigated accordingly and some messages are communicated through the LIN bus system to other ECUs. The actuators and sensors are responsible for the mechanical movement of the steering column to enable tilt and telescopic adjustments. The sensors provide real time feedback about the position and movement of the steering column to the ECU. This feedback loop ensures that the carried out adjustments are precise and within safe operating limits. The LIN bus system is the central communication interface between the ECU and other participants in the vehicle. It enables the exchange of control commands and data. This guarantees that the steering column adjustments are synchronized with other vehicle functions. The master ECU is the primary control unit of this system. It communicates through the LIN bus and coordinates the operations in the network. Other ECUs represents different other control units which also are connected to the same bus system and can interfere and communicate on the same channel. The debug interface offers a diagnostic connection to the ECU, enabling monitoring, debugging and software updates during development.

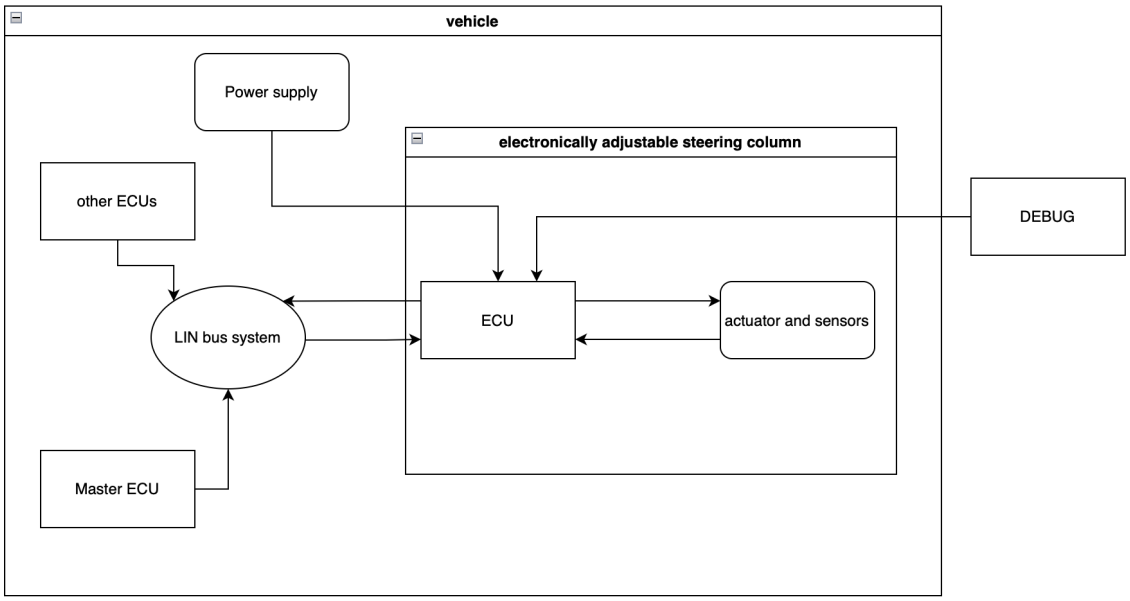

Figure 4.2.: Diagram highlighting the scope of the project

4.2.2. Definition of the Evaluation Criteria

The evaluation criteria for the forensic investigation are defined through three central aspects: (i) Forensic soundness (ii) Relevance (iii) Effort. Each of the aspects are a significant part of the evaluation of the quality and reliability of a forensic investigation. (i) Forensic Soundness is the combination of correctness, atomicity and integrity in a forensic investigation [35]. Correctness describes how closely the identified and derived values match the actual circumstances. Atomicity ensures that an investigation is conducted in complete and continuous steps. This means that forensic processes either get executed fully or not at all. During the investigation, it must be ensured that no other activities occur in the system, which can alter the outcome or affect the investigation itself [23]. Integrity refers to the immutability of the data during and after the investigation [5]. This is especially important if this is a legal investigation and the evidence may not be altered or manipulated in any way. (ii) The second aspect, relevance, refers to the significance and influence of the investigation results in the context of the case as a whole. Relevance assesses the extent to which the data and findings obtained actually contribute to clarifying the case. A high degree of relevance is given if the part of the investigation provides information that advance the final findings. (iii) The third and final aspect is the effort or the resource requirements. This includes the time used, the necessary tools, and the human resources. Especially important is the relation between relevance and effort.

4.2.3. Used Technologies and Tools

This subsection presents the various tools and technologies used in the forensic investigation process of the case study. The use of these advanced technologies is critical to ensure the functionality, reliability, and security of automotive electronic systems.

Tools

The first tool used is (i) CANoe 11.0 SP3 [34]. It is a comprehensive development and testing software for vehicle networks developed by Vector Informatik GmbH. It offers extensive capabilities for the simulation, analysis, and diagnosis of bus-based systems. This tool is used for ECUs and network communication in a simulated environment, providing a controlled environment to assess the performance and reliability of various components and their interactions. (ii) CanCaseXL is the corresponding hardware interface from the same developer, therefore guaranteeing compatibility. It is used to access bus-based vehicle networks by enabling the connection between a PC and the vehicle bus, allowing diagnostic and testing tasks to be performed. It is often combined with CANoe or similar diagnostic software to provide the physical link necessary for in-depth analysis and troubleshooting.

Technologies

Coupled with the used tools is the programming language similar to C (iii) Communication Access Programming Language (CAPL), which is used for creating simulation scripts and test sequences within CANoe. It allows manipulation of bus messages and automating test procedures, offering extensive capabilities for real-time data manipulation and analysis.This language is essential for developing customized testing scenarios that can simulate various operating conditions and system responses. The bus system used in the project for communication of the ECU in the vehicle is (iv) LIN. It is specifically designed for connecting non-safety-critical components such as sensors and actuators. LIN provides a cost-effective alternative to the widely used CAN bus technology for less demanding applications, maintaining adequate performance while reducing overall system costs. This technology is therefore crucial nowadays for ensuring communication in simpler network structures within the vehicle, where comfort electronics is often located. (v) UDS is a protocol used for diagnostic and controlling tasks in the vehicle communication. It enables communication between diagnostic tools and ECUs, including fault diagnosis, parameter settings and calibrations. UDS standardizes diagnostic functions across different vehicle manufacturers, ensuring compatibility and consistency in the diagnostic processes.

4.3. Implementation

This section covers the same forensic process as in the previous chapter. The forensic readiness, data acquisition, data analysis and documentation steps are performed on the project step by step and the results as well as important milestones are mentioned.

4.3.1. Forensic Readiness

In order to ensure the forensic readiness of the electronically adjustable steering column system, a deep analysis was performed to understand the types of data stored and processes, as well as their relevance and how they can be accessed for forensic research purposes. Three key data categories were identified. (i) Personal related data such as the location of the steering column is highly relevant as it provides insights into the drivers preferences and adjustments. (ii) Parameters and settings can provide insights, if the ECU got manipulated and therefore has medium relevance to a forensic investigation. (iii) The protection of the software controlling the steering column is of very high relevance, as it provides detailed information on system operations, potential tampering, and overall functionality.

Understanding how data is transmitted and accessed in the system is also essential for forensic readiness. (i) The location of the steering column is transmitted via the LIN bus system to the master ECU. It would also be possible to observe and analyze the actual physical location, to derive the position. That is why it is not necessary to encrypt the data, although it is possible to draw some conclusions about the driver. (ii) The settings and parameterization can be accessed through UDS, which is embedded in the LIN communication as a diagnostic service. (iii) It is also possible to get some information about the software with UDS, but also via an physical debug interface.

For a forensic analysis of the system, the tools chosen are critical to ensure comprehensive and efficient data analysis. CANoe and CanCase were primarily used due to their robust capabilities in processing and visualizing LIN messages. CANoe simplifies the analysis process by providing a graphical user interface, making it easier to interpret complex data streams. CanCase complements CANoe by providing the necessary hardware interface to access vehicle networks, facilitating the connection between a PC and the vehicle bus for diagnostic and forensic purposes.

While similar results can be achieved with open source products, it is assumed that entities conducting forensic investigations will have access to licensed tools like CANoe and CanCase. These tools offer a broad range of functionalities and ease of use that enhance the efficiency and accuracy of forensic analysis.

4.3.2. Data Acquisition

Investigation scope	Executed techniques	Goal
Without access privileges	Sniffing	Identification of protocols used and extraction of unencrypted data
UDS	Brute forcing	Identification of implemented diagnostic commands and corresponding vulnerabilities
Full control	With help of developer	Help with legal investigations and identification of ECU manipulation
Physical attack	Theoretical	Exploit of hardware vulnerabilities and access through unauthorized interfaces

Table 4.1.: Data acquisition plan using different investigation scopes

For an extensive forensic investigation, it is necessary to properly structure the steps performed to avoid missing any relevant information. The approach in this thesis is to look at different investigation scopes with distinct focuses and access rights. As shown in the left column in Table 4.1, the four main scopes derived are *without access privileges*, *UDS*, *full control* and *physical attack*. The main technique used during the *Without access privileges* investigation is sniffing of the in and out going data transmissions in order to identify the protocols which are used in those data streams and to see if any useful data can be retrieved by doing so. Afterwards, the diagnostic service layer will be utilized. In this case, the protocol used is *UDS*. To identify the implemented diagnostic commands and their corresponding vulnerabilities, a brute forcing attack is performed. To replicate a potential scenario involving legal inquiries or the necessity to demonstrate tampering with the ECU, a setup is created in which the investigator, with assistance from the developer, maintains complete control over the ECU and the master. Finally, theoretical considerations are performed to examine the potential for physical attacks and their impact, if they try to exploit hardware vulnerabilities or if they try to access though unauthorized interfaces. These four possible scopes will be shown in detail in the following subsections.

Without access privileges

Without any additional rights to carry out the investigation, there is only a limited number of possibilities that can be performed. The most promising step is sniffing. Sniffing is used in this case to determine which protocols are used and if some information can be retrieved this way. There are two possible setups to sniff. In Figure 4.3 on the right side, there is the actual setup, how it has to be done in the field. The ECU under investigation is embedded

in the actual vehicle environment communicating on a bus system with other ECUs and depending on the communication protocol used, there might be a master ECU as well. To read the messages transmitted, an external hardware device has to be connected to the bus system. In this case, the CANCaseXL, which then transfers the read data to a PC. In the case study, the bus protocol used is LIN. For simplicity, the investigation was carried out in a simulated environment, as shown in the Figure 4.3 on the left. To simulate other ECUs and especially the master ECU, CANoe was used. There it is possible to setup a schedule table and define the messages which should be sent by the simulated ECUs. The vehicle environment is also simulated. To do this, an evaluation board is used. This is a development hardware tool to recreate the vehicle environment with all relevant features such as buttons and interfaces. This way the investigated ECU does not behave differently compared to the actual environment, as long as the master ECU and the button presses are the same. However, it increases the simplicity by a lot, as it is not necessary to rebuild an entire car for the investigation process.

This strategy does not apply to every investigation. The more the ECU is depended on information and input of the vehicle, the harder it becomes to abstract these and simulate the environment. Sometimes the car or at least some parts of it have to be recreated to perform a proper investigation.

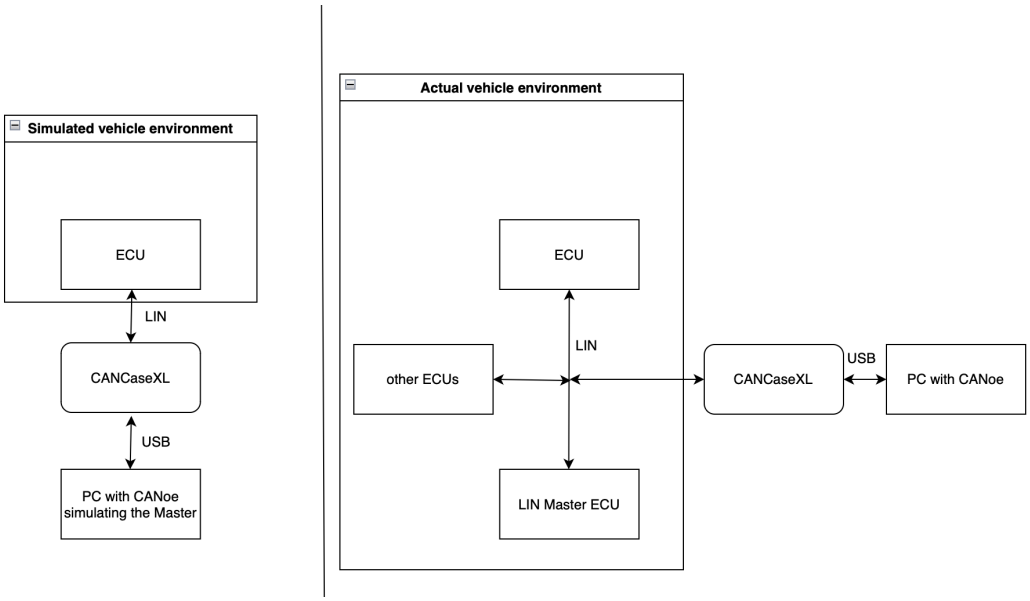

Figure 4.3.: Setup in a simulated vehicle environment and the actual vehicle environment

UDS

Usually some sort of diagnostic service is implemented, in the case of the project, the used protocol is UDS. While it is unnecessary to follow the UDS standard assignment of

services, it is pretty common as it decreases miscommunication between the supplier and the OEM. Nevertheless, for an extensive investigation it is required to also have a look at uncommonly used service IDs. To include all possibilities, a brute force attack can be performed.

In this case this means going through all possible SIDs and try them with all data possibilities. While theoretically, this covers all inquiries, the time for the execution of a brute force rises exponentially with the length of the data sector. To limit the time, of course the best way to be in contact with the developer. This would lead to the same result, but in much shorter time. For this reason it will not get mentioned in the full control over master section even though this would then be a simpler task. For the sake of an example the brute force attack got performed on the SID *0x22 ReadDataByIdentifier* with 2 bytes in the data segment. The actual code can be found in the appendix, but the following lines of code are a simplified version of this:

```
1  void bruteForceReadDataByIdentifier {
2         diagRequest request = 0x000000;
3         request.SetPrimitiveByte(0,0x22);
4         for (hex i =0x0; i<= 0xFF; i++) {
5                 for (hex k =0x0; k<= 0xFF; k++) {
6                         request.SetPrimitiveByte(1,i);
7                         request.SetPrimitiveByte(2,k);
8                         diagSendRequest(request);
9                         wait();
10 }}}
```

In line 1 the request is initialized, followed by the setting of the first byte, which corresponds to the SID to *0x22* in line 2. Then a double loop is performed. The data segment is incremented by one in each iteration, and the request is sent. This leads to all possible identifiers between *0x0000* and *0xFFFF*. In total $2^16 = 65536$ requests are sent in this example. As the ECU has to answer the requests before responding, they cannot just be sent. Assuming the time for request and answer combined are 100ms, executing all read data by identifier with 2 bytes of data takes approximately $(65536/10)/60 \approx 110$ minutes. Carrying out this with all *0xFF* SIDs, would take $((255 * 110)/60)/24 \approx 19$ days of continues requests. Depending on the task and if it is necessary to stay on one particular ECU, this could also be parallelized to multiple ECUs to save some time.

Full control over master

Obtaining complete control over the ECU is a crucial step to ensure effective forensic analysis. This control is typically achieved through collaboration with the OEM or the system developer. By working directly with the OEM, multiple advantages arise. The close collaboration provides access to detailed, proprietary information about the ECU and its functions. This insider knowledge is invaluable for understanding the complexity of the system, which enhances the accuracy, the depth and the speed of the forensic

analysis. Working with the OEM also allows access to specialized tools and resources that are specifically designed for that particular system. These tools are usually not available to the general public or third-party investigators. This approach may raise questions whether this is still part of digital forensics if the producer is involved in the process. The key aspect of this approach is the preventive and collaborative nature. By involving the the OEM from the beginning, the forensic readiness of the system can be enhanced, allowing far more effective post incident analysis. Furthermore, using specialized tools does not decrease the forensic nature but instead ensures that the investigation is as accurate as possible. There are two use cases where full control forensic can be applied. Preventive Forensic is done by considering forensic requirements during the design and development phase and building systems with their forensic capabilities in mind. It also helps in creating more resilient systems. The other form is the post incident analysis. Full control over the ECU is useful in situations where it is necessary to prove that the ECU was manipulated, such as after a vehicle accident. The detailed knowledge and tools provided by the OEM can be crucial in detecting unauthorized changes, thereby supporting legal or insurance claims. In conclusion, the partnership between an OEM and the forensic investigator can help both by facilitating more comprehensive forensic investigations and also by contributing to the development of more secure and forensically ready systems.

Physical attack

When considering forensics of automotive electronic systems, it is necessary to evaluate the potential physical attack on the ECU as well. Due to the risk of permanently damaging the ECU, this analysis was performed only theoretically. As hardware is more of a closed system than software, it is much easier to perform an extensive theoretical analysis. One potential physical attack vector is reactivating the debug interface of the ECU, which usually is disabled in production. If an attack successfully reactivates the interface, they could gain unauthorized access to the system and potentially alter or exchange sensitive data. Another possibility is dismantling the ECU to access internal memory. Directly reading the memory chips could potentially lead to retrieving stored data such as firmware or personal information.

4.3.3. Data Analysis

In this subsection, the results of the previous steps are analyzed. The described methods got implemented and executed on a real ECU. This led to multiple trace, which was then evaluated by hand. The most interesting results are presented in the following pages. To match confidential regulations, the logs are altered in such a way that it is impossible to gather conclusions about the actual system while still maintaining the general findings.

Without access privileges

When trying to analyze in a real world scenario, the first thing is to get information about the used protocol. This can be done by hand or by using advanced tools, which can automatically determine the communication system. In this case LIN is used. Following the definition of LIN, different properties can be retrieved from the messages.

Table 4.3 shows a log of communication events on the LIN bus that documents the transmission (Tx) and reception (Rx) of LIN frames within a short period of time from the master ECU point of view. The table shows important attributes such as the time of the respective event, the channel used, the direction, the event type, the ID and the data transmitted or received. This information is important to understand the communication flow. The time column records the exact time at which event took place. The recorded timestamps, which are accurate to six decimal places, show the high precision with which the events were recorded. For example, the first event occurred at 0.027467 seconds while the last event listed in the table was recorded at 0.105017 seconds. All events were transmitted through the LIN 1 channel, showing that the log relates to the communication of a single LIN bus network. The direction column shows whether the respective data packets were transmitted (Tx) or received (Rx). The events are all classified as unconditional LIN frame which is just the default message type for data transmission. Such frames contain data that are sent regularly without the need for a specific request or condition. The ID column assigns each LIN frame a unique identifier that distinguishes different message types on the LIN bus. The data column contains the actual payload of the LIN frames, represented as hexadecimal values. These values include the transmitted information such as sensor values or control commands.

Repeatability using certain IDs and associated data shows that the system is involved in regular and repetitive data transmission. This is often used by real time systems where continuous monitoring and control is required. A key point that raises from this analysis is the difficulty in uniquely identifying the relevant messages from a particular ECU through sniffing alone. Despite the detailed records of the data sent and received, the specific messages of interest to a particular ECU cannot be identified. The IDs and data patterns used could originate from several ECUs or relate to different functions. This fact highlights the complexity of analyzing LIN bus communication protocols and shows that a deeper analysis is necessary to determine the relevance and origin of individual messages.

As soon as the right IDs are identified, the relevant data can be filtered. The same result can be received by only connecting the relevant ECU to the testing equipment. Without any further input the trace looks like in Figure 4.3. ID 3 is sent from the master to the slave and IDs 4 and 5 are then returned from the slave to the master. All values remain the same, except for the last byte in the ID 5 message. As this increase is regular by always incrementing by 4, even when continuing the log, this pattern suggests the presence of an internal counter mechanism in the system. In addition to that, it is impossible to derive more information.

Time	Channel	Dir	Event Type	ID	Data
0.027467	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
0.034523	LIN 1	Tx	LIN Frame (Unconditional)	0	5A 7F 3D 92 4B 6E 1C
0.037168	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 20 90 67
0.041212	LIN 1	Rx	LIN Frame (Unconditional)	1	2D 4A 9C 6F 7B 1E 88 5A
0.048446	LIN 1	Rx	LIN Frame (Unconditional)	5	84 D3 7A 9C 05 3F 6B E4
0.053019	LIN 1	Tx	LIN Frame (Unconditional)	2	1E 2F 3D 4C 5B 6A 79 88
0.077468	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
0.080555	LIN 1	Tx	LIN Frame (Unconditional)	0	5A 7F 3D 92 4B 6E 1C
0.087186	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 20 90 67
0.090415	LIN 1	Rx	LIN Frame (Unconditional)	1	2D 4A 9C 6F 7B 1E 88 5A
0.098461	LIN 1	Rx	LIN Frame (Unconditional)	5	84 D3 7A 9C 05 3F 6B E8
0.105017	LIN 1	Tx	LIN Frame (Unconditional)	2	1E 2F 3D 4C 5B 6A 79 8C

Table 4.2.: LIN trace in an actual vehicle environment

Time	Channel	Dir	Event Type	ID	Data
0.027467	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
0.037168	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 20 98 67
0.048446	LIN 1	Rx	LIN Frame (Unconditional)	5	84 D3 7A 9C 05 3F 6B E4
0.077468	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
0.087186	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 20 98 67
0.098461	LIN 1	Rx	LIN Frame (Unconditional)	5	84 D3 7A 9C 05 3F 6B E8
0.127470	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
0.137192	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 20 98 67
0.148413	LIN 1	Rx	LIN Frame (Unconditional)	5	84 D3 7A 9C 05 3F 6B EC

Table 4.3.: Filtered LIN trace with no input

Another approach to gain further insights into the structure of the messages exchanged between the master and slave in the LIN bus is to analyze the effects of pressing the buttons that adjust the steering column. By carefully observing the message traffic during the button press, it is possible to recognize patterns and reconstruct the functions of specific bytes within the messages. For example, Table 4.4 provides a detailed log of the data recorded when the "up" button was pressed.

During the examine of the data, it is evident that Message ID 3 remains consistent throughout the entire process. This message is sent from the master to the slave, and as it is unchanged, it is suggested that the master does not alter its instructions, even while the slave unit is actively moving the steering column. This implies that Message ID 3 serves as a constant command or status indicator, independent of the movement initiated by the button press.

In contrast, Message ID 4 shows significant changes in three specific bytes, which are important to understanding the interaction between the button press and the steering column movement. Byte 4 initially holds the value 20 but changes to 28 at timestamp 2.887163 seconds. This change could indicate a change in the operational mode or state of the

slave device in response to the button press. Furthermore, the value of Byte 6 begins to decrease from 67 to 61 shortly after the change in Byte 4. This decrement suggests that Byte 6 maybe is associated with a variable parameter, such as the position of the steering column or the speed of its movement. Similarly, Byte 2, after a short delay, starts increasing from 54 to D4. The connection between these changes and the button press is a complex interaction where multiple bytes in the message contribute to the control or feedback mechanism of the system.

Message ID 5, on the other hand, features the counting mechanism in Byte 8 ensuring the integrity of the message or tracking the sequence of events. Additionally, Bytes 1 and 2 change during the second occurrence of this message ID, but they then remain the same for the entire duration of the button press. This suggests that these bytes might encode specific settings or states that are set once and are maintained throughout the process.

The fact that two values in Message ID 5 change when the button is pressed indicates that these bytes likely represent different aspects of the system's internal states rather than directly indicating the button press. To unravel the exact purpose of these bytes, further investigation is required, involving additional button presses and careful observation of the corresponding changes in the message data.

The patterns observed in the increments and decrements of the byte values in Message IDs 4 and 5 imply that one of these values could represent the position of the steering column, while the other might correspond to a different parameter, such as speed, torque, or a safety-related variable. Continued experimentation, coupled with systematic data collection, will be essential in uncovering the precise role of each byte in the LIN messages and understanding how they contribute to the overall functionality of the steering column adjustment system.

UDS

The Table 4.5 provides an example of the messages during a series of diagnostic requests and responses within the LIN bus system, focusing on RDbID requests in the UDS protocol. The requests, marked with Message ID 5C, are used to request specific data from the slave device by sending the identifier of the desired data. The responses, identified by Message ID 5D, indicate whether the requested data could be retrieved successfully.

The log starts and ends with negative responses, indicated by the response code 7F in the data field of the 5D messages. This negative response code signifies that the slave device could not fulfill the request, possibly due to the requested data being unavailable, an incorrect identifier, or other conditions that prevent a successful retrieval.

In the middle of the log, a few diagnostic responses return valid data, suggesting that under certain conditions, the slave device was able to provide the requested information. However, these successfully retrieved values lack context, making their interpretation chal-

Time	Channel	Dir	Event Type	Id	Data
2.787172	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 20 98 67
2.798499	LIN 1	Rx	LIN Frame (Unconditional)	5	84 D3 7A 9C 05 3F 6B E4
2.827469	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
2.837225	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 20 98 67
2.848445	LIN 1	Rx	LIN Frame (Unconditional)	5	83 D7 7A 9C 05 3F 6B E8
2.877467	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
2.887163	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 28 98 66
2.898486	LIN 1	Rx	LIN Frame (Unconditional)	5	83 D7 7A 9C 05 3F 6B EC
2.927468	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
2.937151	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 28 98 66
2.948422	LIN 1	Rx	LIN Frame (Unconditional)	5	83 D7 7A 9C 05 3F 6B E0
2.977469	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
2.987196	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 54 A7 28 98 65
2.998519	LIN 1	Rx	LIN Frame (Unconditional)	5	83 D7 7A 9C 05 3F 6B E4
3.027467	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
3.037240	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 64 A7 28 98 63
3.048408	LIN 1	Rx	LIN Frame (Unconditional)	5	83 D7 7A 9C 05 3F 6B E8
3.077469	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
3.087180	LIN 1	Rx	LIN Frame (Unconditional)	4	1E 94 A7 28 98 62
3.098451	LIN 1	Rx	LIN Frame (Unconditional)	5	83 D7 7A 9C 05 3F 6B EC
3.127467	LIN 1	Tx	LIN Frame (Unconditional)	3	9A 72 1F 3B 56 6D 88 C4
3.137166	LIN 1	Rx	LIN Frame (Unconditional)	4	1E D4 A7 28 98 61
3.148488	LIN 1	Rx	LIN Frame (Unconditional)	5	83 D7 7A 9C 05 3F 6B E0

Table 4.4.: LIN trace with movement of the steering column

lenging without additional information. The differences in the data returned during these successful responses highlight the need for further analysis to determine what each byte represents.

The pattern of negative responses surrounding a few successful data retrievals underscores the difficulties encountered when attempting to force data retrieval using a brute-force approach. While some information can be extracted, it is often incomplete or lacks the necessary context for immediate interpretation. This indicates the need for further investigation and possibly more targeted diagnostic queries to fully understand the meaning and relevance of the retrieved values.

Table 4.6 shows the communication process involving the Write Data by Identifier (WDbID) and RDbID functions. The requests are again represented by ID 5C, while the responses are denoted by ID 5D. The third byte in the data field of each diagnostic request identifies the type of request: 0x22 indicates a read operation, while 0x2E represents a write operation. Initially, the current value of the identifier 09 7A is read using the RDbID request, yielding a value of 11. Following this, the value is updated to 12 using the WDbID function, confirmed by the positive response in the subsequent frame. A verification step is then performed by reading the value again, which correctly returns 12, confirming that the write operation was successful. Next, an attempt is made to modify the value to 13 13

Time	Channel	Dir	Event Type	Id	Data
248.557703	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 77 FF FF FF
248.608701	LIN 1	Rx	LIN Frame (Configuration Response)	5D	69 03 7F 22 12 FF FF FF
248.657701	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 78 FF FF FF
248.668687	LIN 1	Rx	LIN Frame (Configuration Response)	5D	69 03 7F 22 12 FF FF FF
248.808728	LIN 1	Rx	LIN Frame (Diagnostic Response)	5D	69 05 62 09 79 12 12 FF
248.857701	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 7A FF FF FF
248.868713	LIN 1	Rx	LIN Frame (Diagnostic Response)	5D	69 04 62 09 7A 11 FF FF
248.957700	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 7B FF FF FF
249.008757	LIN 1	Rx	LIN Frame (Diagnostic Response)	5D	69 04 62 09 7B 19 FF FF
249.057702	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 7C FF FF FF
249.068676	LIN 1	Rx	LIN Frame (Diagnostic Response)	5D	69 06 62 09 7C 31 41 59
249.157701	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 7D FF FF FF
249.208714	LIN 1	Rx	LIN Frame (Configuration Response)	5D	69 03 7F 22 12 FF FF FF
249.257702	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 7E FF FF FF
249.268698	LIN 1	Rx	LIN Frame (Configuration Response)	5D	69 03 7F 22 12 FF FF FF

Table 4.5.: LIN trace of UDS read data by identifier commands

using another WDbID request. However, this action results in a negative response , indicating that the write was rejected, probably because it was out of the input range. When reading the identifier, the value remains at 12, demonstrating that the write attempt to 13 13 was not successful.

While RDbID and WDbID are relevant functions during development and integration, they only provide limited insights into the ECU. Only some conclusions about the parameters and their influence on the system can be made. Since there are more powerful SIDs, further brute forcing was performed, but in this case, any relevant commands, like writing or reading by address or reading actual software from the ECU, were not enabled and therefore only returned negative responses.

Time	Channel	Dir	Event Type	Id	Data
54.853.412	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 7A FF FF FF
54.879.811	LIN 1	Rx	LIN Frame (Diagnostic Response)	5D	69 04 62 09 7A 11 FF FF
54.941.298	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 2E 09 7A 12 FF FF
55.007.532	LIN 1	Rx	LIN Frame (Diagnostic Response)	5D	69 04 6E 09 7A FF FF FF
55.068.295	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 7A FF FF FF
55.072.648	LIN 1	Rx	LIN Frame (Diagnostic Response)	5D	69 04 62 09 7A 12 FF FF
55.136.710	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 2E 09 7A 13 13 FF
55.209.384	LIN 1	Rx	LIN Frame (Configuration Response)	5D	69 03 7F 2E 15 FF FF FF
55.260.497	LIN 1	Tx	LIN Frame (Diagnostic Request)	5C	69 03 22 09 7A FF FF FF
55.287.165	LIN 1	Rx	LIN Frame (Diagnostic Response)	5D	69 04 62 09 7A 12 FF FF

Table 4.6.: LIN trace of Write Data by Identifier

Full control over master

Table 4.7 shows the diagnostic communication on the LIN bus, with a specific focus on the process of requesting and receiving hash values from the ECU. This interaction is critical to verify the integrity of the ECU and ensuring that no unauthorized modifications have been made.

In the sequence, messages labeled with the identifier 3C represent diagnostic requests for a hash value. These requests are crucial during investigations, particularly when conducted in collaboration with the manufacturer, to detect any potential tampering or manipulation of the ECU's software or parameters. The integrity of these systems is vital, as even minor alterations can significantly impact the vehicle's performance and safety.

The responses to these requests, identified by 3D, contain the hash values computed by the ECU. These hash values serve as digital fingerprints of the current state of the ECU's software and parameters. By comparing these values with expected or reference hashes, it is possible to determine whether the ECU's state has been altered.

The table also shows that specific parameters were altered during "..." to point out the impact of such changes on the resulting hash values. These modifications highlight how sensitive the hash calculation is to changes in the configuration of the ECU.

For clarity and focus, routine communication data between the ECUs has been filtered out of the table. This selective presentation allows for a more straightforward analysis of

the hash verification process, ensuring that the critical aspects of diagnostic requests and responses are not obscured by unrelated data.

Time	Channel	Dir	Event Type	Id	Data
20.507701	LIN 1	Tx	LIN Frame (Diagnostic Request)	3C	49 03 22 02 45 FF FF FF
20.558674	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 10 23 62 02 45 2A D6
20.608690	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 21 46 8D 70 EA 7B 7E
20.658705	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 22 B3 73 19 07 9A 71
20.708721	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 23 D1 BD BD F5 99 C4
20.758675	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 24 95 43 DB EC 27 91
20.808747	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 25 C6 7D BB 52 6A 4B
...	...	...	...	...	...
32.057701	LIN 1	Tx	LIN Frame (Diagnostic Request)	3C	49 03 22 02 45 FF FF FF
32.108861	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 10 23 62 02 45 27 59
32.158715	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 21 92 68 F3 04 0B 6D
32.208683	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 22 C5 B7 01 75 14 08
32.258704	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 23 8D 98 01 F3 9E FE
32.308775	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 24 D8 3D 08 25 8C 8C
32.358686	LIN 1	Rx	LIN Frame (Diagnostic Response)	3D	49 25 35 3B 6B E0 A0 6B

Table 4.7.: LIN trace of hash inquiries

Physical attack

The debug interface is disabled through a software measure, leaving it inaccessible even if an attacker attempts to physically reconnect to it through the interface. This ensures that any attempts to reactivate the interface are pointless, as the software prevents unauthorized access regardless of physical modifications.

Disassembling the ECU to extract memory is a complex and labor-intensive process that typically yields minimal results. The intricate design of modern ECUs and the difficulty of accessing and interpreting the data make this attack not only technically challenging, but also inefficient. The high effort required, coupled with the low potential payoff, serves as a significant hurdle to potential attackers.

4.3.4. Documentation

The traces serve as documentation. Combined with the executed scripts and a document with step by step instruction how those were used and information about versions etc, will this be sufficient for general forensic investigations. Certain cases may require additional documentation based on legal or OEM specific requirements.

4.4. Results

In this section the results of the case study are analyzed. First the most important findings are gathered and explained. Afterwards, the evaluation criteria gets checked.

4.4.1. Outcome of the Analysis

The analysis performed focuses on assessing the potential vulnerabilities and capabilities associated with various attack vectors on the target system. The key findings are summarized in Table 4.8, highlighting the different scopes of investigation and their corresponding results. (i) The no-input analysis determined that the LIN protocol is used within the system. This lead to messages being sniffed and therefore the possibility to understand and maybe even manipulate the underlying functionality by interpreting the communication data. (ii) The investigation into UDS revealed that it is possible to extract and modify certain parameter values. This capability suggests that an attack could alter the behavior of the system by changing specific configurations. However, it was also found that extracting stored data or software directly from the memory is not possible, which limits the attack potential with this protocol. (iii) When full control over system was assumed, all previous possibilities are much easier to perform due to access to developer tools. This also includes proof of manipulation of the ECU with the help of hash values. (iv) Assessment of physical attacks revealed that while such attacks are possible, they are typically complex and offer limited rewards. The success of these attacks often depends not on software vulnerabilities, but rather on the specific hardware manufacturer. This finding suggests that the practicality of physical attacks is low, particularly in environments where hardware security is robust.

4.4.2. Checking the Evaluation Criteria

In this section, we assess how well the defined evaluation criteria have been implemented during the case study. The relevance, effort and forensic soundness criteria, including correctness, atomicity, and integrity, are used to evaluate each attack vector. Table 4.9 provides an overview of the contents of the upcoming subsections, summarizing the evaluation for each scenario. The following subsections offer a detailed examination of the case study outcomes in relation to these criteria.

In the context of automotive comfort electronics, these criteria, correctness, atomicity, integrity, relevance, and effort were critical for evaluating the viability and impact of different attack vectors. Given the way digital forensics is performed in this domain, each criterion was chosen to reflect both technical soundness and practical applicability in real world scenarios, ensuring that the results are both accurate and usable in a legal or investigative context.

Investigation scope	Results
No input	LIN is the used protocol
	Potential to map certain bytes in messages to actual events
UDS	Possibility to extract and change certain parameter values
	It is not possible to extract stored data or software from memory
Full control	Possibility to confirm manipulation on ECU
Physical attack	Possible attacks to complex for small reward
	Success usually not dependent on software but manufacturer of hardware

Table 4.8.: Summary of the outcome, grouped by the investigation scope

Without access privileges

In this scenario, the relevance of the findings is necessary as they give basic information about used protocols and data to message mapping but has a low overall impact on the system. The effort required to achieve these results was very low, as it involved passive listening to communication between components. The forensic soundness is given, with the correctness assured because the data is directly extracted from the communication logs. Atomicity is also ensured, as the messages and logs are complete, and integrity is maintained since there is no interaction with the system, only observation.

Although passive observation is categorized as low effort, its simplicity embraces the challenge of gaining meaningful insights without manipulating the system. For example, despite the lack of complexity in data collection, correlating observed messages with specific system states or events requires significant analysis, particularly when dealing with encrypted or proprietary protocols.

UDS

The UDS scenario holds high relevance due to its potential to read and alter parameters that directly affect the operation of the ECU. The effort involved is very high, particularly when brute force attacks are employed without prior information, demanding significant amounts of resources. Forensic soundness is not fully given. The interaction between UDS diagnostic commands and the ECU was clear and transactional, which supported both correctness and atomicity. However, modifying parameters is a direct contradiction

Attack Vector	Relevance (Impact)	Effort	Forensic Soundness
Without access privileges	Necessary but low impact	Very low	Correctness, Atomicity, and Integrity all high
UDS	High impact due to ability to read and modify parameters	Very high	Correctness and Atomicity high, Integrity high when reading but not when modifying
Full Control over Master	High impact with additional functionality	Low	Correctness and Atomicity high, Integrity high when reading but not when modifying
Physical Attack	Medium impact with memory extraction potential	Extremely high	Correctness and Atomicity high, Integrity compromised due to potential hardware damage

Table 4.9.: Evaluation of the different attack vectors

to forensic integrity.

Full control over master

This scenario is highly relevant, offering functionality similar to the UDS with the added advantage of determining hash values to detect changes. The effort required is low because developers already have the necessary tools and documentation. Forensic soundness is also similiar to the UDS scenario. Correctness and atomicity are supported, as the ECU interaction follows a clear request response cycle. Integrity is maintained during data reading, but it is not guaranteed when parameters are modified.

Physical attack

Physical attacks have medium relevance due to the potential to extract memory data, but the effort involved is extremely high, given the need to bypass hardware protections.

Forensic soundness could be damaged by this. The accuracy and atomicity are high because the hardware stores exact values and the process can be executed in a single step. However, integrity is often compromised as physical hardware may be damaged during the attack.

Comparison of Attack Vectors

Each attack vector's relevance varies significantly. UDS and Full control over the master provide the highest relevance. These methods offer deep access to the system, enabling investigators to interact with the ECU and retrieve or modify critical parameters that directly influence vehicle behavior. This ability to extract detailed system information or even make changes gives these vectors a significant advantage in understanding the system state. In contrast, the Without access privileges vector has limited relevance, as it involves passive observation without actively influencing the system. While it allows the collection of basic communication logs and general system activity, the depth of information is restricted. Physical attacks hold medium relevance. Although it allows direct memory extraction, the relevance of the results is often hindered by the complexity of interpreting raw memory data and the potential for system damage, which may compromise the investigation.

The effort required to execute each attack vector also shows variation. Without access privileges involves minimal effort. Simply listening to component communication can be done with basic tools, and no special access or manipulation is needed. This simplicity is what makes it a good first step in many investigations, although its overall forensic contribution may be limited. UDS commands, on the other hand, demand significantly more effort, particularly when brute force is needed to gain unauthorized access. Investigators often face challenges such as command encryption, system locking mechanisms, and the time investment required to test multiple diagnostic functions. Full control over master reduces the effort because developers or investigators already have access to specialized tools and documentation, allowing quicker access to system parameters without brute force techniques. Physical attacks present the highest level of effort, as they often require specialized knowledge of the hardware and tools for extracting data directly from memory chips. Additionally, bypassing hardware protections like encrypted memory or tamper proof components adds considerable complexity. This makes physical attacks a resource intensive option, typically only used when other methods have failed.

Forensic soundness, which encompasses correctness, atomicity, and integrity, also differs widely across the attack vectors. The Without access privileges method scores highest in terms of forensic soundness, as the data is collected passively, without any system interaction. Correctness is guaranteed because the collected logs reflect real time communications without manipulation. Atomicity is also assured since the collection process is continuous and non-intrusive, and integrity is maintained because the system remains unaltered. In comparison, UDS and Full control over master offer high correctness and

atomicity when reading data, as both vectors follow a clear request response model. However, the integrity of the data can be compromised when modifications are made, particularly in the case of parameter changes. This is critical in a forensic investigation, as modified data can no longer be considered evidence, and any changes made by an investigator or an attacker might interfere with the reliability of the findings. Physical attacks are the greatest risk to forensic soundness. Although correctness is generally high as data extracted from memory chips is exact, atomicity is at risk due to the complex task of an attack. For instance, if a memory extraction is incomplete, crucial data could be lost. Integrity is the biggest concern here, as physical damage to hardware during the attack can lead to data corruption or loss. Even when memory is successfully extracted, ensuring that no other system alterations occurred during the attack is challenging, undermining the soundness of the findings.

5 Conclusion and Future Work

5.1. Discussion

The objective of this thesis was to explore the relevance of digital forensics in automotive comfort electronics, assess the current support for forensic activities in this environment, and identify the processes and tools that can be employed for acquiring and analyzing relevant data. Additionally, the thesis aimed to determine how comfort electronics suppliers can benefit from the integration of automotive forensics.

The foundation of the research was in the general forensic process model within the automotive domain [6]. This approach was first applied in a generic analysis, followed by a case study on a real world project. The theoretical examination was supported by a small survey, which revealed consistent responses, added by abstraction and personal experience. The case study utilized tools such as CANoe, CanCaseXL, CAPL, LIN, and UDS to apply the forensic process model.

Key findings from the generic analysis highlighted the challenges associated with standardizing forensic processes due to the diversity of ECUs and their varying functions within comfort electronics. This shows the necessity of flexible approaches to adequately address the unique requirements of different ECUs. The analysis also underscored the importance of data privacy, given that personal data is processed within these systems,

and emphasized the need for compliance with legal and regulatory frameworks, including industry standards such as UNECE R 155.

The case study provided deeper insights into the specific challenges encountered during forensic investigations of comfort electronics. It illustrated the need to adapt forensic methods to varying access rights and emphasized the flexibility required to account for different approaches depending on the situation. Additionally, the study highlighted the potential for collaboration between suppliers and forensic experts to enhance investigations and share critical findings. However, it also identified significant obstacles, such as restricted access to software and systems for external investigators, which can extend forensic efforts due to the lack of access to essential data and resources.

In conclusion, while digital forensics in automotive comfort electronics presents considerable challenges, particularly concerning standardization, data privacy, and access limitations, it also offers significant opportunities. By including forensic capabilities early in the development process, suppliers can not only comply with emerging regulations but also gain a competitive advantage by ensuring the security and reliability of their systems and enhance their reputation by successfully helping in investigations.

5.2. Verification of the Evaluation Criteria

The study compared four attack vectors, without access privileges, UDS, full control over the master, and physical attacks, based on their relevance, effort, and forensic soundness. It was found that methods without access privileges offered the highest forensic soundness but delivered limited relevance. UDS and full control over the master provided a balanced trade-off between effort and forensic accuracy, especially during read operations, though modifying parameters posed risks to data integrity. Physical attacks, while enabling access to protected data, required the most effort and carried the highest risk of compromising data integrity. The comparison highlights the need to carefully select the appropriate attack vector, balancing system access, resource demands, and the reliability of the forensic findings.

5.3. Contribution and Outlook

This thesis makes a significant contribution to the field of digital forensics in the automotive industry by specifically focusing on comfort electronics, an area that has not been thoroughly explored in existing literature. While previous research has addressed digital forensics in the automotive sector more generally or within specific subdomains, this thesis distinguishes comfort electronics from other areas and looks into the role that digital forensics plays within this context. Some possible future works have been identified. One

next step involves evaluating the current legal frameworks and regulations which influence comfort electronics, with particular attention to issues of data privacy and security. This evaluation will help determine whether the existing regulatory landscape addresses the unique challenges of comfort electronics or if additional measures are needed. In addition to this, a gap analysis could be conducted to evaluate the application of current regulations. Such an analysis would identify areas where further action is necessary to ensure that digital forensics in comfort electronics is fully covered.

Furthermore, there is an opportunity for standardization within comfort electronics, particularly in areas such as communication protocols and security measures. Standardization could enhance the interoperability and security of these systems across different platforms and manufacturers. Promoting collaboration and the exchange of knowledge between industry stakeholders, regulatory bodies, and other interested parties will be essential for developing and adopting these industry wide standards. Such collaboration can lead to more robust and generally accepted guidelines that benefit the entire sector.

In addition to these technical and regulatory considerations, future research could also dig into more perspectives, considering comfort electronics from the viewpoints of OEMs, regulatory institutions, consumers, and other stakeholders. This approach will help with understanding the diverse needs and expectations of all parties involved, leading to more balanced and effective solutions.

6 List of Acronyms

ASPICE Automotive Software Process Improvement and Capability Determination

CAN Controller Area Network

CAPL Communication Access Programming Language

CRC Cyclic Redundancy Check

DoS Denial of Service

ECU Electronic Control Unit

EEPROM Electrically Erasable Programmable Read-Only Memory

FET Field-effect transistor

I²C Inter-Integrated Circuit

JTAG Joint Test Action Group

KL30 Klemme 30 (battery voltage)

KL31 Klemme 31 (vehicle mass)

LED light-emitting diode

LIN Local Interconnect Network

NFC Near Field Communication

OEM Original Equipment Manufacturer

ODS On-Demand System

OTA Over-The-Air

RAM Random Access Memory

RDbID Read Data by Identifier

ROM Read-Only Memory

SID Service Identifier

SPI Serial Peripheral Interface

TARA Threat Assessment and Remediation Analysis

UART Universal Asynchronous Receiver-Transmitter

UDS Unified Diagnostic Services

UNECE United Nations Economic Commission for Europe

WDbID Write Data by Identifier

6 BIBLIOGRAPHY

[1] Robert Altschaffel, Kevin Lamshöft, Stefan Kiltz, and Jana Dittmann. A survey on open automotive forensics. 04 2017.

[2] P. Anu and S. Vimala. A survey on sniffing attacks on computer networks. In *2017 International Conference on Intelligent Computing and Control (I2C2)*, pages 1–5, 2017. doi: 10.1109/I2C2.2017.8321914.

[3] Kousik Barik, A. Abirami, Karabi Konar, and Saptarshi Das. *Research Perspective on Digital Forensic Tools and Investigation Process*, pages 71–95. Springer International Publishing, Cham, 2022. ISBN 978-3-030-93453-8. doi: 10.1007/978-3-030-93453-8_4. URL https://doi.org/10.1007/978-3-030-93453-8_4.

[4] Disha Bhatnagar and Piyush Rao. *Vehicle Forensics*, pages 65–84. 05 2023. ISBN 9781119760412. doi: 10.1002/9781119763406.ch4.

[5] Bundesamt für Sicherheit in der Informationstechnik. Leitfaden „it-forensik“, March 2011. V. 1.0.1.

[6] Kevin Klaus Gomez Buquerin. Analysis of digital forensics capabilities on state-of-the-art vehicles. Master's thesis, Technical University Ingolstadt, Ingolstadt, GER, December 2019. Available at https://www.researchgate.net/profile/Kevin-Gomez-23/publication/354809700_Analysis_

of_Digital_Forensics_Capabilities_on_State-of-the-art_Vehicles/links/614d9a4ba595d06017e9301a/Analysis-of-Digital-Forensics-Capabilities-on-State-of-the-art-Vehicles.pdf.

[7] LIN Consortium. Lin specification package, 2010. URL https://www.lin-cia.org/fileadmin/microsites/lin-cia.org/resources/documents/LIN_2.2A.pdf.

[8] Konark Truptiben Dave. Brute-force attack 'seeking but distressing'. *Int. J. Innov. Eng. Technol. Brute-force*, 2(3):75–78, 2013.

[9] Sumeet Desai and Yogesh Bhateshvar. Development of unified diagnostic services on can using matlab and arduino. *Materials Today: Proceedings*, 72: 1935–1942, 2023. ISSN 2214-7853. doi: https://doi.org/10.1016/j.matpr.2022.10.157. URL https://www.sciencedirect.com/science/article/pii/S2214785322066731. 2nd International Conference and Exposition on Advances in Mechanical Engineering (ICoAME 2022).

[10] Nguyen van Dung. Overview of unified diagnostic services protocol, Dec 2021. URL https://nvdungx.github.io/unified-diagnostic-protocol-overview/. (accessed: 09.09.24).

[11] CSS Electronics. Uds explained - a simple intro (unified diagnostic services), Dec 2021. URL https://www.csselectronics.com/pages/uds-protocol-tutorial-unified-diagnostic-services. (accessed: 09.09.24).

[12] Joseph M. Ernst and Alan J. Michaels. Lin bus security analysis. In *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, pages 2085–2090, 2018. doi: 10.1109/IECON.2018.8592744.

[13] United Nations Economic Commission for Europe. Un regulation no. 155, 2021. URL https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.

[14] Dragoş Glăvan, Ciprian Răcuciu, Radu Moinescu, and Sergiu Eftimie. Sniffing attacks on computer networks. *Scientific Bulletin" Mircea cel Batran" Naval Academy*, 23(1):202A–207, 2020.

[15] Kevin Klaus Gomez Buquerin, Christopher Corbett, and Hans-Joachim Hof. A generalized approach to automotive forensics. *Forensic Science International: Digital Investigation*, 36:301111, 2021. ISSN 2666-2817. doi: https://doi.org/10.1016/j.fsidi.2021.301111. URL https://www.sciencedirect.com/science/article/pii/S2666281721000056. DFRWS 2021 EU - Selected Papers and Extended Abstracts of the Eighth Annual DFRWS Europe Conference.

[16] Joakim Kävrestad. *Guide to Digital Forensics: A Concise and Practical Introduction*. 01 2017. ISBN 978-3-319-67449-0. doi: 10.1007/978-3-319-67450-6.

[17] Jesse Lacroix, Khalil El-Khatib, and Rajen Akalu. Vehicular digital forensics: What does my vehicle know about me? In *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*, DIVANet '16, page 59–66, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450345064. doi: 10.1145/2989275.2989282. URL https://doi.org/10.1145/2989275.2989282.

[18] Nhien-An Le-Khac, Daniel Jacobs, John Nijhoff, Karsten Bertens, and Kim-Kwang Raymond Choo. Smart vehicle forensics: Challenges and case study. *Future Generation Computer Systems*, 109:500–510, 2020. ISSN 0167-739X. doi: https://doi.org/10.1016/j.future.2018.05.081. URL https://www.sciencedirect.com/science/article/pii/S0167739X17322422.

[19] Áine MacDermott, Thar Baker, Paul Buck, Farkhund Iqbal, and Qi Shi. The internet of things: Challenges and considerations for cybercrime investigations and digital forensics. *International Journal of Digital Crime and Forensics*, 12:1–13, 01 2020. doi: 10.4018/IJDCF.2020010101.

[20] Hafizah Mansor, Konstantinos Markantonakis, Raja Naeem Akram, Keith Mayes, and Iakovos Gurulian. Log your car: The non-invasive vehicle forensics. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 974–982, 2016. doi: 10.1109/TrustCom.2016.0164.

[21] Mirco Marchetti and Dario Stabili. Read: Reverse engineering of automotive data frames. *IEEE Transactions on Information Forensics and Security*, 14(4):1083–1097, 2019. doi: 10.1109/TIFS.2018.2870826.

[22] Dietmar P. F. Möller and Roland E. Haas. *Automotive E/E and Automotive Software Technology*, pages 83–169. Springer International Publishing, Cham, 2019. ISBN 978-3-319-73512-2. doi: 10.1007/978-3-319-73512-2_4. URL https://doi.org/10.1007/978-3-319-73512-2_4.

[23] Jenny Ottmann, Frank Breitinger, and Felix Freiling. Defining Atomicity (and Integrity) for Snapshots of Storage in Forensic Computing. In *Proceedings of the Digital Forensics Research Conference Europe (DFRWS EU) 2022*, 2022. URL https://dfrws.org/presentation/defining-atomicity-and-integrity-for-snapshots-of-storage-in-forensic-computing/.

[24] G. Pangalos, C. Ilioudis, and I. Pagkalos. The importance of corporate forensic readiness in the information security framework. In *2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*, pages 12–16, 2010. doi: 10.1109/WETICE.2010.57.

[25] Roman Rak and Dagmar Kopencova. Actual issues of modern digital vehicle forensic. *Internet of Things and Cloud Computing*, 8:12, 06 2020. doi: 10.11648/j.iotcc.20200801.13.

[26] K. Reif. *Automobilelektronik: Eine Einführung für Ingenieure*. ATZ/MTZ-Fachbuch. Vieweg+Teubner Verlag, 2012. ISBN 9783834886583. URL https://books.google.de/books?id=Tj0gBAAAQBAJ.

[27] Mark Reith, Clint Carr, and Gregg Gunsch. An examination of digital forensic models. 1, 05 2003.

[28] Yeonghun Shin, Sungbum Kim, Wooyeon Jo, and Taeshik Shon. Digital forensic case studies for in-vehicle infotainment systems using android auto and apple carplay. *Sensors*, 22(19), 2022. ISSN 1424-8220. doi: 10.3390/s22197196. URL https://www.mdpi.com/1424-8220/22/19/7196.

[29] D. Sladović, D. Topolčić, K. Hausknecht, and G. Sirovatka. Investigating modern cars. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1159–1164, 2019. doi: 10.23919/MIPRO.2019.8756732.

[30] Kim Strandberg, Nasser Nowdehi, and Tomas Olovsson. A systematic literature review on automotive digital forensics: Challenges, technical solutions and data collection. *IEEE Transactions on Intelligent Vehicles*, 8(2):1350–1367, Feb 2023. ISSN 2379-8904. doi: 10.1109/TIV.2022.3188340.

[31] Monica Sălcianu and Cristian Fosalau. A new can diagnostic fault simulator based on uds protocol. In *2012 International Conference and Exposition on Electrical and Power Engineering*, pages 820–824, 2012. doi: 10.1109/ICEPE.2012.6463580.

[32] Junko Takahashi, Yosuke Aragane, Toshiyuki Miyazawa, Hitoshi Fuji, Hirofumi Yamashita, Keita Hayakawa, Shintarou Ukai, and Hiroshi Hayakawa. Automotive attacks and countermeasures on lin-bus. *Journal of Information Processing*, 25: 220–228, 2017. doi: 10.2197/ipsjjip.25.220.

[33] Colin Urquhart, Xavier Bellekens, Christos Tachtatzis, Robert Atkinson, Hanan Hindy, and Amar Seeam. Cyber-security internals of a skoda octavia vrs: A hands on approach. *IEEE Access*, 7:146057–146069, 2019. doi: 10.1109/ACCESS.2019.2943837.

[34] Vector. Canoe family | vector. URL https://www.vector.com/de/de/produkte/produkte-a-z/software/canoe/. (accessed: 09.09.24).

[35] Stefan Vömel and Felix C. Freiling. Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisition. *Digital Investigation*, 9 (2):125–137, 2012. ISSN 1742-2876. doi: https://doi.org/10.1016/j.diin.2012.04.005. URL https://www.sciencedirect.com/science/article/pii/S1742287612000254.

A

APPENDIX

```
1   includes
2  {}
3
4  variables
5  {
6    diagRequest * Parameter_Req;
7    byte ForceID1 = 0x00;
8    byte ForceID2 =0x00;
9    byte ForceSID = 0x00;
10   msTimer ForceTimer;
11 }
12
13 on key 'b'{
14  BruteforceUDSSID(0x22);
15 }
16
17 void BruteforceUDSSID(byte SID){
18   ForceID1=0x00;
19   ForceID2=0x00;
20   ForceSID =SID;
21   setTimer(ForceTimer,1000);
22  }
23
```

```
24 on timer ForceTimer{
25
26   diagResize(Parameter_Req,3);
27   Parameter_Req.SetPrimitiveByte(0,ForceSID);
28   Parameter_Req.SetPrimitiveByte(1,ForceID1);
29   Parameter_Req.SetPrimitiveByte(2,ForceID2);
30   diagSendRequest(Parameter_Req);
31   if(ForceID2<0xFF){
32     ForceID2++;
33     setTimer(ForceTimer,100);
34   }
35   else{
36     if(ForceID1<0xFF){
37      ForceID2 = 0x00;
38      ForceID1++;
39      setTimer(ForceTimer,100);
40     }
41   }
42 }
```