



Technische Hochschule
Ingolstadt

Technical University Ingolstadt
Faculty of Computer Science

MASTER THESIS

Analysis of Digital Forensics Capabilities on State-of-the-art Vehicles

by

Kevin Klaus Gomez Buquerin

First examiner: Prof. Dr.-Ing. Hans-Joachim Hof

Second examiner: Prof. Dr. Ulrich Margull

Supervisor: M. Sc. Christopher Corbett

Issued on: 25th June 2019

Submitted on: 19th December 2019

Study program: Computer Science

Ingolstadt, March 4, 2020

Declaration

I hereby declare that this thesis is my own work, that I have not presented it elsewhere for examination purposes and that I have not used any sources or aids other than those stated. I have marked verbatim and indirect quotations as such.

Ingolstadt, _____

First name, Surname

Abstract

Vehicles get increased attention in the field of security. During the car hack village at *Defcon Security Conference* in 2016, Charlie Miller and Chris Valasek proved that modern vehicles are vulnerable to manipulation and attacks. At *Pwn2Own* 2019, security researchers were able to manipulate the infotainment of a state-of-the-art electrical vehicle.

New technologies introduced in modern vehicles and new business models, such as car sharing or features on demand, attract an increasing number of security researchers and malicious actors. As a result, Original Equipment Manufacturers (OEMs), legal institutions, insurance companies, and other entities need to be prepared for potential car security incidents. Such responses include forensic analysis to resolve liability issues or identify possible flaws in vehicles.

The master thesis focuses on capabilities of digital forensics for automotive systems. On upcoming chapters, corresponding types of forensic analysis as well as resulting requirements and challenges for automotive forensics are presented. Furthermore, a four-step concept for digital forensic analysis on state-of-the-art vehicles is presented. The process includes a forensic readiness phase, data acquisition phase, analysis phase, and documentation phase. By using the On-Board Diagnostics (OBD)-II interface, an implementation of the presented concept is performed. Communication with a modern vehicle is conducted over Automotive Ethernet with Diagnostics over Internet Protocol (DoIP) and Unified Diagnostic Services (UDS). The concept itself and the automotive forensics results are evaluated for usability in possible prosecutions.

OBD-II is usable to collect data and use it for forensic analysis. On the other hand, several gaps and disadvantages that complicate or even prevent forensic analysis for modern vehicles, are identified. Furthermore, an approach to fix stated gaps is presented.

Acknowledgements

I want to thank Prof. Dr.-Ing. Hans-Joachim Hof for the incredible and enriching talks about this topic, the support during challenging tasks, and the extensive monitoring.

Furthermore, I want to thank Christopher Corbett for the amazingly good conversations and discussions about this study. Due to his knowledge about automotive systems, I was able to write this master thesis.

Special thank to the participants at the DFRWS conference 2019 in Oslo for the interesting discussions about automotive forensics as well as new insights in performing forensic analysis in new domains.

Thanks to my family and my girlfriend for supporting me throughout my master.

Acronyms

AUTOSAR	Automotive Open System Architecture
BSI	Federal Office for Information Security
CAN FD	CAN with Flexible Data-Rate
CAN	Controller Area Network
CLI	Command-Line Interface
CPU	Central Processing Unit
DF	Digital Forensics
DoIP	Diagnostics over Internet Protocol
DTC	Diagnostic Trouble Code
ECU	Electronic Control Unit
EDR	Event Data Recorder
EEPROM	Electrically Erasable Programmable Read-only Memory
GPS	Global Positioning Systems
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System

IoT	Internet of Things
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LIN	Local Interconnect Network
LTE	Long-Term Evolution
MOST	Media Oriented Systems Transport
OBD	On-Board Diagnostics
ODX	Open Diagnostic Data Exchange
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
PCAP	Packet Capture
PC	Personal Computer
POSIX	Portable Operating System Interface
RAM	Random Access Memory
ROM	Read-only Memory
SA	Source Address
SD	Secure Digital
SOME/IP	Scalable service-Oriented MiddlewarE over IP
SPI	Serial Peripheral Interface
TA	Target Address
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module

UDP	User Datagram Protocol
UDS	Unified Diagnostic Services
USB	Universal Serial Bus
VIN	Vehicle Identification Number
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network

List of Figures

2.1	Components of State-of-the-art Vehicles	5
2.2	Example of Vehicle Communication Patterns	6
2.3	Automotive Ethernet Protocol Stack Based on the OSI Model [19]	9
2.4	DoIP Address Layout	11
2.5	UDS Read Data by Identifier Address Layout	11
2.6	UDS Positive Response Address Layout	12
2.7	UDS Negative Response Address Layout	12
4.1	Automotive Topology in Scope	24
5.1	German BSI Digital Forensics Concept	26
5.2	Automotive Forensics Concept	27
5.3	Structure of the Forensic Readiness Phase	29
5.4	Structure of the Data Acquisition Phase	32
5.5	Structure of the Data Analysis Phase	36
5.6	UDS Read Data by Identifier - Positive Response	37
5.7	Structure of the Documentation Phase	38
6.1	Connector Output of a Female OBD-II Interface	42
6.2	Data Acquisition Setup	45
6.3	UDS Service Identifier Result - Calibration Repair Shop Code Or Calibration Equipment Serial Number	47
6.4	UDS Service Identifier Result - ODX File	48
6.5	SHA256 Hash of the Original PCAP File	49
6.6	UDS Read Data by Identifier - Negative Response	50

List of Tables

4.1	Comparison of IT, Embedded, and Automotive Forensics based on Rogers and Seigfried Survey [80]	17
4.2	Digital Forensic Research Challenges Mapped on Automotive Systems	21
6.1	UDS Data Identifier to Determine Modification of Software or Hardware	51

Contents

1	Introduction	1
2	Fundamentals	3
2.1	Forensic Science	3
2.2	State-of-the-art Vehicles	4
2.2.1	Vehicle Architecture and Communication Patterns . . .	4
2.2.2	ECU	6
2.2.3	Bus Systems	7
2.2.4	Communication Systems	10
2.2.5	Storage Systems and Technologies	12
3	Related Work	14
4	Approach to Analysis of Automotive Forensics	16
4.1	Comparison of IT Forensics, Embedded Forensics, and Auto- motive Forensics	16
4.2	Scenarios	18
4.3	Types	19
4.4	Requirements	20
4.5	Challenges	21
4.6	Scope of the Study	24
5	Design of a Concept for Digital Forensic Analysis on State- of-the-art Vehicles	25
5.1	Forensic Readiness Phase	28
5.2	Data Acquisition Phase	31
5.3	Analysis Phase	34
5.4	Documentation Phase	37

5.5	Summary	39
6	Implementation of Automotive Forensics Concept Based on a Modern Vehicle	40
6.1	Determining Forensic Readiness of a State-of-the-art Vehicle (A)	41
6.1.1	Analysis of Potential Data Sources (A:1)	41
6.1.2	Determination of Interfaces and Data Exchange Methods (A:2)	41
6.2	Performing Data Acquisition on a State-of-the-art Vehicle (B)	43
6.2.1	Determination of Model Variant and Vehicle Series (B:1)	43
6.2.2	Evaluation of Chosen Data Sources (B:2)	43
6.2.3	Selection of an Interface and Data Exchange Method (B:3)	44
6.2.4	Determination of the Final Acquisition Setup and Tool / Instrument Check (B:4)	44
6.2.5	Implementation of Data Acquisition (B:5)	46
6.2.6	Duplication of Original Evidence (B:6)	48
6.3	Analysis of Collected Data (C)	49
6.3.1	Initial Inspection of Data (C:1)	49
6.3.2	Filter for Relevant Data Section and / or Events (C:2)	50
6.3.3	Creation of Time-line and Evidence Trails (C:3)	50
6.4	Documenting the Automotive Forensics Process	51
6.4.1	Collection of Documentation from Prior Phases and Steps (D:1)	51
6.4.2	Creation of a Final Report (D:2)	51
6.4.3	Implementation of Reviews (D:3)	52
6.5	Summary	52
7	Evaluation of the Automotive Forensic Analysis	53
7.1	Practical Applicability of the Presented Automotive Forensics Concept	53
7.1.1	Evaluation of Phase A – Forensic Readiness	53
7.1.2	Evaluation of Phase B – Data Acquisition	54
7.1.3	Evaluation of Phase C – Data Analysis	55
7.1.4	Evaluation of Phase D – Documentation	56
7.2	Gap Analysis	56
7.2.1	Gaps of the Automotive Forensics Concept	56

7.2.2	Gaps in the Used Tools and Instruments	56
7.2.3	Gaps in the Targeted Vehicle	57
8	Conclusion and Future Work	58

Chapter 1

Introduction

Due to a report by Peterson and published by Forbes, the interest of customers in self-driving cars increases [76]. Because of this interest, OEMs invest heavily in autonomous driving. An example is Volkswagen which invested \$2.6-billion in self-driving car technology presented in a report by Reuters [64]. These examples display a paradigm shift towards assisted and autonomous driving within the automotive industry.

Through introduction of mobility services, vehicles get more integrated in the environment. Smart home integration as well as connections between smartphones and vehicles are two examples [17]. For OEMs, this shift and integration introduces new business models, such as features on demand, where new opportunities and challenges emerge. To enable those features in automotive systems, new devices and computers are necessary. Hence, automotive systems get more complex. As stated by Manadhata and Wing in [66], this trend leads to a wider attack surface and more vulnerabilities in the overall system.

This shift in the automotive industry attracts attackers and security researchers. Business models hold the potential of fraud, while a wider attack surface increases the risk of IT security related crimes against automotive system.

To resolve security incidents, Digital Forensics (DF) science for automotive systems is an essential tool for OEMs, insurance companies, legal instances, and other entities. Forensic analyses enable OEMs to identify issues in their products and defend themselves against accusations. For example, forensic analysis can assist in answering different questions, such as "*Did the incident occur due to an in-vehicle error or by a mistake of the driver?*".

In addition, insurance companies and legal instances are capable to answer questions of guilt in insured events.

Hence, we state the following questions: Is it possible to perform forensic analysis on state-of-the-art vehicles? How reliable are the results in court?

Following, fundamentals are presented, which are required for the master thesis. Chapter 3 gives an overview of research on similar topics. Next, Chapter 4 analysis automotive forensics in more detail. Chapter 5 presents a concept for digital forensic analysis on state-of-the-art vehicles, which is implemented in Chapter 6. An evaluation of the practical applicability of the automotive forensics concept as well as a gap-analysis is presented in Chapter 7. Finally, future work and conclusion of the master thesis is presented in Chapter 8.

Chapter 2

Fundamentals

A common basis of terminology for digital forensics and state-of the-art vehicles is described in the following chapter.

2.1 Forensic Science

Locard's Exchange Principle is a fundamental principle of forensic science. Saferstein summarizes it as follows: "*Whenever two objects come into contact with one another, there is exchange of materials between them.*" [82, p. 11]. Hence, forensic science is used to reconstruct incidents using available evidence in form of material exchange within crime investigations.

As defined by Palmer and Mitro Corporation, Locard's principle is applicable to DF [74]. An example is the change of metadata, if files on Personal Computers (PCs) are modified. In addition, key goals of DF are the determination of an attacker or attacker group, as well as the entry point and its corresponding damage, as presented by Geschonneck in [52].

The following six questions are essential for DF science (6 *W*'s of forensics):

- *Who* attacked the system?
- *Why* was the system attacked?
- *Where* was initial and further impact noticeable?
- *When* was the system attacked?

- *What* was attacked?
- *How* was the system attacked?

To answer those questions, two approaches are identified. An hypotheses based procedure or by separating each question into individual aspects as presented by Geschonneck [52]. Hypothesis based approaches use the outcome of brainstorm sessions, initial present evidence (e. g. someone was seen on the crime scene), or other methods. Next, collected data is used to validate those hypotheses. Depending on the result (proven true or proven wrong) stated questions are answerable. Another approach is the separation into individual aspects. In [52, p. 66] Geschonneck presents several questions, such as "*How can you verify the attacker?*" and "*In which sequence should the data be collected?*". This method decreases the complexity of a questions.

The displayed approaches show that a forensic analysis process itself is affected by questions an analyst wants to answer and the collectable data.

2.2 State-of-the-art Vehicles

Figure 2.1 on page 5 gives an overview of different components of state-of-the-art vehicles. The following sections describe those aspects in more detail.

2.2.1 Vehicle Architecture and Communication Patterns

Vehicle architecture represents the internal structure of cars as well as networking of different devices such as Electronic Control Units (ECUs) or in-vehicle Gateways [88]. Depending on the technology, costs, and system requirements, different topologies are used. It includes stars, rings, trees, and point-to-point connections [67]. In addition, different communication patterns are utilised. They represent the flow of data in a system and are technology depended. Figure 2.2 presents an example of communication patterns.

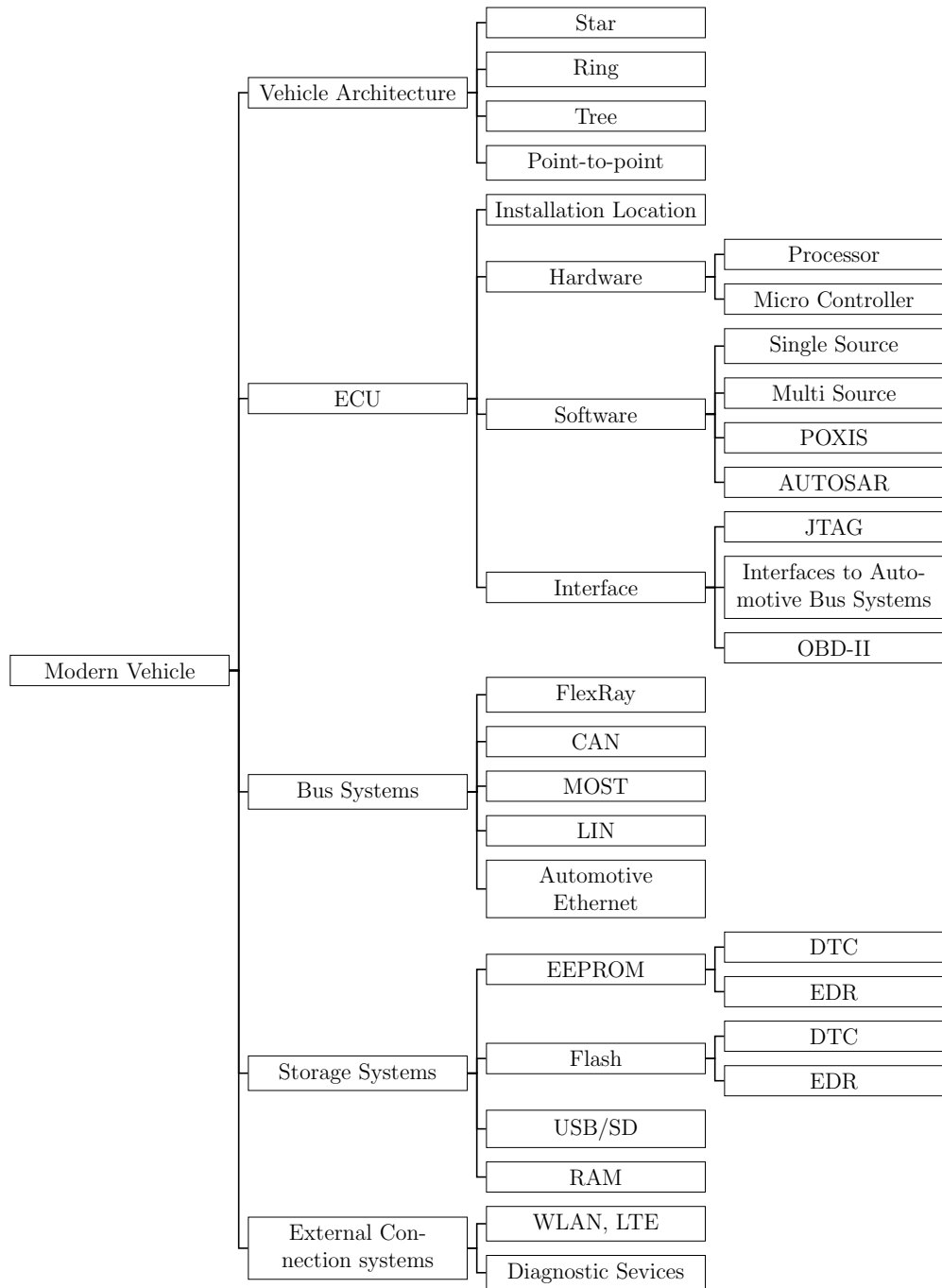


Figure 2.1: Components of State-of-the-art Vehicles

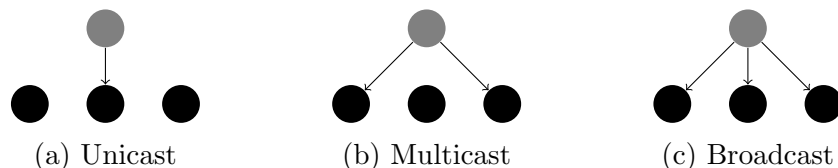


Figure 2.2: Example of Vehicle Communication Patterns

Unicast presents data flow with the corresponding addressing logic to one other system, *multicast* to multiple systems (but no all), and *broadcast* to all systems. Communication partners of all network participants are defined in the specification of an automotive architecture.

In-vehicle communication is point-to-point or cyclic. Devices connect in series result in point-to-point communication. Each device is connected to another unit and no loops within this structure are present. Cyclic communication results in loops within the communication structure. It is relevant for autonomous driving, where decision have to be made by automotive system and information from the past needs to be consumed. In addition, several ECUs are involved in decision making (e. g. should the car break or not?). Due to the risk of deadlocks, open loops can lead to safety issues. The impact on safety requirements for cyclic or loop based communication is higher compared to point-to-point communication [70].

2.2.2 ECU

Embedded computer systems in vehicles are called ECUs and are used to consume as well as transmit data of the in-vehicle network. According to Hergenhan and Heiser, modern cars are equipped with up to 100 ECUs [55].

The location of an ECU differs depending on the need of cable reduction, weight distribution, temperature management, available space, and anti-theft. As a result, some ECUs are physically difficult to access by design.

ECUs use micro-processors or micro-controllers as their main Central Processing Unit (CPU). In contrast to micro-processors, micro-controllers do have different hardware features such as Read-only Memory (ROM), Random Access Memory (RAM), or safety relevant lock-step technologies¹ (e. g. Infineon AURIX Tricore Series [2]).

¹Operations are verified by another identical processor.

To provide requested functionality, software in form of firmware operates on ECUs. It is either single- (one development company) or multi-source (multiple companies develop software for the same ECU) developed. These software modules operate on Portable Operating System Interface (POSIX) or real-time operating systems such as VxWorks, QNX, or OSEK. To achieve standardized micro-controller and micro-processor software, the development partnership Automotive Open System Architecture (AUTOSAR) and Adaptive AUTOSAR for POSIX based microprocessors is used. New software is flashed on an ECU by using the JTAG interface or diagnostic services.

2.2.3 Bus Systems

Modern vehicles use multiple bus systems, such as FlexRay, Controller Area Network (CAN), Media Oriented Systems Transport (MOST), and Automotive Ethernet.

Legacy Bus Systems

Due to their comparatively advanced age and low data rates, FlexRay, CAN, Local Interconnect Network (LIN), and MOST are often defined in literature as legacy bus systems.

FlexRay is standardized in ISO 17458-1 to ISO 17458-5 [30, 31, 32, 33, 34]. It is represented in star and basic multi-bus network. The technology supports high bandwidths up to 10 Mbit/s and is common in multimedia related automotive systems [31].

The multi-master serial bus system CAN, connects several CAN nodes on two different signalling methods [23]. First, high speed CAN where signalling towards 5 Volt is used [36]. Second, low speed CAN where signalling towards 0 Volt is used [25].

Another legacy bus system is LIN. It is standardized in ISO 17987-1 to ISO 17987-8 [43, 37, 38, 39, 40, 27, 41, 42]. As a cost-efficient alternative to CAN, the master-slave bus system supports one master and multiple slaves.

MOST is a high-speed bus and mainly used for multimedia systems of vehicles. It uses a ring topology where multiple devices are connected [53].

Automotive Ethernet

Chapter 1 stated, that an increasing demand for faster and larger data transfers is noticeable. As a result, new technologies with extended bandwidth are required. Depending on the automotive architecture and concepts of OEMs, different technologies are developed. Trends focus on fast data rates such as CAN with Flexible Data-Rate (CAN FD) and Automotive Ethernet. CAN FD was introduced by Bosch² in 2012 [11] and is standardized in ISO 11898-1 [35].

Automotive Ethernet is a possible successor for the legacy bus system MOST in the infotainment domain and a potential enabler for sensor fusion (camera, lidar, radare, etc.) in autonomous driving concepts [84]. Automotive Ethernet introduces multiple access schemes. They are based on switching, queuing, and independent decisions for each link on the network. Robustness is achieved by modern modulation techniques and filtering. [67]

Figure 2.3 displays the Automotive Ethernet protocol stack based on the Open Systems Interconnection (OSI) model. The physical layer (L1) implements 100Base-T1 (standardized in IEEE 802.3bw [6]) and 1000Base-T1 (standardized in IEEE 802.3bp [5]). Both standards use single twisted-pair copper cable to transport information. As a result, 100/1000 Mbps per link and direction are achievable.

IEEE Standard 802.3 [7] defines Ethernet. Virtual Local Area Network (VLAN) [44] is standardized in IEEE 802.1Q. Both are located within the data link layer (L2).

Further on, Internet Protocol Version 4 (IPv4) (standardized in RFC-791 [46]) and Internet Protocol Version 6 (IPv6) (standardized in RFC-6071 [50]) are implemented on the network layer (L3). IPv4 is used to route internet traffic between IPs. One difference between IPv6 and IPv4 is the size of address range. IPv6 uses 128-bit IP addresses compared to 32-bit addresses for IPv4.

Next up is layer 4, the transportation layer. Within Automotive Ethernet, User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) are used. UDP is standardized in RFC-768 [45] and TCP in RFC-793[47]. The main difference between both protocols is the type, where UDP is connection-less and TCP is connection-oriented.

²<https://www.bosch.com/> last accessed 11. December 2019

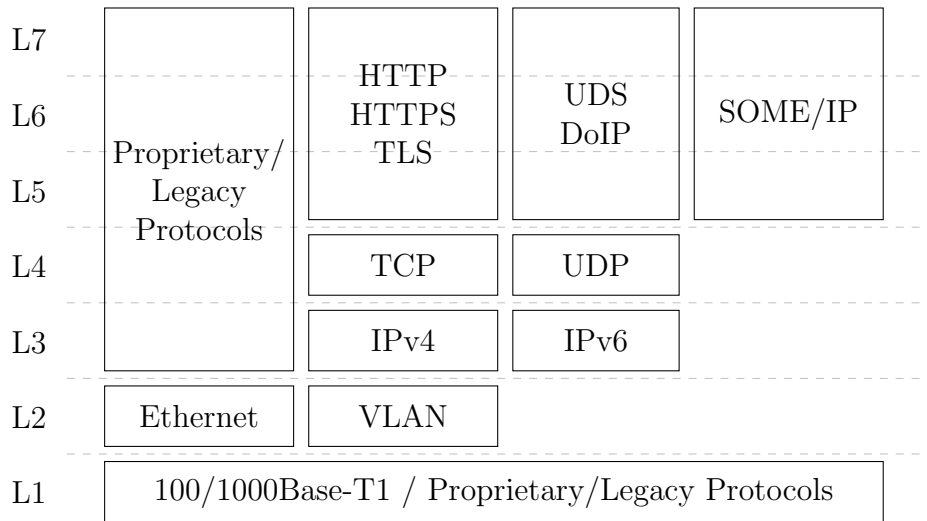


Figure 2.3: Automotive Ethernet Protocol Stack Based on the OSI Model [19]

Session (L5), presentation (L6), and application layer (L7) introduce automotive specific technologies. Scalable service-Oriented MiddlewarE over IP (SOME/IP), DoIP, and UDS, are examples for those protocols. HyperText Transfer Protocol (HTTP) (defined in RFC-7230 [49]), Hypertext Transfer Protocol Secure (HTTPS) (defined in RFC 2818 [48]), SOME/IP (standardized by AUTOSAR in [9]), as well as UDS (standardized in ISO-14229 [26]), and DoIP (standardized in ISO-13400 [28]) are located in the top three layers. HTTP and the Transport Layer Security (TLS) encrypted version HTTPS, are used to display information within the application layer. AUTOSAR developed SOME/IP to support multiple automotive based middleware features. The following sections will introduce UDP and DoIP in more detail. Both are one main part of this master thesis.

Proprietary and legacy protocols are used in layer 1 and further expand from layer 3 up to 7. Those allow OEMs to reuse technology over several model versions and implement custom protocols to fulfill all requirements. As a result, OEMs do not need to develop automotive system from the ground on.

2.2.4 Communication Systems

Vehicles allow multiple connections and communications to their environment. Examples are wireless based technologies such as Wireless Local Area Network (WLAN) and mobile broadband (Long-Term Evolution (LTE) or 3G). These technologies can be used to integrate vehicles into a smart home or to provide a hot-spot for internet connectivity. Mobile broadband is utilized to allow live updates of navigation information, weather data, and more.

Automotive Diagnostics

Automotive diagnostic services allow workshops to perform engineering, manufacturing, and service routine tasks on vehicle components. A physical connection from the testing or workshop computer to a car is conducted using OBD communication. OBD is standardized in ISO-27145 [29] and its services enable multiple purposes, such as fault code extraction, software updates, and parametrisation.

A connection to vehicles is implemented in two ways. Either through point-to-point or a more complex network of automotive devices. Point-to-point connections link the diagnostic computer directly to the vehicle by using OBD. On the other hand, a more complex network is implemented by connecting several cars to a network (e. g. by using a switch). The testing or workshop computer is also part of the network. It allows workshops to perform maintenance and service tasks on multiple vehicles at the same time.

DoIP and UDS

DoIP and UDS are both technologies that aim to fulfill new requirements such as increased data transfer rates. DoIP [28] is a transfer protocol and UDS [26] a service based protocol. These different services are presented in the following listing:

- Prescribed by law services
- OEM specific services
- standardized services
- Supplier specific services
- Proprietary services

DoIP intends to separate in-vehicle networks and external testing equipment within an IP based network [28]. It is located in layer 5 to 7 of the

OSI model and introduces several use cases such as engineering and manufacturing (e. g. flash ECU), workshop services (e. g. read Diagnostic Trouble Code (DTC)), and inspections (e. g. validate compliance of safety requirements).

Figure 2.4 displays the address layout for a DoIP message. The first byte contains the *protocol version*. For robustness reasons, another byte is used to store an *inverse of the protocol version*. Following, two bytes for the *message type* and four bytes for the *message length of the following UDS message*. Finally, 4 bytes are used for the *diagnostic message Source Address (SA)* and the *diagnostic message Target Address (TA)*. SA holds the sender address and TA the destination address.

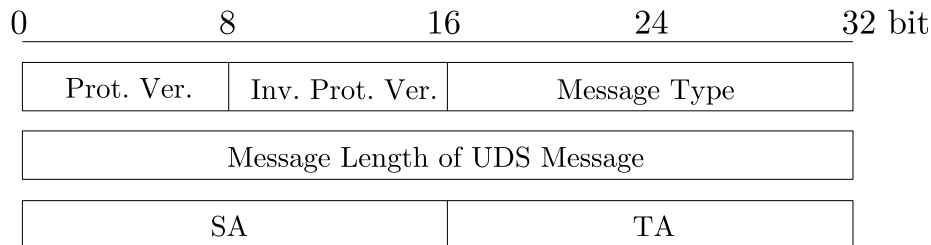


Figure 2.4: DoIP Address Layout

DoIP primary uses IPv4 and IPv6 for address assignment. Regardless of TCP or UDP, communication is performed on the fixed port 13400. To communicate using TCP, at least one socket needs to be created and kept alive. First, vehicle announcement and discovery is performed. For this purpose, the vehicles IP address on the network needs to be known and an UDS routing activation request must be send to the vehicle.

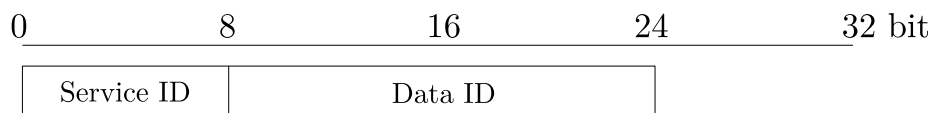


Figure 2.5: UDS Read Data by Identifier Address Layout

Diagnostic messages are always acknowledged. Either through positive (ACK) or negative (NAK) responses. Figure 2.6 depicts the address layout

for positive responses. The first byte contains the *service identifier*. The *data identifier* resides in the second byte. In a positive response, the final six bytes contain the *data record string*.

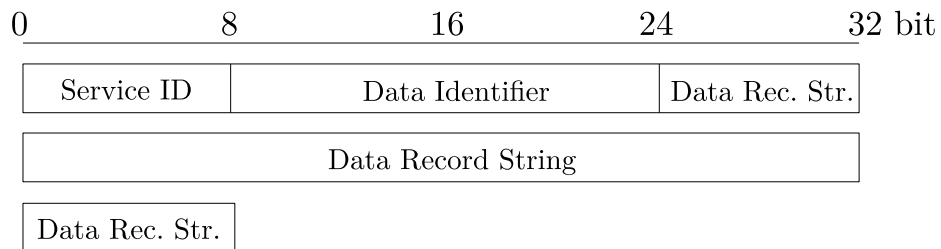


Figure 2.6: UDS Positive Response Address Layout

If a *Read Data by Identifier* message is negative, a NAK response will be received. Figure 2.7 displays the corresponding address layout. The first byte contains the *service identifier* (NAK in this case). The second byte holds the *service identifier* of the requested message (e.g. *Read Data by Identifier*). Last, the *response code* (e.g. *Request out of range*) is located in the last byte.

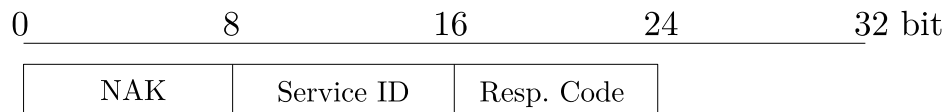


Figure 2.7: UDS Negative Response Address Layout

To summarize, a valid DoIP messages must be send first. Next, a corresponding UDS message is necessary. It contains a response and if positive the desired data.

2.2.5 Storage Systems and Technologies

Examples for in-vehicle storage are program code, logs, card material, multi-media related information, and configuration data. The following list displays common storage system used in vehicles:

- DTC
- USB, SD Cards
- EEPROM
- RAM
- Flash
- EDR

DTCs are predefined error codes that reside persistent in ECU memory, if a matching situation occurs. Universal Serial Bus (USB) sticks and Secure Digital (SD) cards store navigation maps or other multimedia-related data. Electrically Erasable Programmable Read-only Memory (EEPROM) is non-volatile memory used to hold data such as engine parameters. It is located internally (directly on the ECU) or externally (e. g. connected using Serial Peripheral Interface (SPI)). RAM stores data and machine code of firmware. Flash memory holds the source code of the firmware and gets loaded on system boot. Similar to EEPROMs it is located internally or externally. At this point in time, Event Data Recorders (EDRs) are not compulsory in European state-of-the-art passenger cars. Although, those data recorders are installed in trucks and will be prescribed for European passenger cars by law in 2022 [72].

Chapter 3

Related Work

In the field of DF for automotive systems, some research was already performed.

In [71], Nilsson and Larson published an article focusing on CAN. Based on an attacker model, the authors displayed requirements for in-vehicle networks to perform forensic analysis. Those demands include advanced storage systems and a security violation detection system to be placed in the vehicle. The authors were able to perform forensic analysis by implementing a *readiness phase, deployment phase, physical crime scene investigation phase, digital crime scene investigation phase, and presentation phase* in chronological order. Nilsson and Larson state detailed requirements on data within a vehicle and consider detection as a key part for secure vehicles.

Kiltz et al. displayed and gathered different data sources for automotive systems in [89]. The authors acquired data using self-diagnosis capabilities of ECUs. Specifically, by communicating through background debug mode (BDM), which is similar to JTAG. This included hardware data, raw data, meta data, session data, user information, and more. As a result, lots of information was retrievable and valuable for forensic analysis.

In [56], Hoppe et al. described a process for digital forensics in context of automotive incident investigations. The authors illustrated a process using a *hit-and-run suspect* scenario. Analysis were performed under the assumption of a CAN bus data logger. While applying the German Federal Office for Information Security (BSI) guide for IT forensics [51], they used the gathered data to reconstruct a travel route of the suspect. Reconstruction was performed by evaluating changes in speed in combination with steering angles.

The authors mapped the collected information on a geographical map and were able to reconstruct a plausible travel route.

Walter and Walter described techniques to acquire data from light-duty vehicles using OBD and CAN in [86]. The authors presented an overview for different automotive protocols and technologies. The *HEM DAWN OBD Mini Logger*¹ was used as for connectivity between vehicle and analysis computer. As a result, absolute load of the vehicle, throttle position, barometric pressure, and more was available for further analysis.

All prior published work is based on specific communication standards (e. g. CAN) or by assuming additional in-vehicle systems (e. g. EDR or Intrusion Detection System (IDS)). These are not present in state-of-the-art vehicles. New in-vehicle communication techniques, such as Automotive Ethernet, are not viewed in forensic research articles.

¹<http://hemdata.com/products/dawn/obd-mini-logger> last accessed 13. December 2019

Chapter 4

Approach to Analysis of Automotive Forensics

The following sections compare computer forensics approaches in general IT systems, embedded systems, and automotive systems. Furthermore, scenarios that require forensic analysis, different types of automotive forensic analysis, and corresponding requirements for usability in prosecution are described. Finally, challenges in automotive forensics and the scope of this study is described.

4.1 Comparison of IT Forensics, Embedded Forensics, and Automotive Forensics

To create a better understanding for automotive forensics, a comparison between general IT (e. g. personal computers), embedded (e. g. smartphones), and automotive forensics is performed. This comparison is based on a survey conducted by Rogers and Seigfried, in 2004 [80]. The authors asked 60 participants (researchers, students, academics, and private/public sector practitioners) about issues in computer forensics. Table 4.1 compares all three domains based on the survey. The issue *other* is left out, since it grants no benefit for this comparison.

The valuation is performed as follows: \uparrow represents good, \rightarrow medium or average, and \downarrow poor coverage or level of development within the specific area of application. * represents that a valuation of this issues can not be conducted, since it differs regarding the specific area and country of application.

Survey Issue	IT Forensics	Embedded Forensics	Automotive Forensics
Education/Training/Certification	↑	↑	↓
Technologies	↑	↑	↓
Encryption	↑	→	→
Data Acquisition	↑	↑	↓
Tools	↑	↑	↓
Evidence Correlation	↑	↑	↓
Legal Justice System	*	*	*
Funding	*	*	*

Table 4.1: Comparison of IT, Embedded, and Automotive Forensics based on Rogers and Seigfried Survey [80]

↑ : Good Coverage → : Medium or Average
↓ : Poor Coverage * : Can Not be Conducted

Compared to automotive forensics, the amount of **educational resources, trainings, and certifications** for IT and embedded forensics is high. Examples are certifications such as GCFE¹ (forensic examiner), GCFA² (forensic analyst), or GASF³ (advanced smartphone forensics). Within the automotive domain, nothing similar is offered.

Available and used **technologies** in IT and embedded forensics are advanced. Poor coverage is chosen for automotive forensics. Due to the period of time from vehicle design to a final product (product development cycle), technologies installed in a car can be outdated [69].

IT devices offer advanced **encryption** capabilities. An example is Apple’s T2 Security Chip⁴. Within the embedded devices domain these capabilities differ. Encryption of secure smartphone messengers such as Threema⁵ is advanced. As stated by Suo et al. in [85], available cryptographic techniques and encryption capability in Internet of Things (IoT) is not well researched, because this domain is in his primary phase. Automotive hardware offers

¹<https://digital-forensics.sans.org/certification/gcfe> last accessed 13. December 2019

²<https://digital-forensics.sans.org/certification/gcfa> last accessed 13. December 2019

³<https://digital-forensics.sans.org/certification/gasf> last accessed 13. December 2019

⁴<https://support.apple.com/en-us/HT208862> last accessed 13. December 2019

⁵<https://threema.ch/en> last accessed 13. December 2019

encryption algorithms too. Examples are Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs). As mentioned for the technology survey issue, due to the long product development cycle they can be outdated.

Data acquisition and **evidence correlation** is associated with **tools**. Advanced instruments offer standardized data acquisition and corresponding association. As a result, IT and embedded forensics offer great tool chains, such as FTK Imager⁶. Besides acquisition of DTCs and OEM specific tool-chains, no further instruments for automotive forensics are identified.

Legal justice system and **funding** differs depending on the specific area (IoT, Smartphones, Personal Computers, etc.) and country (e. g. encryption law in Australia [8]). Hence, no valuation is conducted.

Table 4.1 visualizes the level of development in automotive forensics compared to IT as well as embedded forensics and a need for research in this area of application.

4.2 Scenarios

Before automotive forensic analysis are applied, certain scenarios must be defined.

The following listing gives examples for different crime scenarios in the automotive domain:

- Vehicle manipulation
- Hit and run
- Grand theft auto
- Stealing of intellectual property

Vehicle manipulation is a modification of automotive components such as ECUs. It can lead to unexpected behaviour since the system configuration was not tested by an OEM or technical association (e. g. German TÜV). As a result, guarantee and warranty can be void.

Grand theft auto is the conscious stealing of a vehicle [61]. The methods used to steal a car lead from physically breaking the vehicle to utilizing *hacking* tools such as copying the digital keys.

⁶<https://accessdata.com/product-download/ftk-imager-version-4.2.0> last accessed 13. December 2019

If a suspect causes an accident and moves away from the crime scene, **hit and run** is committed [62]. Global Positioning Systems (GPS) and location data is valuable for further reconnaissance of the incident.

Breaking into in-vehicle systems such as ECUs and breaking encryption mechanisms leads to **disclosure of intellectual property** [61]. In this case, OEMs are interested in answering questions such as ” *Who broke into the vehicle?*” or ” *What information did the attacker obtain?*”.

4.3 Types

Implementation of forensic analysis is separated in two categories: *Live* and *post-mortem forensic analysis*. *Live forensic analysis* is an acquisition process during system runtime [54]. This brings several benefits, including the ability to gather volatile data (e. g. RAM) or to perform fast analysis and triage. Disadvantages are unintentional alteration of data or manipulation of the system, because the acquisition process itself can generate log data that overwrites existing evidence. An example is the creation of RAM memory images by using the tool FTK Imager. In the automotive domain, this type of analysis is gathering data of obscured ECUs.

Post-mortem forensic analysis is performed, if the system of interest is not running. In this case, volatile memory is already lost [16]. There is no impact on possible evidence compared to *live forensic analysis*. Examples are gathering of log files from non-volatile memory or restoring deleted files. Within automotive systems, acquisition of DTC information is one example of *post-mortem forensic analysis*. Compared to non-volatile storage such as EEPROM, volatile memory costs less. Due to this, it is common in modern vehicles.

Summarizing, *live forensic analysis* is more efficient and provides richer data sets for automotive systems.

The vehicle will be in different conditions (destroyed, damaged, or intact), if automotive forensic analysis are required. Hence, acquisition is performed in an *online* or *offline* manner.

Online forensic analysis is performed by using software based techniques such as log file analysis. It is not destructive since there is no disassembling of the car necessary. Besides a connection device, analysis computer, and

acquisition software, no further equipment is needed. However, due to the translation of physical data the possible amount of collectable evidence is limited.

Offline forensic analysis includes hardware based techniques such as desoldering of components from the ECU or reading varying voltage signals on devices using an oscilloscope. It is destructive to the vehicle, because devices need to be separated from the in-vehicle system. Furthermore, it is more time consuming compared to *online forensic analysis*. On the other hand, it allows to acquire more data since the information is read directly from the devices and no signal translation is necessary.

4.4 Requirements

As stated in Chapter 4.1, automotive systems and forensics do not offer a lot of available research. Hence, the use in legal proceedings is limited.

In [52], Geschonneck displays several requirements for forensic analysis and lists the following demands:

- Acceptance - Used technologies and methods should be accepted within the forensic community and should be proven to work
- Functionality - Used technologies and methods should be understood and performing as required
- Robustness - Used technologies and methods should be robust against changes of the environment
- Reproducibility - Methods should be usable by third parties and the results should be the same
- Integrity - Gathered data should not be changed
- Consistency - Connection between people, results, and evidence trails should be logical and comprehensible

If a concept for forensic analysis and gathered data fulfills the requirements, it is determined as usable for legal proceedings. If not, collected evidence might not be usable in court.

Figure 2.1 on page 5 displays components of state-of-the-art vehicles. Requirements such as integrity and acceptance are not given by using standard configured bus systems such as FlexRay, CAN, or MOST. Secure communication between forensic analysis computer and vehicle is performed by using encryption solutions such as CAN or FlexRay with SecOC (version 4.2 release of AUTOSARs Secure Onboard Communication [12]). In addition, by the use of TLS, secure communication is achieved within Automotive Ethernet⁷ based systems. These security technologies consume different time slots within vehicle communication. These time slots need to be precalculated and given in the design of an automotive system.

4.5 Challenges

To use evidence and automotive forensic analysis results in prosecutions, the goal is to achieve a good rating for all given requirements. As a result, challenges for automotive forensics are identified.

In [78], Reghavan displays digital forensic research challenges. As displayed on Table 4.2, those are applied on automotive systems to determine research challenges.

Digital Forensic Research Challenge	Relevance for Automotive Systems
Complexity Problem	Relevant
Diversity Problem	Not Relevant
Consistency and Correlation	Relevant
Quantity or Volume Problem	Relevant
Unified Time-lining Problem	Relevant

Table 4.2: Digital Forensic Research Challenges Mapped on Automotive Systems

The **complexity problem** describes an increase of complex systems and intricate processing of data representations. Forensic analysis is more expensive for complex systems, because more data is acquirable and more difficult to extract. Due to increasing number of ECUs, this problem is relevant for vehicles. In 1994, approximate 10 ECUs were embedded in a car, where in

⁷As a higher layer protocol, TLS is used on other automotive bus systems too.

2000 40, and 2010 more than 100 control units are installed in vehicles [20]. An increasing number of mobility services for cars result in more complex system.

Due to the **diversity problem**, big volumes must be separated into smaller chunks, which results in less time-consuming analysis. Since no large storage devices are used within vehicles, this research challenge is not relevant for automotive systems.

Consistency and correlation are comprehensive in digital forensics. Multiple data sources need to be correlated to generate usable evidence. Due to the great amount of ECUs in modern vehicles, consistency and correlation is a suitable challenge for automotive systems.

A high number of devices introduce a lot of data, which leads to **quantity and volume problems**. A lot of small memory chunks create a large amount of data for analysis. As a result, the research problem is relevant for automotive systems.

To evaluate the order of events occurred in a system, a correlation of timestamps for different systems must be applied. Although, various in-vehicle sub-systems track, interpret, and calculate time differently. ECUs with access to GPS get the current GPS-Time. Other ECUs use this time as a reference point. Different data sources might lead to problems while correlating timestamps. Depending on requirements, specifications, and costs, the degree of precision in calculating time, differs between ECUs. As a result, **unified time-lining problem** is applicable to automotive systems.

In addition to Reghavans digital forensics research challenges, other deficiencies are defined:

- Limited processing power
- Accessibility
- Safety requirements
- Different ECU topologies and future hypervisor support

Processing power on modern ECUs is limited compared to IT systems. The ST⁸ 32-bit power architecture microcontroller *SPC58NE84E7* from the *SPC58EE_x*, *SPC58NE_x* family, implements up to two cores with 180 MHz

⁸<https://www.st.com/> last accessed 13. December 2019

each as well as 6576 KB (6288 KB code flash + 288 KB data flash) on-chip flash memory [83]. Areas of application are advanced driver assistance systems, in-vehicle infotainment, mobility services, and other. This example states the low processing power of in-vehicle devices. Therefore, forensic analysis can interfere with in-vehicle systems and leads to unintended changes of evidence. By default, such devices offer no storage to log data for later forensic analysis.

Accessibility to automotive systems is challenging. It is demanding from the outside perspective and internal perspective. Usually, a vehicle is located at the customer. Hence, limited accessibility for forensic analyst is given. Access to ECUs over-the-air is not implemented on most modern vehicles. From a security perspective, an implementation of these privileges is difficult. To resolve this particular accessibility issue, the vehicle needs to be physically accessible (e. g. in a workshop). To perform extensive forensic analysis, several ECUs must be extracted from the vehicle. Exact location and linkage of those ECUs, as well as dependencies between ECUs, is only available to the manufacturer and not always present for a forensic analyst. In addition, extraction of ECUs, might lead to disturbances and unintended changes of evidence. Interfaces such as OBD-II or JTAG are promising because disturbances and unintended changes are less distinct compared physically extraction of ECUs.

Automotive systems are designed to fulfill **safety requirements** and standards. Issues can occur, if changes to automotive software are not tested. This leads to potential violation of safety requirements. Throughout a forensic analysis it must be ensured to not change the state of the vehicle. This is primarily important while performing live forensic analysis.

Since **topologies** between OEMs differ, general techniques and methods must be implement. To perform forensic analysis, the targeted system must be known. In addition, future vehicle systems will introduce **hypervisor support**. Early 2019, Infineon⁹ published a technical paper on a new microcontroller family called *AURIX TriCore* [2]. This controller generation will introduce hypervisor support for automotive applications where safety-critical tasks will be executed in a hypervisor. An introduction of this technology will introduce further challenges such as secure access and information gathering for hypervisors.

⁹<https://www.infineon.com/cms/en/about-infineon/> last accessed 13. December 2019

4.6 Scope of the Study

As described in Chapter 4.2, damage to the overall vehicle leads to manipulation of evidence. This master thesis focuses on *online forensic analysis*. Compared to *offline forensic analysis*, *online forensic analysis* is more cost optimised for an OEM, because no further hardware or tooling is required. In addition, the vehicle does not get damaged, which reduces costs for the vehicle owner, OEM, or insurance company.

Due to its high data rates and new introduction into vehicles, Automotive Ethernet is selected as the protocol in scope. It offers secure data transfer by using TLS. As displayed in Figure 4.1, data directly after the DC (domain controller, which controls multiple micro controllers) is encrypted by using Automotive Ethernet with TLS.

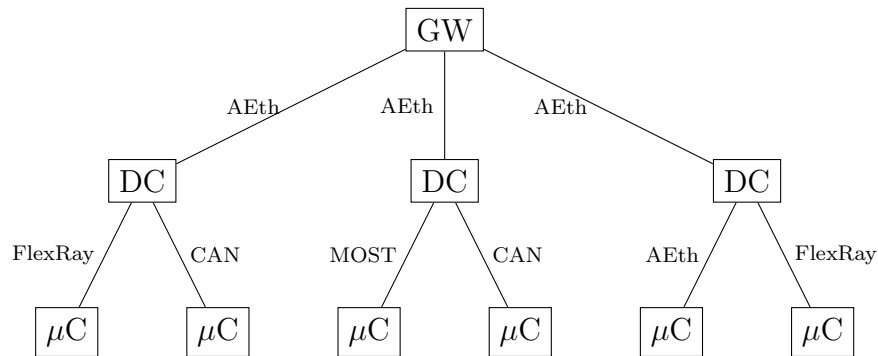


Figure 4.1: Automotive Topology in Scope

AEth : Automotive Ethernet μC : Micro-Controller
GW : Gateway DC : Domain Controller

To gather data from in-vehicle systems, OBD-II is selected. It is standardized and implemented in all European passenger cars. Furthermore, it offers a rich set of diagnostic data for forensic analysis.

Chapter 5

Design of a Concept for Digital Forensic Analysis on State-of-the-art Vehicles

Based on results of Chapter 4, the design of a concept for digital forensic analysis on state-of-the-art vehicles is presented.

In digital forensics, different concepts are known. On the one hand, they are general and use a standardized structure. Others present concept frameworks and are used to adapt the procedure on specific areas of application such as avionics, commodity IT, smartphones, or automotive.

In [51], German BSI presented a generic process to perform forensic analysis for specific domains. General IT systems such as personal computers and servers were in scope. As displayed in Figure 5.1, the concept is separated in six phases. A strategic preparation phase to enable logging on possible relevant systems. An operational preparation phase to determine present data sources. Third, data acquisition where creation of cryptographic secure images to store acquired data is performed and data examination phase. Here, a selection of data that is valuable for further forensic analysis is chosen. During data analysis phase, collected and selected data is analysed and correlated. Finally, a documentation phase is performed. It consists of process-related documentation and creation of a final report, which presents all performed steps and collected results.

In [65], Luttgens et al. presented a process for computer forensic. Scope of the authors book was consumer electronics (e. g. computer systems running

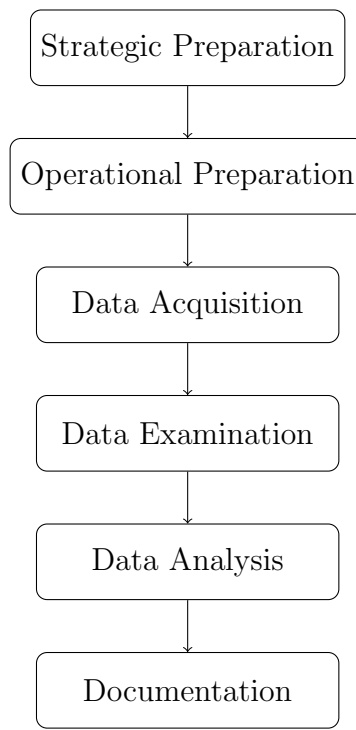


Figure 5.1: German BSI Digital Forensics Concept

Windows, UNIX, and Mac OS X), network devices, and enterprise systems. The authors discussed reasons for live data collection and importance of forensic data duplication as well as an evaluation of available data sources for all mentioned domains.

Comparing both processes, BSI presented a more detailed approach to perform forensic analysis, while Luttgens et al. viewed different domains and presented a more general concept.

Automotive forensics introduces several sub-systems with multiple technologies and different operating systems as evaluated in Chapter 2. This diversity requires a more general approach using a standardized structure for forensic analysis. To achieve usability, an increased focus must be set in presenting as well as evaluating implemented operating systems and used technologies. Due to this, a more general concept with four main phases is presented. As displayed in Figure 5.2, it introduces a forensic readiness phase, followed by a data acquisition and data analysis phase. Last, a doc-

umentation phase is performed. The concept must fulfill requirements for possible prosecutions (Section 4.4) and handle digital forensics challenges (Section 4.5).

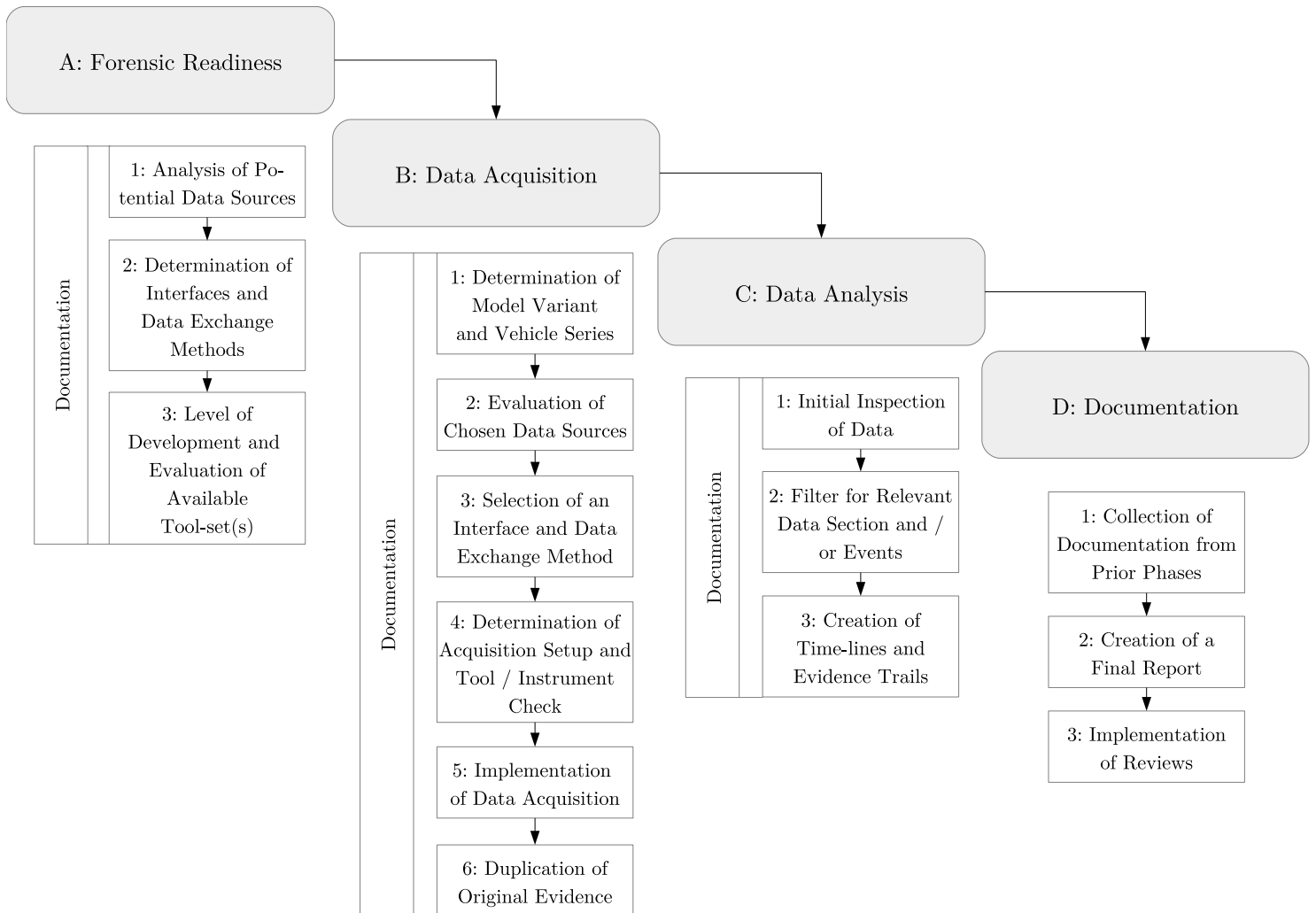


Figure 5.2: Automotive Forensics Concept

Subsequent sub-sections are structured as follows:

- Definition and presentation of state-of-the-art for the phase
- Importance and key points of the phase

- Relevance for and reference to automotive systems
- Structure of the phase
- Implementation of the phase
- Results of the phase
- Positive and negative examples

5.1 Forensic Readiness Phase

First, a definition as well as state-of-the-art for forensic readiness are presented. Rowlingson defined forensic readiness as "*the ability of an organisation to maximise its potential to use digital evidence whilst minimising the cost of an investigation.*" [81, p. 1]. In [22], Endicott et al. presented importance of forensic readiness for an organisation. The authors stated that this phase allows businesses to increase effectiveness of forensic investigations. Both definitions show, forensic readiness is relevant for organisations, willing to perform forensic analysis. More focus on this phase results in greater outcome of forensic investigations. It grants the ability to increase the value of forensic analysis.

As evaluated by Ivanisevic et al. in [57], cost effectiveness is of interest for a business. OEMs cannot be excluded from this statement. Processes need to be optimised and the value for different actions must be maximised. By definition, focus on forensic readiness maximises this value. As a result, OEMs are able to get the most out of a forensic investigation and achieve cost effectiveness.

Figure 5.3 displays the structure of the forensic readiness phase in more detail. Documentation during and of all performed steps is utilized. Reproducibility requirement is fulfilled, if a final documentation is available. By using this report, any third-party should be able to reproduce results.

First, an analysis of potential data sources is performed, where a determination of in-vehicle components and used technologies is utilized. In general, most vehicles implement similar data sources. Used technologies differ between manufacturer and model. A more in-depth or abstract analysis of

potential data sources is feasible. Depending on the questions a forensic investigation should answer, the type of analysis differs. Common vehicle literature and, if available, OEM documentation are usable as an instrument.

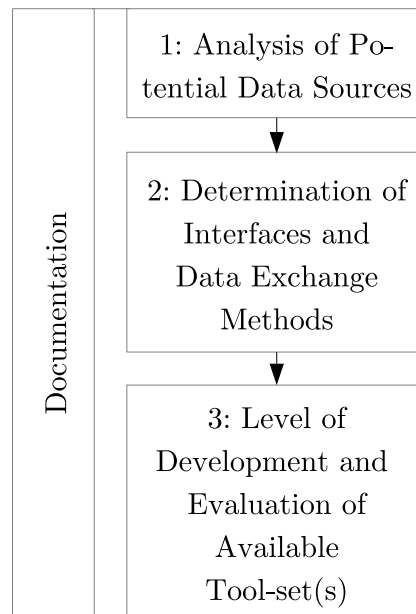


Figure 5.3: Structure of the Forensic Readiness Phase

The second step of this phase is a determination of interfaces and data exchange methods. Depending on the type of forensic investigation (*live* or *post-mortem*) as well as acquisition method (*online* and *offline*), different exchange methods and interfaces are applicable. To acquire data using JTAG, direct access to an ECU is necessary. OBD-II allows to acquire data without physical access to an ECU. This phase must ensure to fulfill the integrity requirement and therefore not tamper potential evidence.

Next, the level of development for automotive forensics and availability of a tool-set must be evaluated. Goal of this step is to determine how much forensic analysis experience is available for automotive forensics. It allows forensic analysts to use known as well as functioning technologies and methods during forensic investigations. If the level of development for a specific domain is extensive, the acceptance requirement is attainable. In addition, solutions for digital forensics challenges might be present and applicable.

To acquire data from vehicles, hardware and software tools must be

present. A functional and working tool-set ensures to fulfill the consistency, robustness, and reproducibility requirements. The consistency and correlation problem as well as the quantity or volume problem are manageable, if a functional tool-set is present.

By performing analysis of a modern vehicle, automotive forensics is achievable. Three different resources are available to determine potential data sources, interfaces and data exchange methods, available tool-sets, and the level of development. First, common literature is suitable. This source of data is available to the public and due to its publication, accepted by the community. Second, manufacturer documentation is usable. This source might not be publicly available, because manufacturers aim to protect their intellectual property. Since these resources are mostly unpublished, the acceptance requirement is not fulfilled. Finally, researchers and forensic analysts are able to create their own documentation of a specific vehicle by reverse engineering all necessary components. This task is time consuming due to the amount of in-vehicle components. If during implementation of the forensic readiness phase one of the mentioned resources is unavailable, another method must be used. Relevant components are evaluated based on prior work in this field or by performing evaluation of different data sources. Based on connection interfaces as well as technology of interest, tools are chosen or developed.

Different deliverables are achieved in this phase. First, a detailed evaluation of available data sources. Second, presence of a tool-set is determined. Last, selection of a connection interface to acquire data for the vehicle is performed.

A positive example is the presence of an EDR. Such a device allows dedicated storage of events. Effectiveness for such components was presented by Böhm et al. in [13]. The authors evaluated vehicle control units as data sources for events stored in an EDR. The presented design of a vehicle black box focused on modern hybrid and electric vehicles. Another positive example is a system, where ECU data is accessible with little effort. This includes presence of available connection interfaces like OBD-II. Here, flash and EEPROM data is collectable by communicating with installed ECUs.

In a negative example, no connection interface is present. Data acquisition must be performed by using *offline forensic techniques*, which is error

prone and time consuming. Furthermore, lack of documentation or asset management is negative for forensic readiness of a specific system. If no data sources and connection interfaces are identifiable, forensic analysis is not feasible.

5.2 Data Acquisition Phase

Watson and Jones defined data acquisition as the collection of predefined data sources [87]. Those are the result of a forensic readiness phase. In [18], Clark et al. defined data acquisition as a process where data collection is performed. The authors analysed a DJI Phantom III drone and separated the process into data acquisition from drone, controller, and drone control unit. Comparing both definitions, the outcome is equal. During data acquisition, information is collected from predefined and evaluated sources of data.

This phase introduces multiple important points. To fulfill the integrity requirement, original data must not be corrupted. As presented by Kcuik in [60], it is important to ensure one way communication (write only). It is achievable by using a write-blocker as presented and formally specified by Enbacka and Laibinis in [21]. Those devices allow read-actions only and block every write-action to the connected system. This method protects against accidental changes to the overall environment. Collected as well as available data needs to be trustworthy. As presented in Chapter 4.4, the used tool-set must fulfill the acceptance, functionality, and reproducibility requirement. In addition, it is required to duplicate original data and create mirror images for further analysis. This avoids accidental manipulation of original collected data.

Similar to digital forensics of general IT systems, the stated important points must be fulfilled for automotive systems too. Otherwise integrity of collected data is not achievable. Vehicle systems do not implement backups. Reconstruction of manipulated data is not possible. This underlines importance of protection against accidental and unintentional changes to the vehicle systems.

Figure 5.4 presents the data acquisition phase in more detail. During all steps, precise documentation must be created. This ensures to fulfill the

reproducibility requirement.

First, determination of model variant and vehicle series is performed. This was already part of the forensic readiness phase. It is important to reassure the actual model variant and therefore used technologies. This check leads to a fulfillment of the functionality, reproducibility, and consistency requirement. Due to this, the chosen tool-set will work on the original evidence and any third-party is able to emulate the same results as well as evidence trails.

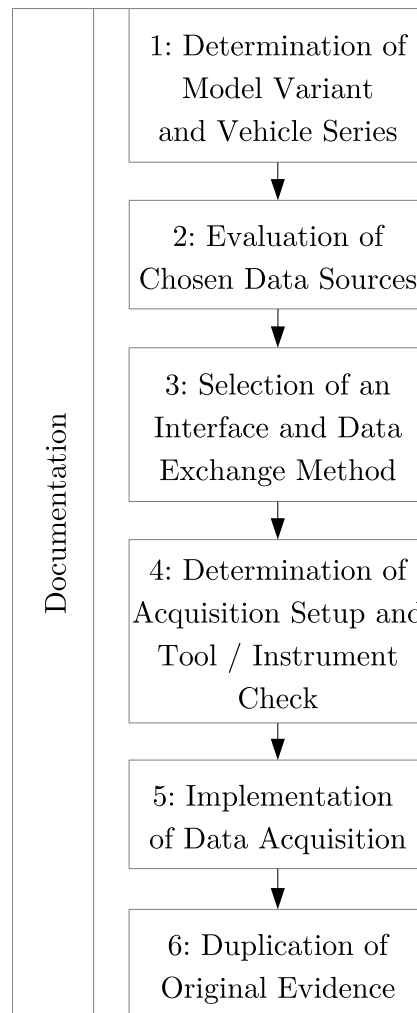


Figure 5.4: Structure of the Data Acquisition Phase

Following, an evaluation of chosen data sources is utilized. Depending on

the answers that need to be answered by the forensic investigation, this evaluation differs. If general and standardized data sources need to be present for acquisition (e. g. flash or EEPROM), this task is feasible by reviewing the forensic readiness phase. On the other hand, if specific and non-standardized data sources (e. g. vehicle black box that is only installed by a specific OEM) are of interest, additional resources are required. This includes internal documentation or reverse engineering of an identical vehicle model. The complexity problem is solved, if data sources are known. A forensic analyst will know what to expect from different data sources.

Third step of this phase is the selection of an interface. The forensic readiness phase presented different available interfaces and data exchange as well as acquisition methods. This includes OBD-II, JTAG, and actual soldering of chips. Depending on the chosen interface and data exchange method, the acceptance, reproducibility, and integrity requirement are fulfilled. Quantity or volume problem is manageable, if an interface that connects to a component network is chosen. Due to the amount of ECUs in modern vehicles, soldering of in-vehicle components is very time consuming. Hence, quantity or volume problem is still relevant and not solved.

Step four introduces the presentation of the final acquisition setup and implements a tool / instrument check. A determination, if necessary components and tool-set(s) are fully functional and perform as required, is utilized. If the tests are positive, the functionality requirements is fulfilled. Otherwise, fulfillment of this requirement is not guaranteed.

Next, implementation of data acquisition is performed. During this step, a forensic analyst collects data from selected sources, while using the chosen interface and tools.

Integrity of original evidence must be given, even after data acquisition. To achieve this, duplication of original evidence and creation of a secure cryptographic hash sum for original data is performed.

To perform data acquisition on vehicles, different components are required. First, the targeted subject. Next, an acquisition computer to communicate with in-vehicle systems. Following, a tool-set that is installed on the acquisition computer. It allows communication with in-vehicle components and systems. To connect the acquisition computer with the car, a corresponding cable is required. The connector depends on the connection interface chosen during forensic readiness phase. Examples are OBD-II to Bluetooth, OBD-II to Ethernet, and JTAG to USB cables. If everything is

set up, data acquisition is feasible. During data collection, errors can occur. Error messages and faulty circumstances need to be documented. Afterwards, data acquisition phase continues with the step, that led to the error. If a problem is not solvable by restarting different phases, forensic readiness phase, determination of model variant and vehicle series, as well as evaluation of chosen data sources needs to be redone. Problems can occur, if the selected tool-set and instruments do not allow communication with in-vehicle components.

Results of this phase include the documentation, the original collected data including its SHA256 hash, and a copy of the original data for further analysis.

A positive example is the acquisition of data using OBD-II and a predefined tool-set that is known and accepted by the forensic community. Communication between analysis computer and vehicle is performed by using the selected tool-set. Collected data is stored and duplicated to avoid changes of the original data. Another positive example is data acquisition by using the JTAG interface. A connector such as JTAG to USB is used. Identical to the OBD-II example, acquired data is duplicated to prevent unintentional changes of original data. While performing both acquisition methods, every step is documented.

In a negative example, implementation of *offline forensic techniques* is utilized. Furthermore, an analyst tries to acquire data multiple times without a prior plan. As a result, the overall system is damaged and evidence is tampered or even destroyed. The integrity and reproducibility requirement can not be fulfilled.

5.3 Analysis Phase

In [51], German BSI defined the analysis phase where log files might need to be correlated in order to create evidence trails. Carrier and Spafford stated that during analysis phase, a reconstruction of events, occurred throughout the incident, is performed [14]. Both sources display that the goal of analysis phase is a reconstruction of events to create logical and comprehensive evidence trails.

A copy of the original collected data is used for analysis to fulfill the integrity requirement. Correlation of logs needs to be logical and comprehensive to handle the consistency and correlation problem. In addition, errors and problems can occur during analysis phase. If so, faulty circumstances and present error messages need to be documented. Similar to error handling during acquisition phase, the step which led to the error must be redone. This ensures to fulfill the reproducibility requirement.

Vehicles introduce a lot of data sources. As mentioned in Chapter 2, it includes ECUs, gateways, bus systems, and more. Communication logs allow correlation and construction of evidence trails. Furthermore, it is possible to correlate data from ECUs with information collected from smartphones. GPS data from the smartphone are comparable with GPS information from the car. Those methods allow to collect evidence from two separate device types. If data on the smartphone is tampered by an adversary, data from in-vehicle systems is still trustworthy and usable. In general, this phase aims to fulfill the reproducibility, integrity, and consistency requirement. The unified time-lining problem must be handled, if different sources of data are addressed. Here, interpretation of time is of interest to build comprehensive and logical evidence trails.

Figure 5.5 presents the detailed structure of the analysis phase. While conducting different steps of the analysis phase, all performed activities are documented. As a result, the reproducibility requirement is fulfilled.

At the beginning of an analysis phase, the amount of data is relatively high. Therefore, an initial inspection of collected data is performed. The complexity as well as quantity or volume problem are addressed.

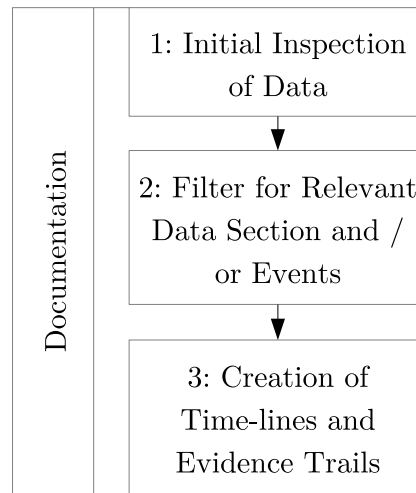


Figure 5.5: Structure of the Data Analysis Phase

Next, filters for relevant data section and / or events are applied. The goal is to determine data sections and / or events, that are usable as evidence in potential prosecutions. It is important to answer stated questions for the forensic investigation. The complexity problem is addressed and the relatively high amount of data is stripped down to only interesting parts.

Third, creation of time-lines and evidence trails is utilized. This is feasible by using specific tools or manually. Goal is to handle the unified time-lining problem and build comprehensive and logical evidence trails. The consistency requirement is fulfilled, if time-lines and evidence trails are reproducible by any third-party.

An implementation of this phase includes inspection of acquired data using a predefined tool such as Wireshark for PCAP files. Next, data is separated into smaller chunks. Filtering for specific types of events (e. g. only successful requests as presented in Figure 5.6) is an option. Positive responses contain usable information such as data identifiers, DTCs, ECU version numbers, and more. The use of tools allow automated analysis of data (e. g. SANS SIFT¹). Other tools are able to build time-lines based on collected data (e. g. Plasos log2timeline²).

¹<https://digital-forensics.sans.org/community/downloads> last accessed 16. December 2019

²<https://github.com/log2timeline/plaso> last accessed 16. December 2019

Figure 5.6: UDS Read Data by Identifier - Positive Response

Result of the analysis phase is the creation of logical and comprehensible evidence trails.

A positive example for a successful analysis phase is an examination of captured network traffic from an in-vehicle gateway. As a result, reconstruction of events based on timestamps, is performed. An identification of different entities, their connection times, and interaction events are used to build logical and comprehensible evidence trails.

Extraction of data from an ECU and wrong interpretation of this data are defined as a negative example. If a forensic analyst comes to hypothetical conclusions based on wrong interpretation of data, another negative example is given. Such conclusions and corresponding results might not be accepted by a judge, because the robustness, integrity, and consistency requirement are not met.

5.4 Documentation Phase

Merriam-Webster defines documentation as "*the provision of documents in substantiation*" [68]. The phase aims to create paperwork that allows third-parties to reconstruct performed tasks and present a transparent as well as comprehensible documentation of the forensic investigation.

It is important to provide the document in human readable form and an appropriate format such as PDF. Key points from prior phases need to be pointed out. In-depth explanation of all performed steps are required to allow reconstruction of the forensic investigation. Hence, the reproducibility requirement is fulfilled. Time stamps of performed actions and the creation as well as review date of the final report must be part of the document.

Similar to documentation in other area of application, this phase is important for automotive forensics too. During legal proceeding, the final report will be used to present collected evidence. This evidence must withstand all questions from the judge and other involved entities. Inconsistencies and inaccurate reports may raise more questions than it should answer.

Figure 5.7 displays the documentation phase in more detail. First, a collection of all documentations from prior phases is utilized. The goal is to describe performed steps for all prior phases of the automotive forensics concept.

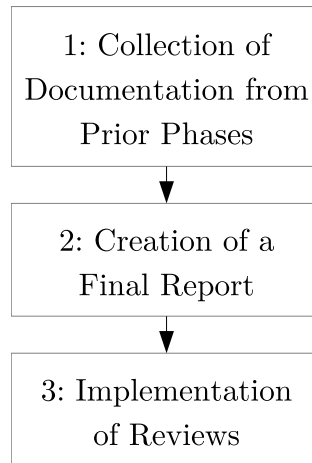


Figure 5.7: Structure of the Documentation Phase

Second, a consolidation of all document pieces into one final report is performed. This allows any third-party to reproduce results and perform the automotive forensics analysis themselves. As a result, the reproducibility requirement is fulfilled.

Finally, an implementation of reviews is utilized, The goal is to avoid inconsistencies and fulfill the consistency requirement.

The outcome of this phase is a final report in human readable format.

A positive example is a PDF document including different paragraphs for prior phases. The timeline of performed steps is visible, the final report is ready for court presentations, and no inconsistencies are present.

If everything is documented without a visible structure and inconsistencies a negative example is given.

5.5 Summary

This chapter displays a concept for automotive forensics. It consists of four different phases. A forensic readiness phase to determine the level of forensic capabilities including presence of suitable data sources and tool-sets. Next, an acquisition phase, which gathers data from selected sources by using a specific tool-set as well as setup. Third, the analysis phase where collected data is analysed to create logical and comprehensible evidence trails. Finally, a documentation phase, to prepare all findings, procedures, and results within a final report.

Chapter 6

Implementation of Automotive Forensics Concept Based on a Modern Vehicle

This chapter presents an implementation of the automotive forensics concept phases introduced in Chapter 5.

Chapter 4.2 described multiple scenarios with relevance for OEMs, legal entities, and insurance companies. In this implementation, a modification of engine parameters is chosen as a scenario. As stated by the insurer Allianz in [4], unauthorized and unregistered software changes lead to loss of insurance cover. In some cases even in loss of vehicle registration. If modifications are performed, the resulting software states are not tested by the manufacturer. Due to this, safety requirements are not fulfilled.

The selected vehicle is manufactured by an OEM from the premium segment and it was build in 2018.

The implementation of the concept was structured as follows: First, each phase of the automotive forensics concept (*A* to *D*) was implemented. Next, each step (*1* to n^1) within the phases was performed accordingly. A presentation of the final acquisition setup is displayed in the Subsection 6.2.4 (step *B:4*). During implementation, we aimed to fulfill requirements and handle challenges presented in Chapter 4.

¹The value differs for each phase.

6.1 Determining Forensic Readiness of a State-of-the-art Vehicle (A)

Initially, forensic readiness for the targeted vehicle was determined. During all steps, detailed documentation was performed.

6.1.1 Analysis of Potential Data Sources (A:1)

Starting with phase *A*, potential data sources for the vehicle of interest were analysed. To achieve this, two different instruments were used, common literature and visual inspection of the car.

During implementation of the automotive forensics concept, no internal documentation for the vehicle was available. Hence, common literature was chosen as the first instrument. Chapter 2 described vehicle data sources including DTCs, USB, SD cards, EEPROM, RAM, flash, and EDRs. Due to this foundation, several possible data storage points were detected. No publicly available resources regarding model or manufacturer specific storage devices were noticeable. Possible examples are EDR, Black Boxes, and Data Loggers.

By performing visual inspection of the car, modern technology and assistance systems was noticeable. Such components store configuration parameters in EEPROM and flash memory. The used storage technology depends on ECU implementation. In addition, the installed infotainment system allows to store multi-media related information.

6.1.2 Determination of Interfaces and Data Exchange Methods (A:2)

Chapter 2 presented technologies including OBD-II and JTAG. As displayed in Figure 6.1, the OBD-II standard introduces PINs for different protocols such as CAN, LIN, Ethernet, and manufacturer specific ones [29]. The used protocol depends on the ECU implementation.

JTAG is available, if the ECU would be taken out of the car and if the interface would be still enabled. Manufacturer disable JTAG to prevent debugging capabilities on the component. The interface would allow to collect

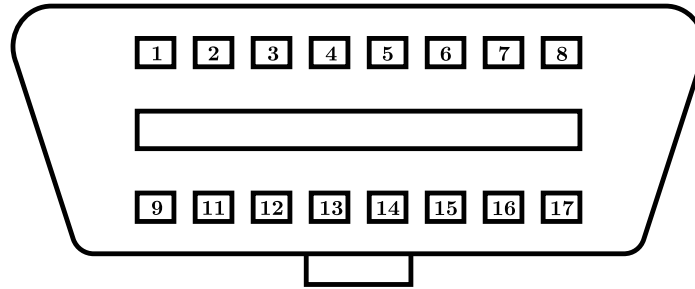


Figure 6.1: Connector Output of a Female OBD-II Interface

- | | |
|------------------------------|------------------------------|
| 1 : Manufacturer Discretion | 2 : SAE J1850 |
| 3 : Manufacturer Discretion | 4 : Chassis Ground |
| 5 : Signal Ground | 6 : CAN High |
| 7 : K-Line ISO 9141-2 | 8 : Manufacturer Discretion |
| 9 : Manufacturer Discretion | 10 : SAE J1850 |
| 11 : Manufacturer Discretion | 12 : Manufacturer Discretion |
| 13 : Manufacturer Discretion | 14 : CAN Low |
| 15 : L-Line ISO 9141-2 | 16 : Battery Power |

cryptographic secrets and tamper the device (e. g. flash custom firmware on the ECU).

Infotainment specific interfaces and data exchange methods were identified too. USB sticks and SD cards are one example. At the REcon security conference in 2018, Regalado et al. presented a new attack vector over USB [79]. The authors targeted vehicle infotainment systems over this data exchange method. Another example for an infotainment specific data exchange method we identified was Bluetooth.

LTE is used for manufacturer back-end communication and allows services like live weather feed. WLAN is utilized for communication of systems located within the car. Smartphones are one example. Both technologies were present at the car and corresponding devices might hold valuable data.

Another method to acquire information was by desoldering components from the logical or main board and perform embedded forensics. In [58], Jacobs et al. implemented forensic analysis on a Volkswagen infotainment system by performing a chip-off. By utilizing this destructive method, on-board chips are removed from a component. The data they are holding is read with a separate device.

6.2 Performing Data Acquisition on a State-of-the-art Vehicle (*B*)

As presented in phase *A*, forensic readiness for the vehicle of interested was given. The next phase was *B* where data acquisition was performed. Detailed documentation was conducted during all steps.

6.2.1 Determination of Model Variant and Vehicle Series (*B:1*)

To achieve a determination of model variant and vehicle series, the Vehicle Identification Number (VIN) of the car was collected. The 17 digit number was visible from the outside and was documented in the vehicle manual. For European cars, the first three digits are world manufacturer identifier. The German *Kraftfahrt-Bundesamt* (federal motor vehicle transport authority) presented different manufacturer identifier in [59]. Digits 4 to 8 describe general characteristics of the car. For each vehicle type (e. g. passenger car, truck, motorcycle, etc.) different information is displayed. Digit 9 holds a checksum calculated by using the other 16 digits. The last section (digits 10 to 17) describes the identification of the car. It includes model year, production number, and more. In Germany, VINs might be personal information. In [63], the state representative of data protection for Niedersachsen gave an unclear statement, if a VIN is personal information or not. As a result, we will not show the VIN of the targeted vehicle in this master thesis.

Another method to determine model variant and vehicle series was by visual inspection. Based on visible logos, model labels, and unique design, we were able to identify the vehicle of interest.

6.2.2 Evaluation of Chosen Data Sources (*B:2*)

During step *B:2*, we evaluated the presented data sources from section *A:1* and determined which we used during the acquisition phase.

As presented in Chapter 2, the amount of available data sources was one challenge we encountered during this step. Another difficulty was to choose one of those. Due to the lack of manufacturer-internal documentation, we had to find appropriate publicly available literature. This type of source

was limited because of the lack of research done in the automotive forensics domain.

Changes of software and hardware configuration parameters, versions, access timestamps, and more are stored in EEPROM and flash memory. The exact storage medium depends on the ECU implementation. To answer questions for the stated scenario, we chose to acquire EEPROM and flash memory.

6.2.3 Selection of an Interface and Data Exchange Method (*B:3*)

To not damage the vehicle by taking apart components, *live forensics* and *online analysis* were selected. JTAG was not in the focus because we did not had physical access to the logic board of ECUs. Therefore, the OBD-II interface was chosen. In the target vehicle the OBD-II interface is located below the steering wheel.

6.2.4 Determination of the Final Acquisition Setup and Tool / Instrument Check (*B:4*)

Following, the final acquisition setup was determined and a tool / instrument check was performed.

The final setup is displayed in Figure 6.2². First, an Apple MacBook Pro running macOS 10.14 Mojave was chosen as an analysis computer. In addition, different tools were developed. These implemented a Python³ version 2.7 framework for the publicly available DoIP and UDS standards. It introduces all message types and structures defined by the corresponding standards. Additionally, a scanning application utilizing the protocol implementation was developed. In this case, the Python version 2.7 programming language was chosen too. This application allowed us to determine all installed in-vehicle components, which are connected to the OBD-II port. Traffic between analysis computer and car was captured in Packet Capture (PCAP) files. To achieve this, Wireshark⁴ version 2.6 was used. The packet anal-

²Icons provided by Justin Blake, Arthur Shlain, C. V. Galli, Vectorstall, and Xoneca.

³<https://www.python.org/> last accessed 16. December 2019

⁴<https://www.wireshark.org/> last accessed 16. December 2019

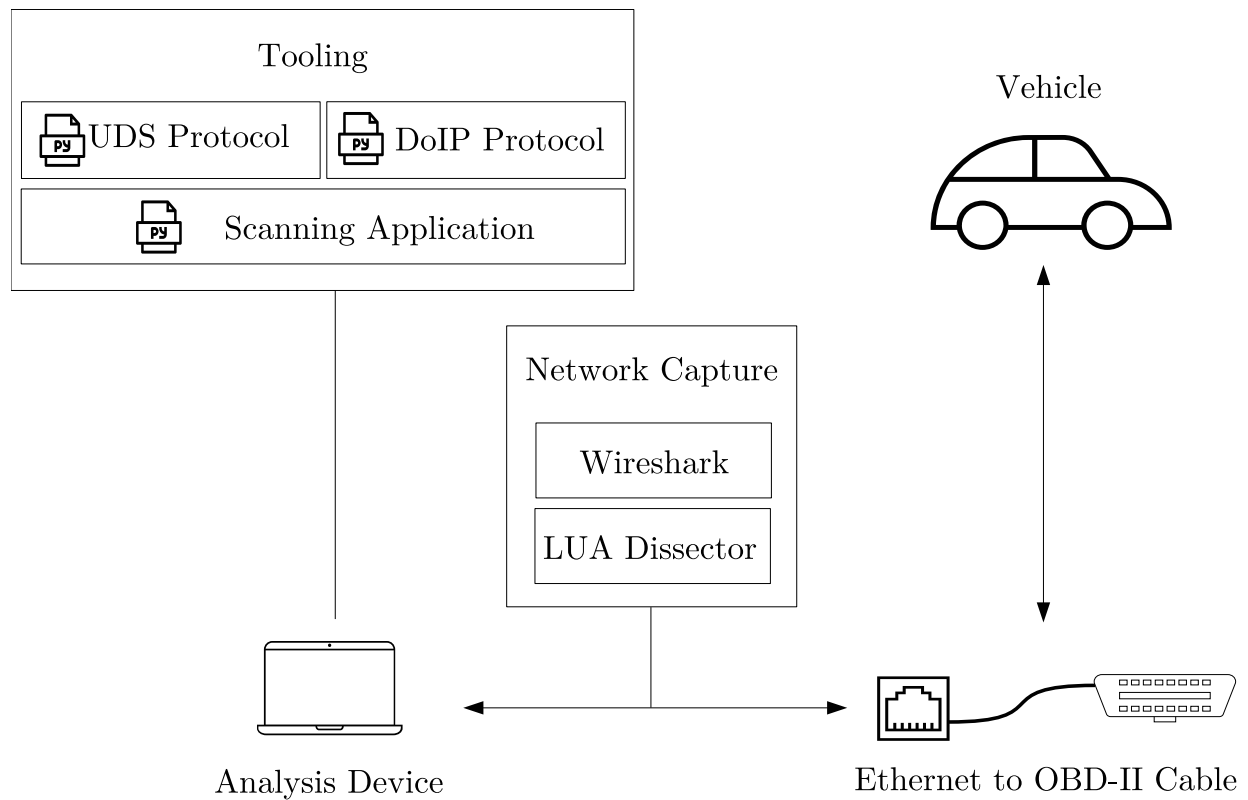


Figure 6.2: Data Acquisition Setup

user allowed to capture all events on a specific networking interface and store them as a PCAP file. Per default, Wireshark comes with a variety of different packet dissectors already implemented by the community. Those are either programmed in the C or LUA⁵ programming language and used to decode parts of a protocol to make them more readable for humans. No DoIP and UDS dissector was publicly available. Therefore, we implemented a dissector for both protocols in the LUA programming language.

To implement a tool / instrument check, we used a similar vehicle. We connected the analysis computer to the car over OBD-II and communicated with different ECUs to determine functionality. Everything went fine and no error occurred during this step.

⁵<https://www.lua.org/> last accessed 16. December 2019

6.2.5 Implementation of Data Acquisition (*B:5*)

Data acquisition was the next step for the implementation of the automotive forensics concept.

First, the scanning tool was used to create a JSON file with all devices connected to the diagnostic interface. We captured more than 100 unique TAs and therefore installed devices.

Next, we started to capture traffic and iterated over all UDS identifiers listed in [26, p. 259-263] for all installed devices. Depending on the ECU implementation we received data. The PCAP file was saved after the iteration was done. During acquisition, no error occurred.

Figure 6.3 and Figure 6.4 display screenshots for some of the corresponding events that were captured. Figure 6.3 presents the ID of the last used equipment serial number of a repair shop in the *Data Record String* field. Figure 6.4 displays the name of a corresponding Open Diagnostic Data Exchange (ODX) file for a specific ECU. Those files store information such as temperature or voltage of the corresponding component. After all UDS data identifies are requested and the network packets were captured by Wireshark, the traffic was saved as a PCAP file.

No.	Time	Source	Destination	Protocol	Length	Info
1030	79.911810	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
1031	79.911999	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
1032	79.913139	192.168.88.249	192.168.88.238	UDS	93	Read Data By Identifier Positive Response
1033	79.913314	192.168.88.238	192.168.88.249	TCP	60	██████████ → 13400 [ACK] Seq=287 Ack=565 Win=63676 Len=0
1034	79.967631	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
1035	79.967785	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
1036	79.968097	192.168.88.249	192.168.88.238	UDS	76	Read Data By Identifier Positive Response
1037	79.968119	192.168.88.238	192.168.88.249	TCP	60	██████████ → 13400 [ACK] Seq=302 Ack=600 Win=63641 Len=0
1038	80.072284	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
1039	80.072353	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
1040	80.073176	192.168.88.249	192.168.88.238	UDS	101	Read Data By Identifier Positive Response
1041	80.073208	192.168.88.238	192.168.88.249	TCP	60	██████████ → 13400 [ACK] Seq=317 Ack=660 Win=63581 Len=0
1042	80.295293	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
1043	80.295398	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
1044	80.297394	192.168.88.249	192.168.88.238	UDS	75	Read Data By Identifier Positive Response
1045	80.297423	192.168.88.238	192.168.88.249	TCP	60	██████████ → 13400 [ACK] Seq=332 Ack=694 Win=63547 Len=0
1046	80.323649	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
1047	80.323872	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
1048	80.324340	192.168.88.249	192.168.88.238	UDS	75	Read Data By Identifier Positive Response
1049	80.324454	192.168.88.238	192.168.88.249	TCP	60	██████████ → 13400 [ACK] Seq=347 Ack=728 Win=63513 Len=0
1050	80.344128	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
1051	80.344316	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK

▶ Frame 1044: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
 ▶ Ethernet II, Src: ██████████
 ▶ Internet Protocol Version 4, Src: 192.168.88.249, Dst: 192.168.88.238
 ▶ Transmission Control Protocol, Src Port: 13400, Dst Port: ██████████, Seq: 673, Ack: 332, Len: 21
 ▶ Diagnostics over Internet Protocol
 ▼ Unified Diagnostic Service
 Service Identifier: 0x62 (Read Data By Identifier Positive Response)
 Suppress Response: True (0x80)
 Data Identifier: 0xf19a (Data Identifier 1)(Calibration Repair Shop Code Or Calibration Equipment Serial Number Data Identifier)
 Data Identifier MSB: 0xf1 (Data Identifier 1 MSB)
 Data Identifier LSB: 0x9a (Data Identifier 1 LSB)
 Data Record String: \357\277 ██████████

Packets: 3883 · Displayed: 3883 (100.0%) Profile: Default

Figure 6.3: UDS Service Identifier Result - Calibration Repair Shop Code Or Calibration Equipment Serial Number

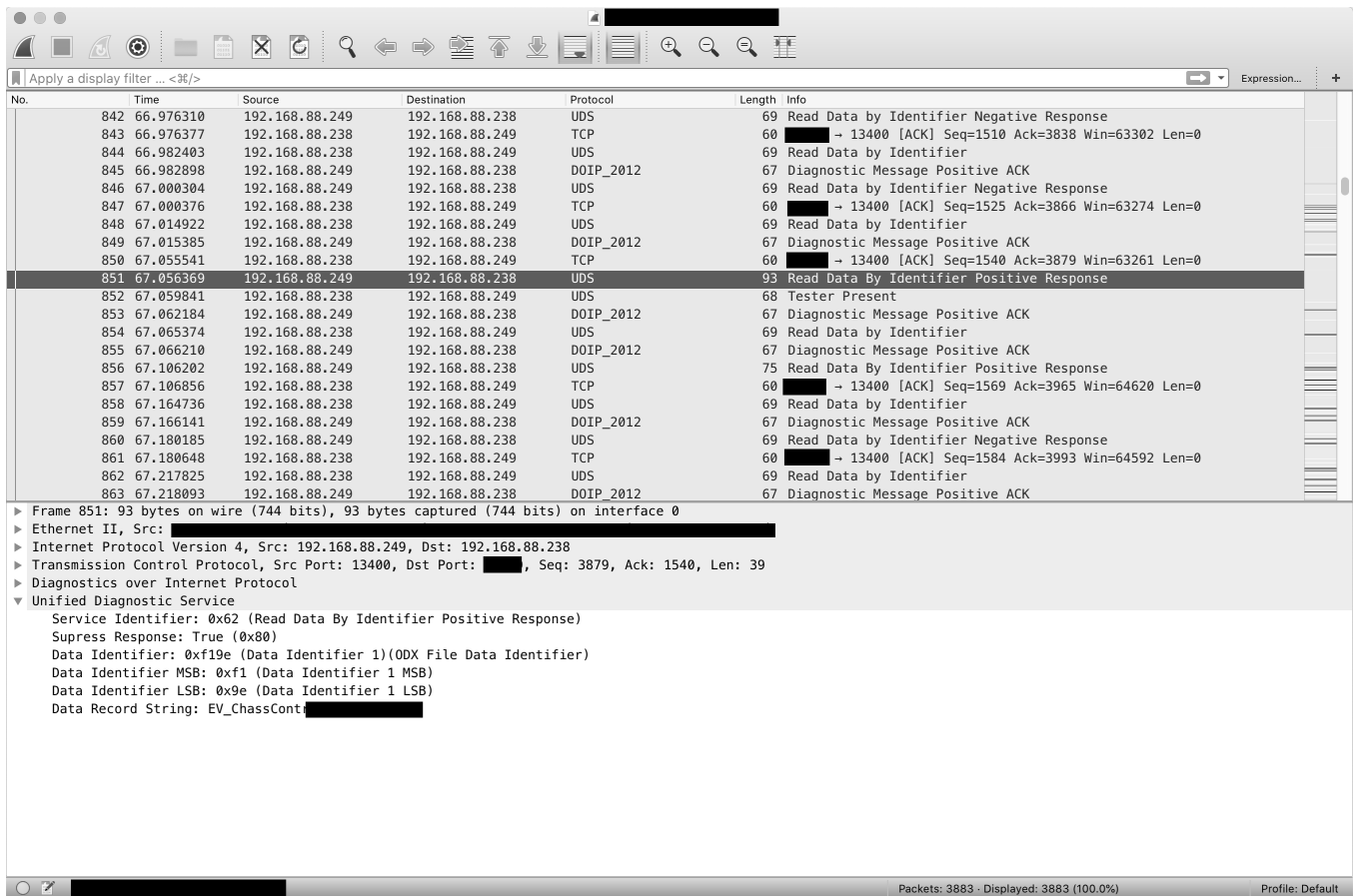


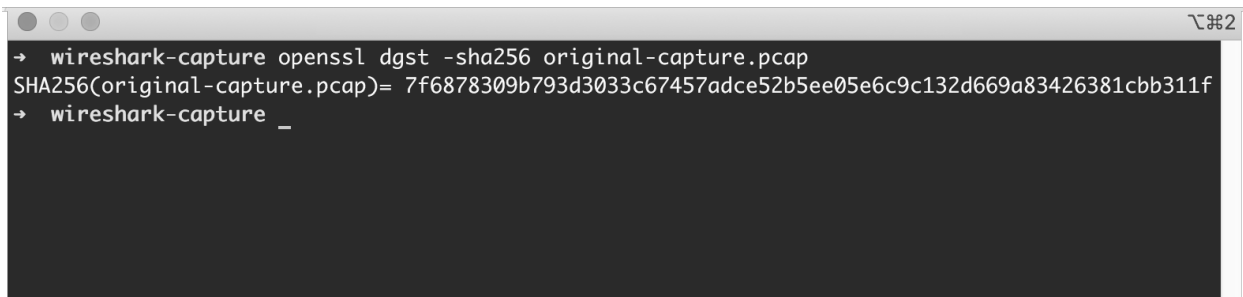
Figure 6.4: UDS Service Identifier Result - ODX File

6.2.6 Duplication of Original Evidence (*B:6*)

The last step of phase *B* was to perform a duplication of original evidence.

To avoid changes of the original collected information, the PCAP was duplicated using the *cp* Command-Line Interface (CLI) tool. The command "`cp original-capture.pcap duplicated-capture.pcap`" was used.

Next, the tool *openssl-sha265*, from the *openssl* library, was used to create a SHA256 hash of the PCAP file. It allows to create hashes for files and folders. As presented in Figure 6.5, the command "`openssl dgst -sha256 original-capture.pcap`" was utilized.



```
→ wireshark-capture openssl dgst -sha256 original-capture.pcap
SHA256(original-capture.pcap)= 7f6878309b793d3033c67457adce52b5ee05e6c9c132d669a83426381cbb311f
→ wireshark-capture _
```

Figure 6.5: SHA256 Hash of the Original PCAP File

Both, the hash and original PCAP, were moved to an external hard drive.

6.3 Analysis of Collected Data (*C*)

The third phase (*C*) was analysis of collected data. During all steps, detailed documentation was performed.

6.3.1 Initial Inspection of Data (*C:1*)

The first step of this phase, was an inspection of the collected data.

More than 3800 unique events were captured in step *B:5*. As described in Chapter 2, some events presented manufacturer specific requests. This data was not interpretable because no manufacture documentation was available. In addition, lots of negative responses were captured. Figure 6.6 displays three events (frame 538, 542, and 553) that present a negative response for a *Read Data by Identifier* UDS request. If a requested *Read Data by Identifier* messages is not attainable by an ECU, a negative response will be send and no usable data is provided. Furthermore, communication structure specific events (e. g. TCP ACKs and NAKs) were captured too. They were not relevant for forensic analysis, because no data such as hard- and software identifiers, configuration data, and more were supplied.

538	62.884150	192.168.88.249	192.168.88.238	UDS	69	Read Data by Identifier Negative Response
539	62.884320	192.168.88.238	192.168.88.249	TCP	60	██████ → 13400 [ACK] Seq=379 Ack=1539 Win=64161 Len=0
540	62.889958	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
541	62.890353	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
542	62.905235	192.168.88.249	192.168.88.238	UDS	69	Read Data by Identifier Negative Response
543	62.905581	192.168.88.238	192.168.88.249	TCP	60	██████ → 13400 [ACK] Seq=394 Ack=1567 Win=64133 Len=0
544	62.919842	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
545	62.920442	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
546	62.960617	192.168.88.238	192.168.88.249	TCP	60	██████ → 13400 [ACK] Seq=409 Ack=1580 Win=64120 Len=0
547	62.971576	192.168.88.249	192.168.88.238	UDS	87	Read Data By Identifier Positive Response
548	62.974381	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
549	62.975205	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
550	62.991446	192.168.88.249	192.168.88.238	UDS	75	Read Data By Identifier Positive Response
551	62.991916	192.168.88.238	192.168.88.249	TCP	60	██████ → 13400 [ACK] Seq=424 Ack=1647 Win=64053 Len=0
552	63.042865	192.168.88.238	192.168.88.249	UDS	69	Read Data by Identifier
553	63.043013	192.168.88.249	192.168.88.238	DOIP_2012	67	Diagnostic Message Positive ACK
554	63.044107	192.168.88.249	192.168.88.238	UDS	69	Read Data by Identifier Negative Response

Figure 6.6: UDS Read Data by Identifier - Negative Response

6.3.2 Filter for Relevant Data Section and / or Events (C:2)

After the initial inspection, filtering of the collected data was performed.

To determine if changes to software or hardware happened, different filters were developed. Indicators for the entity who changed the data was of interest. The Wireshark filter "uds.service_identifier == 0x62" was used to strip down the number of events. Due to this, only positive responses and no communication structure data were visible. The number of displayed events decreased to 245.

Following, filters to answer stated questions were created. The goal was to determine the last entity that performed changes to in-vehicle systems. It includes the last used tester serial number, repair shop code or equipment serial number, and more. Table 6.1 displays corresponding UDS data identifiers. Those were used in additional filters to look explicitly at those.

6.3.3 Creation of Time-line and Evidence Trails (C:3)

Next, a time-line was created. It was based on the filtered results from step C:2.

No available tool for automated creation of time-lines based on DoIP and UDS events was present. This problem resulted in the manual creation of a time-line. While inspecting the filtered events, a change of the last active tester was identified. The corresponding event displayed its serial number.

Data Identifier in Hex	Description
0xf180	<i>bootSoftwareIdentificationDataIdentifier</i>
0xf181	<i>applicationSoftwareIdentificationDataIdentifier</i>
0xf183	<i>bootSoftwareFingerprintDataIdentifier</i>
0xf184	<i>applicationSoftwareFingerprintDataIdentifier</i>
0xf198	<i>repairShopCodeOrTesterSerialNumberDataIdentifier</i>
0xf199	<i>programmingDateDataIdentifier</i>
0xf19a	<i>calibrationRepairShopCodeOrCalibration-EquipmentSerialNumberDataIdentifier</i>

Table 6.1: UDS Data Identifier to Determine Modification of Software or Hardware

However, no change of software or hardware was identified after the last active tester changed. The UDS data identifier *programmingData* was not noticeable.

6.4 Documenting the Automotive Forensics Process

Last phase (*D*) was the final documentation of all prior performed steps.

6.4.1 Collection of Documentation from Prior Phases and Steps (*D:1*)

The collection of the documentation from prior phases (*A* to *C*) was utilized in the first step of *D*. For each stage an according section including a paragraph was created. The structure was similar to the current chapter of this master thesis.

6.4.2 Creation of a Final Report (*D:2*)

A human readable PDF document was created in this step of phase *D*. In-depth explanation of all performed steps (*A:1* to *C:3*) were included into the report. In addition, stated questions of the scenario were answered in the documentation.

6.4.3 Implementation of Reviews (*D:3*)

To avoid inconsistencies and errors in the final report, reviews were performed. Another analyst (not the original author) utilized this step. After a successful review, the analyst signed the PDF document.

6.5 Summary

This chapter performed the concept for automotive forensic analysis on a modern and state-of-the-art vehicle. As a result, a documentation report with all relevant information and steps performed during the analysis, is available. If necessary, results are presentable in front of court by a forensic analyst.

Chapter 7

Evaluation of the Automotive Forensic Analysis

Chapter 5 presented the concept, which was then implemented in Chapter 6 on a modern vehicle. Goal was to fulfill requirements and handle challenges presented in Chapter 4. This chapter evaluates the automotive forensics analysis.

The structure of this chapter is as follows: First, the practical applicability of the automotive forensics concept is determined. Second, a resulting gap-analysis is performed.

7.1 Practical Applicability of the Presented Automotive Forensics Concept

The following sections evaluate all phases (A to D) and their corresponding steps (1 to n^1) while looking at the fulfillment of requirements and handling of digital forensics challenges.

7.1.1 Evaluation of Phase A – Forensic Readiness

Collected potential data sources ($A:1$), interface and data exchange methods ($A:2$), and tool-set(s) ($A:3$) are based on publicly available literature and

¹The value differs for each phase.

resources. Those are published and accepted by the community. Due to this, acceptance, functionality, and reproducibility requirement are fulfilled.

The performed visual inspection in step *A:1* allowed to determine car specific technologies. However, internal documentation would allow to perform more precise evaluation of forensic readiness. Additional data storage points for a specific vehicle would be identifiable. Actual and recommend implementation of ECUs can differ. Standards, norms, and best practises for car components are not mandatory for manufactures. As a result, the functionality requirement is improvable and the complexity problem is more manageable with internal documentation.

7.1.2 Evaluation of Phase *B* – Data Acquisition

In step *B:1*, determination of model variant and vehicle series was conducted by using the VIN. This identifier is standardized and differs between geographical areas (e. g. Europe and Asia). Hence, this type of determination is applicable for all cars in one region. Visual inspection of the car allowed to determine manufacturer and vehicle model too. It was utilized based on logos and design of the car. Due to both methods, the acceptance, functionality, robustness, reproducibility, and consistency requirement are fulfilled. The complexity problem is manageable because no interaction with installed devices is necessary.

Step *B:2* selected flash and EEPROM storage as data sources. In [75], Park et al. evaluated that flash is usable in forensic analysis. Casadei et al. used EEPROM to perform forensic analysis on SIM cards [15]. Both publications lead to a fulfillment of the acceptance requirement. At this point in time, no tamper proof storage is used in vehicles. The integrity requirement is not fulfilled.

For step *B:3* we chose *live forensics* and *online analysis*. As presented in Chapter 4, both allow fast acquisition and prevention of damage to the overall system. However, they provide less data compared to *post-mortem forensics* and *offline analysis*. The quantity or volume problem is manageable.

The used connection interface is OBD-II. Due to its standardization, the acceptance, reproducibility, robustness, and functionality requirement are fulfilled. The diagnostic interface connects multiple devices together. It allows to acquire a lot of data from different components over one interface. Those characteristics lead to manageability of the quantity or volume problem. The easy access to the interface results in manageability of the accessi-

bility and complexity problem. In addition, the reproducibility requirement is fulfilled.

B:4 described that an OBD-II to Ethernet cable was used. Because of the standardization of OBD-II, data translation to Ethernet is implementable.

Python was used as a programming language. Both, the framework and scanning application are academic code. They are not tested properly. However, the framework was developed based on DoIP and UDS standards. It leads to fulfillment of the acceptance requirement.

PCAP is part of the *libpcap* repository and usable for all common operating systems. The format is used in different research projects [24][3][10] for anomaly detection in networks. To capture PCAP files, Wireshark was utilized. It is one of the main network traffic analyser tools and has proven to work in [73]. We chose LUA because no compilation is necessary. The LUA dissector is academic code too. For PCAP, Wireshark, and LUA the acceptance and functionality requirements are fulfilled because no error occurred during implementation of the automotive forensics concept.

During the step *B:5*, no error occurred. Therefore, no faults within the tool-set are noticeable. This leads to fulfillment of the functionality requirement.

The last step for the data acquisition phase is *B:6*. Duplication of the collected PCAP file ensures integrity. The used SHA256 hash algorithm is seen as cryptographic secure as presented by Preneel in [77].

7.1.3 Evaluation of Phase *C* – Data Analysis

Based on the scenario, different filters are applied in step *C:2*. The reduction of events lead to a manageability of the complexity, consistency and correlation, as well as the quantity or volume problem.

Manufacturer specific UDS data identifiers would allow more information for forensic analysis. To make usage of this, internal documentation or reverse engineering for the specific manufacturer are necessary.

Integrity of time stamps is not given because they can differ between ECU implementation. No documentation of the different in-vehicle components was available. The unified time-lining problem is not manageable.

During step *C:3*, manual analysis was conducted. Due to the human factor, mistakes can occur. Automated analysis would eliminate this coefficient.

7.1.4 Evaluation of Phase *D* – Documentation

The PDF format is portable to other representation standards and programs. It is standardized by Adobe in [1]. Due to this, the functionality, reproducibility, and robustness requirements are fulfilled.

In step *D:3*, reviews are performed by another person. This ensures to give an additional view on the final report. Error and inconsistencies are eliminated. Consistency and correlation problem are manageable. The acceptance and consistency requirements are fulfilled.

7.2 Gap Analysis

Based on the prior evaluation, a gap analysis is performed.

7.2.1 Gaps of the Automotive Forensics Concept

During implementation of the automotive forensics concept in Chapter 6, no gaps in the process are identifiable.

Increased adaptability of the concept to other vehicle models is performable by creating an abstract model of cars to identify data sources. It can be used to determine, which questions are answerable by a forensic investigation. Based on this model, an abstract to in-depth concept is utilisable. First, acquisition over OBD-II to in-depth analysis using embedded forensics is an example.

7.2.2 Gaps in the Used Tools and Instruments

The framework is academic code and therefore not properly tested (e. g. unit tests). It further must be extended with other protocols such as SOME/IP to ensure adaptability on other vehicle models.

The current implementation is applicable over OBD-II only. Another increase in functionality is achievable by extending the framework with other communication interfaces such as LTE, Bluetooth, or WLAN. Internal documentation and / or reverse engineering of manufacturer specific implementations would also increase the amount of collectable data.

7.2.3 Gaps in the Targeted Vehicle

The vehicle of interest implements no tamper proof storage. Flash as well as EEPROM allow read and write operations. An attacker is able to overwrite stored data. This results in loss of integrity for the collected data.

Modern vehicles introduce no dedicated storage system to collect events over multiple in-vehicle components. Examples are event based EDRs as presented by Böhm et al. in [13], black boxes, data loggers, and data collectors. Those can further be expanded with security related events to answer the 6 H's of forensic investigations as presented in Chapter 2.

Internal documentation or reverse engineering of all in-vehicle components allow to perform faster and more extensive forensic analysis on cars. Those resources allow to close gaps for forensic analysis in modern vehicles.

Chapter 8

Conclusion and Future Work

Chapter 1 stated three research questions. First, "*Is it possible to perform forensic analysis on state-of-the-art vehicles?*", second, "*How resilient are the results in court?*", and third, "*What potential shortcomings and gaps within state-of-the-art vehicles are identified and must be addressed?*".

To answer those questions, an automotive forensics concept with four phases was implemented. A forensic readiness phase to determine, if the acquisition object contains valuable data and if a tool set is ready to collect as well as analyse possible evidence was utilized. Next, a data acquisition phase, to collect data over OBD-II, DoIP, and UDS was performed. During the third phase, a copy of gathered data was analysed. Results are logical and comprehensible evidence trails, which are reconstructable by any third-party. Finally, a documentation phase was performed. All prior phases are documented in a human-readable format (PDF). Based on this, any third-party is able to comprehend the results and the report is ready for any legal proceeding or prosecutions.

The answer for the question "*Is it possible to perform forensic analysis on state-of-the-art vehicles?*" is yes. Chapter 2 (fundamentals) and Chapter 6 (implementation of the automotive forensics concept) clearly displayed the amount of information in vehicles, which allow an implementation of forensic analysis. Furthermore, existing tools and standards allow acquisition of potential evidence by using those.

An answer of the question "*How resilient are the results in court?*" depends on the acquired data source. In this master thesis, all collected evidence and results (DoIP/UDS messages) are usable in court, because of

the fulfillment of all displayed requirements. However, tamper-proof storage within a vehicle must be ensured in order to fulfill the integrity requirement.

To answer the third question, the Python framework as well as LUA script need to implement other standards too. A possible feature for future work is an expansion for other protocols such as SOME/IP. If those gaps are closed and the presented concept is accepted by the community, forensic analysis for automotive systems are able to withstand legal proceeding and prosecutions.

Future work for automotive forensics will focus on other interfaces. Modern and future vehicles introduce connection interfaces such as 4G. Usability for those acquisition points will be evaluated in future work. Furthermore, an abstract view on possible automotive data will be evaluated too. This includes the realisation of initial triage and fast forensic acquisition on vehicles without and with EDRs.

Bibliography

- [1] Adobe. Document management — Portable document format — Part 1: PDF 1.7. online, 2008.
- [2] I. T. AG. AURIX™ 32-bit microcontrollers for Automotive and Industrial Applications - Highly Integrated and Performance Optimized. Technical Report B158-I0090-V5-7600-EU-EC-P, Infineon Technologies AG, 81726 Munich, Germany, February 2019.
- [3] S. T. F. Al-Janabi and H. A. Saeed. A neural network based anomaly intrusion detection system. In *2011 Developments in E-systems Engineering*, pages 221–226. IEEE, 2011.
- [4] Allianz. Wer den Motor aufmotzt, ist rechtlich auf Schleuderkurs. online, 2011.
- [5] I. S. Association. *IEEE 802.3bp-2016 - IEEE Standard for Ethernet Amendment 4: Physical Layer Specifications and Management Parameters for 1 Gb/s Operation over a Single Twisted-Pair Copper Cable*. IEEE Standards Association, September 2016.
- [6] I. S. Association. *IEEE 802.3bw-2015 - IEEE Standard for Ethernet Amendment 1: Physical Layer Specifications and Management Parameters for 100 Mb/s Operation over a Single Balanced Twisted Pair Cable (100BASE-T1)*. IEEE Standards Association, September 2016.
- [7] I. S. Association. *IEEE 802.3-2018 - IEEE Standard for Ethernet*. IEEE Standards Association, June 2018.
- [8] Australian-Government. Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018. online, December 2018.

- [9] Autosar. *SOME/IP Protocol Specification*. AUTOSAR, November 2016.
- [10] L. Bontemps, J. McDermott, N.-A. Le-Khac, et al. Collective anomaly detection based on long short-term memory recurrent neural networks. In *International Conference on Future Data and Security Engineering*, pages 141–152. Springer, 2016.
- [11] Bosch. *CAN FD – CAN Protocol Extension for More Data Throughput*. Robert Bosch GmbH, 2019.
- [12] A. Bretting and M. Ha. Vehicle Control Unit Security using OpenSource AUTOSAR. Master’s thesis in software engineering, Chalmers University of Technology and University of Gothenburg, Gothenburg, Sweden, June 2015.
- [13] K. Böhm, A. Nitsche, K. Birke, and H.-G. Schweiger. Application of Vehicle Control Units as Event Data Recorders in Hybrid and Electric Vehicles. In *EVU Congress 2017*, 10 2017.
- [14] B. D. Carrier and E. H. Spafford. Getting Physical with the Digital Investigation Process. *IJDE*, 2:20, 2003.
- [15] F. Casadei, A. Savoldi, and P. Gubian. Forensics and sim cards: an overview. *International Journal of Digital Evidence*, 5(1):1–21, 2006.
- [16] E. Casey. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, Inc., Orlando, FL, USA, 3rd edition, 2011.
- [17] L. Chunhua, K. Chau, D. Wu, and S. Gao. Opportunities and Challenges of Vehicle-to-Home, Vehicle-to-Vehicle, and Vehicle-to-Grid Technologies. *Proceedings of the IEEE*, 101:2409–2427, 11 2013.
- [18] D. R. Clark, C. Meffert, I. Baggili, and F. Breitingner. DROP (DRone Open Source Parser) your Drone: Forensic ASnalysis of the DJI Phantom III. *Digital Investigation*, 22:S3 – S14, 2017.
- [19] C. Corbett, T. Basic, T. Lukaseder, and F. Kargl. A Testing Framework Architecture for Automotive Intrusion Detection Systems. In P. Dencker, H. Klenk, H. B. Keller, and E. Plöderer, editors, *Automotive - Safety & Security 2017 - Sicherheit und Zuverlässigkeit für*

- automobile Informationstechnik*, pages 89–102. Gesellschaft für Informatik, Bonn, 2017.
- [20] C. Ebert and C. Jones. Embedded Software: Facts, Figures, and Future. *Computer*, 42(4):42–52, 4 2009.
- [21] A. Enbacka and L. Laibinis. *Formal Specification and Refinement of a Write Blocker System for Digital Forensics*. Turku Centre for Computer Science, 2005.
- [22] B. Endicott, N. K. Popovsky, and C. Rudolph. Forensic Readiness: Emerging Discipline for Creating Reliable and Secure Digital Evidence. *Journal of Harbin Institute of Technology (New Series)*, 22(1):99–106, 2015.
- [23] H. Engels. *CAN-Bus: Feldbusse im Überblick, CAN-Bus-Protokolle, CAN-Bus-Meßtechnik, Anwendungen ; [neu: mit TTCAN]*. Franzis, 2002.
- [24] R. Fontugne, J. Mazel, and K. Fukuda. Hashdoop: A mapreduce framework for network anomaly detection. In *2014 IEEE conference on computer communications workshops (INFOCOM WKSHPs)*, pages 494–499. IEEE, 2014.
- [25] I. O. for Standardization. *Road vehicles – Controller area network (CAN) – Part 3: Low-speed, fault-tolerant, medium-dependent interface*, June 2006.
- [26] I. O. for Standardization. *Road vehicles - Unified diagnostic services (UDS)*. International Organization for Standardization, April 2006.
- [27] I. O. for Standardization. *Road vehicles — Vehicle identification number (VIN) — Content and structure*. International Organization for Standardization, October 2009.
- [28] I. O. for Standardization. *Road vehicles - Diagnostic communication over Internet Protocol (DoIP)*. International Organization for Standardization, October 2011.
- [29] I. O. for Standardization. *Road vehicles - Implementation of World-Wide Harmonized On-Board Diagnostics (WWH-OBD) communication*

- requirements*. International Organization for Standardization, August 2012.
- [30] I. O. for Standardization. *Road vehicles – FlexRay communications system – Part 1: General information and use case definition*, February 2013.
 - [31] I. O. for Standardization. *Road vehicles – FlexRay communications system – Part 2: Data link layer specification*, February 2013.
 - [32] I. O. for Standardization. *Road vehicles – FlexRay communications system – Part 3: Data link layer conformance test specification*, February 2013.
 - [33] I. O. for Standardization. *Road vehicles – FlexRay communications system – Part 4: Electrical physical layer specification*, February 2013.
 - [34] I. O. for Standardization. *Road vehicles – FlexRay communications system – Part 5: Electrical physical layer conformance test specification*, February 2013.
 - [35] I. O. for Standardization. *Road vehicles - Controller area network (CAN)*. International Organization for Standardization, December 2015.
 - [36] I. O. for Standardization. *Road vehicles – Controller area network (CAN) – Part 2: High-speed medium access units*, December 2016.
 - [37] I. O. for Standardization. *Road Vehicles – Local Interconnect Network (LIN) – Part 2: Transport Protocol and Network Layer Services*. International Organization for Standardization, August 2016.
 - [38] I. O. for Standardization. *Road Vehicles – Local Interconnect Network (LIN) – Part 3: Protocol Specifications*. International Organization for Standardization, August 2016.
 - [39] I. O. for Standardization. *Road Vehicles – Local Interconnect Network (LIN) – Part 4: Electrical Physical Layer (EPL) Specification 12 V / 24 V*. International Organization for Standardization, September 2016.
 - [40] I. O. for Standardization. *Road Vehicles – Local Interconnect Network (LIN) – Part 5: Application Programmers Interface (API)*. International Organization for Standardization, August 2016.

- [41] I. O. for Standardization. *Road Vehicles – Local Interconnect Network (LIN) – Part 7: Electrical Physical Layer (EPL) Conformance Test Specifications*. International Organization for Standardization, December 2016.
- [42] I. O. for Standardization. *Road Vehicles – Local Interconnect Network (LIN) – Part 8: Electrical Physical Layer (EPL) Specification: LiIN over DC Powerline (DC-LIN)*. International Organization for Standardization, December 2016.
- [43] I. O. for Standardization. *Road Vehicles – Local Interconnect Network (LIN)– Part 1: General Information and Use Case Definition*. International Organization for Standardization, August 2016.
- [44] I. O. for Standardization. *IEEE 802.1Q-2018 - IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks*. IEEE Standards Association, May 2018.
- [45] I. E. T. Force. *User Datagram Protocol*. Internet Engineering Task Force (IETF), August 1980.
- [46] I. E. T. Force. *Internet Protocol*. Internet Engineering Task Force (IETF), September 1981.
- [47] I. E. T. Force. *Transmission Control Protocol*. Internet Engineering Task Force (IETF), September 1981.
- [48] I. E. T. Force. *HTTP Over TLS*. Internet Engineering Task Force (IETF), May 2000.
- [49] I. E. T. Force. *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. Internet Engineering Task Force (IETF), June 2014.
- [50] I. E. T. Force. *Internet Protocol, Version 6 (IPv6)*. Internet Engineering Task Force (IETF), July 2017.
- [51] B. für Sicherheit in der Informationstechnik. *Leitfaden IT-Forensik*. online, 03 2011.
- [52] A. Geschonneck. *Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären*. dpunkt-Verlag, 6 edition, 2014.

- [53] A. Grzemba. *MOST: das Multimedia-Bussystem für den Einsatz im Automobil*. Elektronik- & Elektrotechnik-Bibliothek. Franzis, 2007.
- [54] B. Hay, M. Bishop, and K. Nance. Live Analysis: Progress and Challenges. *IEEE Security Privacy*, 7(2):30–37, March 2009.
- [55] A. Hergenhan and G. Heiser. Operating Systems Technology for Converged ECUs. In *6th Emb. Security in Cars Conf.(escar)*. Hamburg, Germany: ISITS, 2008.
- [56] T. Hoppe, S. Kuhlmann, S. Kiltz, and J. Dittmann. IT-Forensic Automotive Investigations on the Example of Route Reconstruction on Automotive System and Communication Data. In F. Ortmeier and P. Daniel, editors, *Computer Safety, Reliability, and Security*, pages 125–136, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.
- [57] A. Ivanisevic, I. Katic, B. Buchmeister, and M. Leber. Business Plan Feedback for Cost Effective Business Processes. *Advances in Production Engineering & Management*, 11:173–182, 09 2016.
- [58] D. Jacobs, K. R. Choo, M. Kechadi, and N. Le-Khac. Volkswagen car entertainment system forensics. In *2017 IEEE Trustcom/Big-DataSE/ICSS*, pages 699–705, Aug 2017.
- [59] KBA. Verzeichnis der Herstellervon Kraftfahrzeugen und Kraftfahrzeuganhängern - List of manufacturersof motor vehicles and their trailers, 2019.
- [60] M. Kciuk. OpenWRT Operating System based Controllers for Mobile Robot and Building Automation System Students Projects Realization. In *15th International Workshop on Research and Education in Mechatronics (REM)*, pages 1–4, Sep. 2014.
- [61] U. Kindhäuser. Strafgesetzbuch – StGB § 242 Diebstahl, 2017.
- [62] B. Kretschmer. Strafgesetzbuch – StGB § 142 Unerlaubtes Entfernen vom Unfallort, 2017.
- [63] Landesbeauftragte für den Datenschutz Niedersachsen. 10 Fragen und Antworten zum Thema Datenschutz im Kfz. online, 2014.

- [64] P. Lienert. Volkswagen Investment Vaults Argo into Top Ranks of Self-driving Firms. online, July 2019.
- [65] J. T. Luttgens, M. Pepe, and K. Mandia. *Incident Response & Computer Forensics*. McGraw-Hill Education Group, third edition, 2014.
- [66] P. K. Manadhata and J. M. Wing. An Attack Surface Metric. *IEEE Transactions on Software Engineering*, 37(3):371–386, May 2011.
- [67] K. Matheus and T. Königseder. *Automotive Ethernet*. Cambridge University Press, 2 edition, 2017.
- [68] Merriam-Webster. *Definition of "documentation"*. 2019.
- [69] J. M. Morgan and J. K. Liker. *The Toyota Product Development System*, volume 13533. New York: Productivity Press, 2006.
- [70] J. Morton, T. A. Wheeler, and M. J. Kochenderfer. Closed-Loop Policies for Operational Tests of Safety-Critical Systems. *IEEE Transactions on Intelligent Vehicles*, 3(3):317–328, Sep. 2018.
- [71] D. K. Nilsson and U. E. Larson. Conducting Forensic Investigations of Cyber Attacks on Automobile In-vehicle Networks. In *Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia and Workshop, e-Forensics '08*, pages 8:1–8:6, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
- [72] C. of the European Union. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on type-approval Requirements for Motor Vehicles and their Trailers, and Systems, Components and Separate Technical Units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/... and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009, March 2019.
- [73] A. Orebaugh, G. Ramirez, and J. Beale. *Wireshark & Ethereal network protocol analyzer toolkit*. Elsevier, 2006.

- [74] G. Palmer and M. Corporation. A Road Map for Digital Forensic Research. Technical report, Digital Forensic Research Conference, 11 2001.
- [75] J. Park, H. Chung, and S. Lee. Forensic Analysis Techniques for Fragmented Flash Memory Pages in smartphones. *Digital Investigation*, 9(2):109 – 118, 2012.
- [76] G. Peterson. Consumer Interest In Self-Driving Cars Increasing. online, June 2016.
- [77] B. Preneel. Cryptographic Hash Functions. *European Transactions on Telecommunications*, 5(4):431–448, 1994.
- [78] S. Raghavan. Digital Forensic Research: Current State of the Art. *CSI Transactions on ICT*, 1(1):91–114, Mar 2013.
- [79] D. Regalado, G. Iglesias, and K. Hsu. Meet salinas, the first ever sms-commanded car infotainment rat. Presentation, 2018.
- [80] M. Rogers and K. Seigfried. The Future of Computer Forensics: A Needs Analysis Survey. *Computers & Security*, 23(1):12–16, 2004.
- [81] R. Rowlingson. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, 2(3):1–28, 2004.
- [82] R. Saferstein. *Criminalistics - An Introduction to Forensic Science*. Pearson, 10 edition, December 2016.
- [83] ST. *SPC58EEEx, SPC58NEEx - 32-bit Power Architecture® microcontroller for automotive ASIL-D applications*. ST, 3 edition, October 2017.
- [84] T. Steinbach, K. Müller, F. Korf, and R. Röllig. Demo: Real-time Ethernet in-car Backbones: First Insights into an Automotive prototype. In *2014 IEEE Vehicular Networking Conference (VNC)*, pages 133–134, Dec 2014.
- [85] H. Suo, J. Wan, C. Zou, and J. Liu. Security in the Internet of Things: A Review. In *2012 International Conference on Computer Science and Electronics Engineering*, volume 3, pages 648–651, March 2012.
- [86] E. Walter and R. Walter. *Data Acquisition from Light-Duty Vehicles Using OBD and CAN*. SAE International, nov 2018.

- [87] D. Watson and A. Jones. Chapter 8 - Incident Response. In D. Watson and A. Jones, editors, *Digital Forensics Processing and Procedures*, pages 313 – 365. Syngress, Boston, 2013.
- [88] N. Zaman. *Automotive Electronics Design Fundamentals*. Springer, Switzerland, 2015.
- [89] S. Kiltz, M. Hildebrandt, and J. Dittmann. forensische datenarten und -analysen in automotiven systemen. In *DACH Security*, pages 141–152. syssec, 05 2009.