Practical Data Acquisition and Analysis Method for Automobile Event Data Recorders Forensics

Yousik Lee[1] and Samuel Woo[2*]

[1]ESCRYPT GmbH, Gyeonggi-do 13494, South Korea
yousik.lee@escrypt.com

[2]Dankook University, Gyeonggi-do 16890, South Korea
samuelwoo@dankook.ac.kr

Received: May 30, 2022; Accepted: July 29, 2022; Published: August 31, 2022

Abstract

As modern vehicles converge with information and communication technology (ICT), an increasing number of software packages are being installed in vehicles. The software can generate an audit log whenever an event occurs, and by using this, the condition of the vehicle can be understood easily. However, vehicle forensics is not well established in the automotive industry. In particular, it is difficult to properly understand the situation at the time of a crime using a vehicle or a traffic accident. Vehicles are obliged to be equipped with events and data recorders (EDRs) to infer certain situations, but there can be difficulties in interpreting data when the vehicle does not use a standardized protocol, or to the method of acquisition of data in non-canonical situations has not yet been systematically processed. In this study, we have proposed a systematic data acquisition and analysis method for the EDR. We demonstrated the efficiency of our proposed method through experiments on mass-production vehicles.

Keywords: Vehicle forensics, Automotive forensics, Event Data Recorder (EDR), Data Storage System for Automated Driving (DSSAD)

1 Introduction

Over the past decade, modern vehicles have shifted from machinery to complex information technology (IT) systems. An increasing number of machines in the vehicles are being replaced by software, and this phenomenon is becoming more rapid with respect to the development in autonomous vehicles and connected cars. For this reason, when vehicles stop either due to the presence of sand in the engine or due to a previously broken connecting pipe, it is now more likely that the vehicle stalls due to a software error. In the former case, a professional mechanic thoroughly investigates the vehicle to determine the cause and thereby solve the problem; in the latter case, the problem can be easily solved using a diagnostic tool or device. In addition, this diagnostic tool also helps to infer the accident situation when one occurs.

While investigating a vehicle, it is very important to reenact the situation at the time of the investigation. To do this, it is necessary to collect and analyze the data communicated and stored in the vehicle. These types of processes: collection and analysis are called vehicle forensics. Vehicle forensics is becoming increasingly important in criminal and traffic accident investigations. Vehicle forensics uses

Journal of Internet Services and Information Security (JISIS), volume: 12, number: 3 (August), pp. 76-86
DOI:*10.22667/JISIS.2022.08.31.076*

*Corresponding author: Division of Software Science, Dankook University, Gyeonggi-do 16890, South Korea, Tel: +82-31-8005-3234

digital evidence sources such as event data recorders (EDRs), telematics and infotainment systems such as audio video navigation (AVN) systems, electric control units (ECU), and other devices that store data in the vehicle [1]. In this study, we have introduced methodologies and processes for investigating the EDR, which is currently the main target of vehicle forensics. Our main goal is to collect and analyze data to recreate accident situations in terms of crime and accident investigations. Thus, EDR analysis is the best way to achieve the goal for today's mass production vehicles.

In this study, we analyzed the EDR for mass-produced vehicles, and we have described the processes and methods involved, and the results in detail. The analysis method, which we have proposed is a general-purpose method that can be applied to other vehicles, and through further research, they can contribute to the development of a vehicle forensic framework in connection with a data storage system for automated driving (DSSAD), an intrusion detection system (IDS), a vehicle-to-everything (V2X) on-board unit (OBU), and autonomous driving devices. This paper is organized as follows: Section 2 explains the related studies, and an overview of vehicle forensics is reviewed in Section 3. Thereafter, we have described the data acquisition and analysis methods and processes in detail in Section 4 from the EDR perspective. Section 5 concludes the paper with a proposal for the future research.

2 Related work

With the increasing demand for vehicle forensics, several researchers have suggested various methods of data collection and analyses. Mansor et al. proposed DiaLOG, which is a mobile application that stores and protects data for vehicle forensics [2]. There are disadvantages to the current EDR and insurance blackbox from the perspective of transparency and privacy. Therefore, they proposed the necessity of secure remote storage that provides user access and privacy. For a mobile phone to communicate with a vehicle, authentication must be performed, and a hardware security module (HSM) that is compatible with the E-safety vehicle intrusion protected application (EVITA) specification should be installed on a telecommunication device such as a communication control unit (CCU) [3]. They demonstrated their proposals by implementing the CCU and mobile applications.

Bortles et al. introduced a method for collecting and analyzing the data from vehicle telematics and infotainment systems [4]. To acquire data from the vehicle, they used Berla iVE, which is a vehicle forensics tool, that acquires data from the vehicles and allows investigators to analyze it. They tested whether vehicle data could be imported correctly by the following examinations: Door open/close events, gear shift events, parking light on/off events, telephone calls, short message services, and vehicle tracklogs. Although they demonstrated the method to acquire and analyze data from the telematics system effectively, they did not explain how to acquire and analyze the data while using the phone project systems and in unusual situations, such as when the device was damaged owing to an accident.

Hossain et al. proposed Trust-IoV, a trustworthy forensic investigation framework for the internet of vehicles (IoV) [5]. They considered vehicles as smart objects that have communication features such as the Internet and wireless networks to collaborate with other objects such as other vehicles, pedestrians, and backend infrastructure. The proposed architecture consists of two main components: forensic gateway (FG) and IoV-forensic service (IoV-FS). They established the architecture by focusing on the data flow and processing method of each component rather than the generation and storage of forensic data in the end components, such as vehicles.

Buquerin et al. proposed a systematic vehicle forensics procedure [6]. They classified the related stakeholders and scenarios, forensic types and acquisition methods, and data types. Furthermore, they defined the processes involved in vehicle forensics in the following four steps: forensic readiness, data acquisition, data analysis, and documentation. They presented a general and applicable vehicle forensic

process and demonstrated that forensic analysis is possible in real vehicles using simple commercial tools, such as Wireshark and ODB interfaces. However, sufficient completeness for the proposed forensic process was not provided as we did not consider abnormal situations, such as situations where the OBD interface could not be used.

As digital forensic technology develops in the coventional IT field, vehicle forensics is also undergoing a revolutionary transformation. The advent of autonomous vehicles and popularization of connectivity services and phone projection systems will change the direction of vehicle forensics. Despite several studies on vehicle forensics, practical methods and processes for collecting and analyzing data from EDR in various situations have not been proposed yet. We intend to present these methods and processes in this study.

3 Vehicle forensics overview

The traditional automotive electrical/electronic (E/E) architecture has a domain-based topology. [7] Domains such as the powertrain, chassis, body, and infotainment are classified according to their functionalities and physical connectivities. Components with similar functions can be grouped into the same domain, and sensors and actuators can be shared by the components in the same domain. Figure 1 depicts a modern automotive E/E architecture using a domain-based topology.

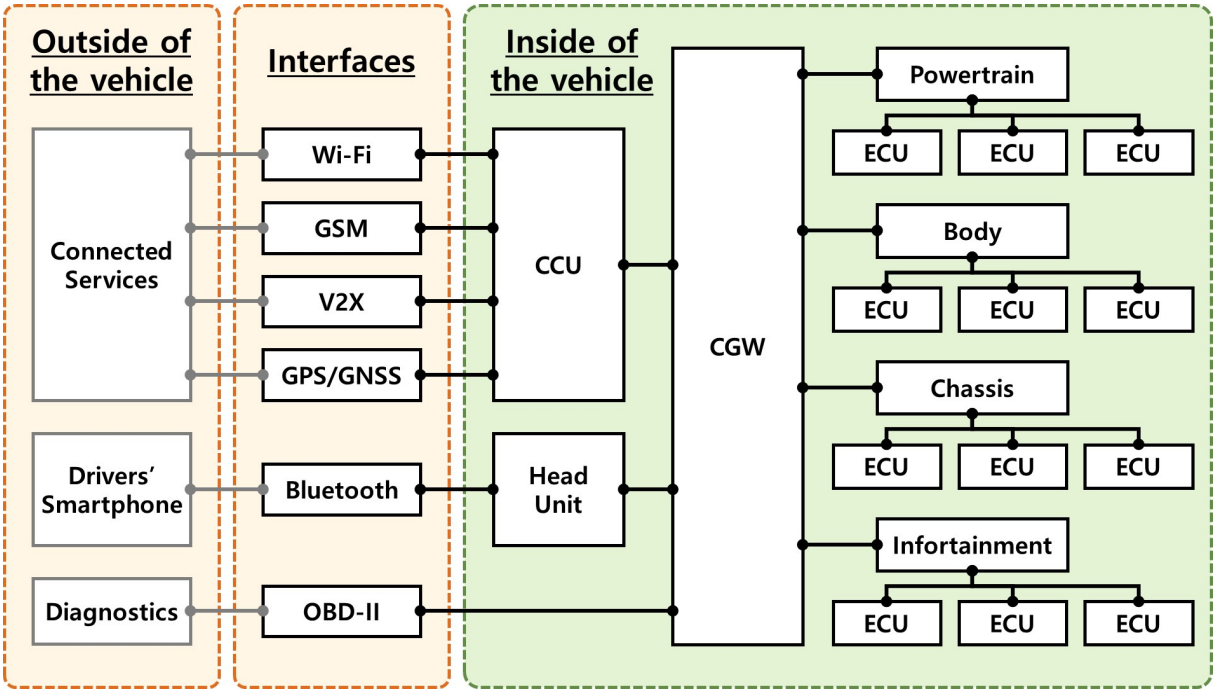

Figure 1: Modern automotive E/E architecture

In general, the powertrain, chassis, and body domain control the vehicle physically and communicate data between respective electronic control units (ECUs) through the in-vehicle network, which uses specific network protocols such as the controller area network (CAN), CAN flexible data-rate (FD), local interconnected network (LIN), media-oriented systems transport (MOST), FlexRay, and Ethernet. The infotainment system connects both the internal and external networks of the vehicle. Drivers can connect to the vehicle through interfaces such as a universal serial bus (USB) / secure digital (SD) card or Bluetooth and use connected services via Wi-Fi, global system for mobile communications (GSM),

and vehicle-to-everything (V2X) communication. The data transmitted from outside the vehicle are transferred to the in-vehicle network, as per the requirements. In this study, we focused on the method for analyzing events such as vehicle accidents from the point of view of forensic investigations.

3.1 EDR/DSSAD

An event data recorder (EDR) refers to a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to an event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta-V vs. time), intended for retrieval after the crash event." [8] In general, an EDR is mounted on an airbag control unit (ACU) and is connected to various electronic control systems through an in-vehicle network. To acquire and analyze data stored in the EDR, it is necessary to access and decode the raw data present in the EDR. The EDR monitors several key systems, such as brakes, airbags, and seatbelts, and captures data when an event occurs. There are trigger conditions for the EDR to store data obtained as a result of a physical collision or accident. The following two conditions are the examples of trigger conditions:

- When an airbag is deployed: the data are stored in the memory of the EDR and locked to prevent it from being erased or overwritten by other data.
- When the seatbelt pretensioner is activated without deploying the airbag: the data are stored in the memory of the EDR, but is not locked so that it can be erased or overwritten by other data.

Each country obliges vehicles to store specific data; however, the amount of data that must be stored are different in various countries. Table 1 lists the data stored by the National Highway Traffic Safety Administration (NHTSA). [9]

Table 1: Data elements required for all vehicles equipped with an EDR

Data Element	Recording Interval/Time	Data Sample Rate (Second)
Delta-V, longitudinal	0 –250 ms	100
Maximum delta-V, longitudinal	0–300 ms	n.a.
Time, maximum delta-V	0–300 ms	n.a.
Speed, vehicle indicated	-5.0 –0 s	2
Engine throttle, % full (or accelerator pedal, % full)	-5.0 –0 s	2
Service brake, on/off	-5.0 –0 s	2
Ignition cycle, crash	-1.0 s	n.a.
Ignition cycle, download	At the time of download	n.a.
Safety belt status, driver	-1.0 s	n.a.
Frontal airbag warning lamp, on/off	-1.0 s	n.a.
Air bag deployment	Event	n.a.
Multi-event, number of events	Event	n.a.
Time from event 1 –2	As per the requirement.	n.a.
Complete file recorded (yes, no)	Following other data	n.a.

Unlike the EDR, a data storage system for automated driving (DSSAD) stores the data that indicates who controls the vehicle at any given time, either the driver or the autonomous driving system. Autonomous vehicles are becoming common, and consequently, cyberattacks will increase rapidly. Therefore, it is important not only to understand the fragmentary accident situation, but also to identify the

driver of the vehicle at the time of the accident and the reason for the accident. Therefore, along with EDR, the importance of data from intrusion detection systems (IDS), V2X, and DSSAD is expected to increase. A DSSAD is obligatory to be installed according to the UN regulation No.157. [10] Because UN regulation No.157 was adopted in June 2020 and came into effect in January 2021, there have been no production vehicles yet. Therefore, practical forensics for DSSAD were not covered in this study.

4 EDR Data acquisition and analysis

4.1 EDR Data acquisition

There are two main methods to collect data from the EDR:

•**Canonical method:** At first, if the EDR device works properly and the regular interface is not broken, the EDR data can be collected through a regular interface. A 'regular interface' means a standardized or widely used interface regarding vehicles. In this study, two regular interfaces were used for experiments:

- OBD-II on the vehicle by
- Direct connection to the ECU through the wire-haness connector

And two acquisition method according to the tool as follows:

- The dedicated EDR software
- The tester (as known as a diagnostic tool) using unified diagnostic service (UDS) protocol

FIgure 2 shows all acquisition methods described above. OBD-II is the generally preferred regular interface for access from outside the vehicle to the inside. If OBD-II works properly, we can access to the target ACU via OBD-II without direct connection to ACU itself.

Otherwise, we can acquire data through a direct connection to the target ACU after getting the ACU out of the vehicle and supply power to it separately. After the connection between the dedicated software and the ACU whether through OBD-II or direct connection, EDR data can be easily obtained with dedicated EDR software such as Bosch CDR. Bosch has provided a dedicated tester called Bosch crash data retrieval (CDR) since 2000 [11]. Because Bosch is the largest automotive supplier and has provided enormous EDR devices for a long time, we utilized this tester. The EDR data can be easily retrieved via Bosch CDR if the target vehicle uses the Bosch EDR device. If there is no dedicated EDR software, EDR data can be acquisited by using an UDS and testers (as known as diagnostic devices). UDS is the most widely used communication protocols to for maintenance and diagonsis vehicles, which is specified in the ISO 14229-1 [12]. Table 2 shows data input/output related services among various services of UDS.

Table 2: data input/output related services of UDS

Services	Request service ID(HEX)	Response service ID(HEX)
ReadDataByIdentifier	0x22	0x62
ReadMemoryByAddress	0x23	0x63
ReadDataByPeriodicIdenticfier	0x2A	0x6A
DynamicallyDefineDataIdentifier	0x2C	0x6C
WriteDataByIdentifier	0x2E	0x6E
WriteMemoryByAddress	0x3D	0x7D

To acquisite data using UDS, “ReadMemoryByAddress” service is usefule. If the memory address that stores EDR data is 0x2048 1392 and data size is 259 bytes (0x103), the request and response process are as Table 3 and Table 4.

Table 3: Request

Message direction	client → server	
Message type	request	
Data byte	Description	Value
♯ 1	service ID of ‘ReadMemoryByAddress’ request	0x23
♯ 2	addressAndLengthFormatIdentifier	0x24
♯ 3	memoryAddress [byte♯1] (MSB)	0x20
♯ 4	memoryAddress [byte♯2]	0x48
♯ 5	memoryAddress [byte♯3]	0x13
♯ 6	memoryAddress [byte♯4]	0x92
♯ 7	memorySize [byte♯1] (MSB)	0x01
♯ 8	memorySize [byte♯2]	0x03

While dedicated EDR software automatically generates a report, in the case of using UDS, it is required user to create a report by analyzing the acquired data. To do that, user must know the specification of EDR data. i.e., the user should know the meaning of the specific memory value based on the respective

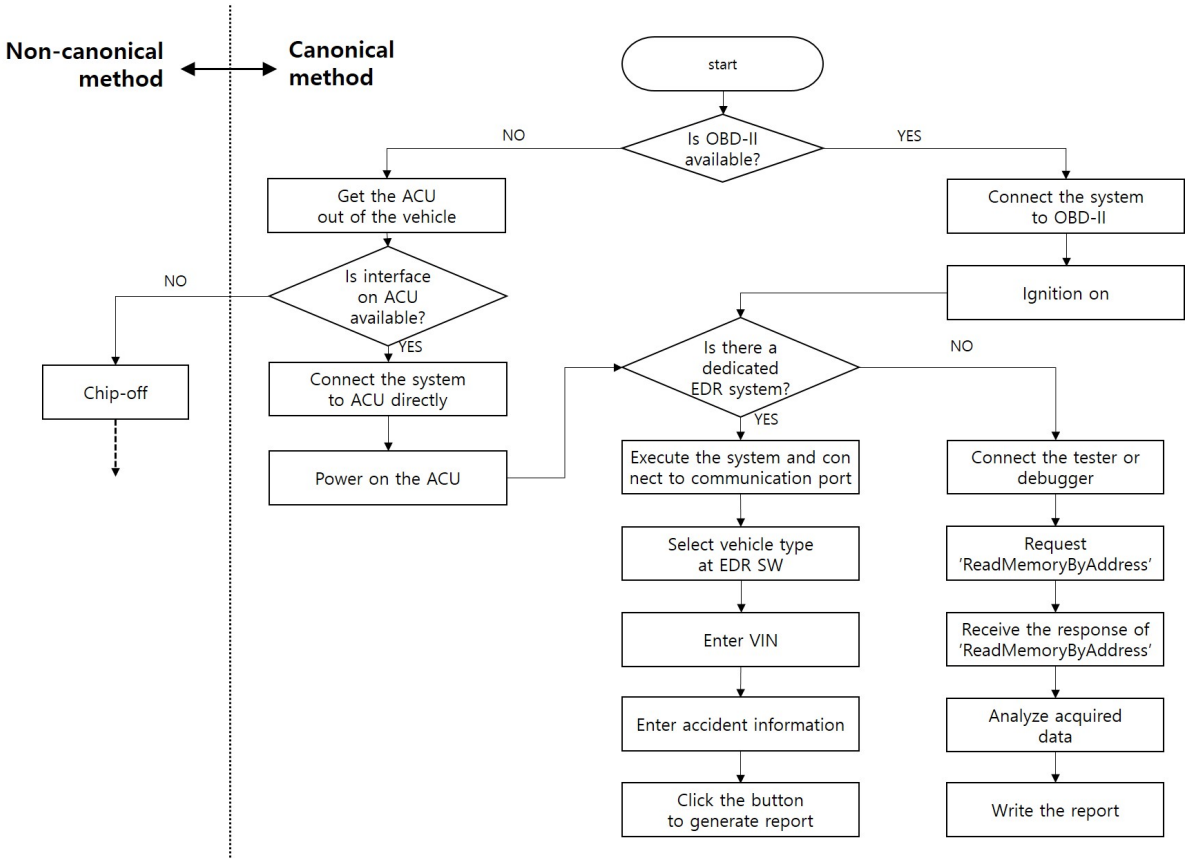

Figure 2: Vehicle forensic procedure in the perspective of acquisition method

Table 4: Response

Message direction	client ← server	
Message type	response	
Data byte	Description	Value
♯ 1	service ID of 'ReadMemoryByAddress' response	0x63
♯ 2	dataRecord [data ♯1]	0x00
...	...	...
♯ 259 + 1	dataRecord [data ♯259]	0x8C

vehicle manufacturer. Since the CAN specification is the intellectural property of vehicle manufacturers, it is not easy to analyze the EDR data without dedicated EDR software. In this study, we obtained the EDR data from a BMW Mini via Bosch CDR. Fiqure 3 shows a Bosch CDR based EDR data acquisition process and results. It is easy to use Bosch CDR and obtain data; however, unfortunately, we could not obtain any meaningful data because the target vehicle did not have any accident history.

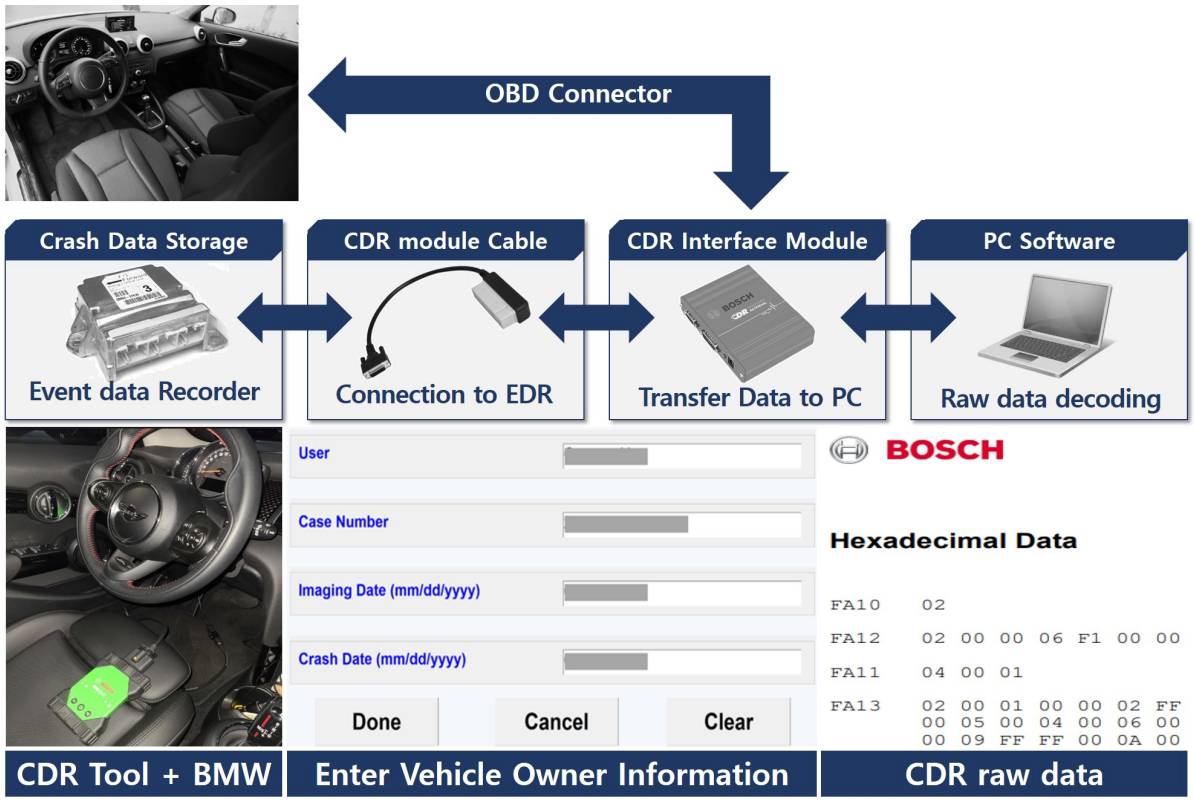

Figure 3: BOSCH CDR data acquisition and analysis process

•**Non-canonical method:** A canonical method can be used when regular interfaces operate properly. That is, if the OBD-II port works normally or if the debug interface of the ECU, such as a joint test action group (JTAG), works even if the OBD-II port is broken, data can be acquired in a canonical manner. In other words, a canonical method cannot be used when regular interfaces do not operate, as depicted in Figure 4.

In this case, a non-canonical method such as a chip-off is used. In this study, a chip-off-based raw EDR data acquisition experiment was conducted using the ACU from 2012 Korando [13]. We could not

secure a dedicated diagnostic device for the vehicle, and chip-off was the only way to perform forensics. The experimental process is as follows:

- STEP1: Acquisition of the ACU module in which the EDR data are stored in the accident vehicle. The service manual is helpful for determining the position of the installed ACU.
- STEP2: Identification of the memory in which the EDR data are stored in the ACU. In general, EDR data are stored in an electrically erasable programmable read-only memory (EEPROM).

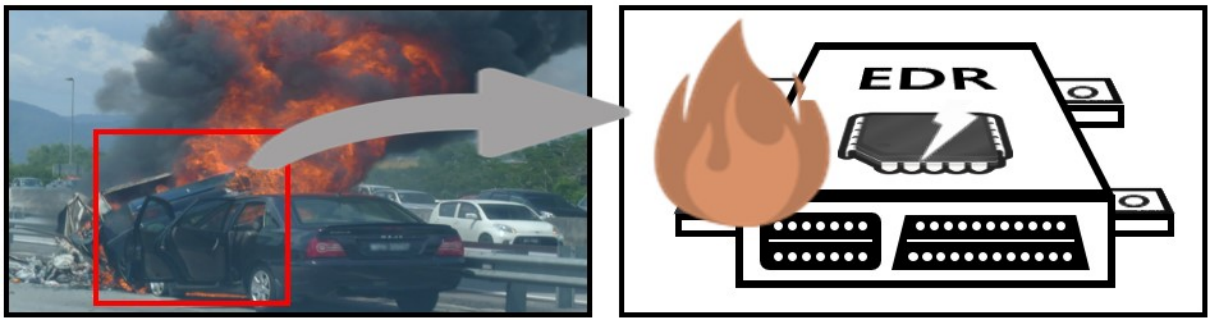

Figure 4: Example of damaged EDR device due to traffic accident[14]

- STEP3: To easily check the pin map of the EEPROM, we should know the model number. After identifying the EEPROM, the protective film on the top of the EEPROM is removed and the model number is checked, as depicted in Figure 5.

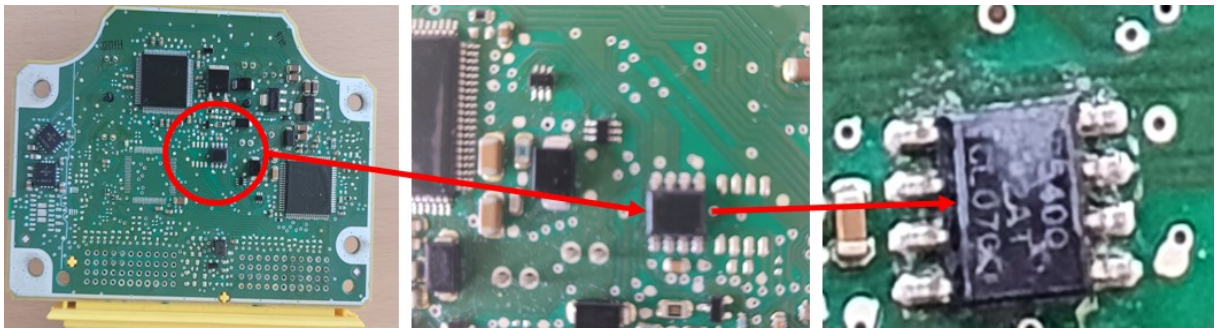

Figure 5: Example of checking model number

- STEP4: A serial communication cable was used to connect the identified EEPROM and the data acquisition software. The EEPROM used in this experiment has a total of eight pins, but according to the specification of the model, only three pins are used for data transmission. After checking the pin map, a serial communication cable was made, and the manufactured serial cable was connected directly to the data transmission pin of the EEPROM, as depicted in Figure 6.
- STEP5: Perform data acquisition. In this study, we used the dedicated commercial software, CARPROG. [15] The result of processing and acquisition of the data are depicted in Figure 7.

4.2 EDR data analysis

The EDR data are stored in the device as raw data according to the manufacturer's specifications, which is required to understand the data. If we know the manufacturer's specifications or have the tester in which

Figure 6: Manufacturing process of a serial communication cable and connecting it to the EEPROM

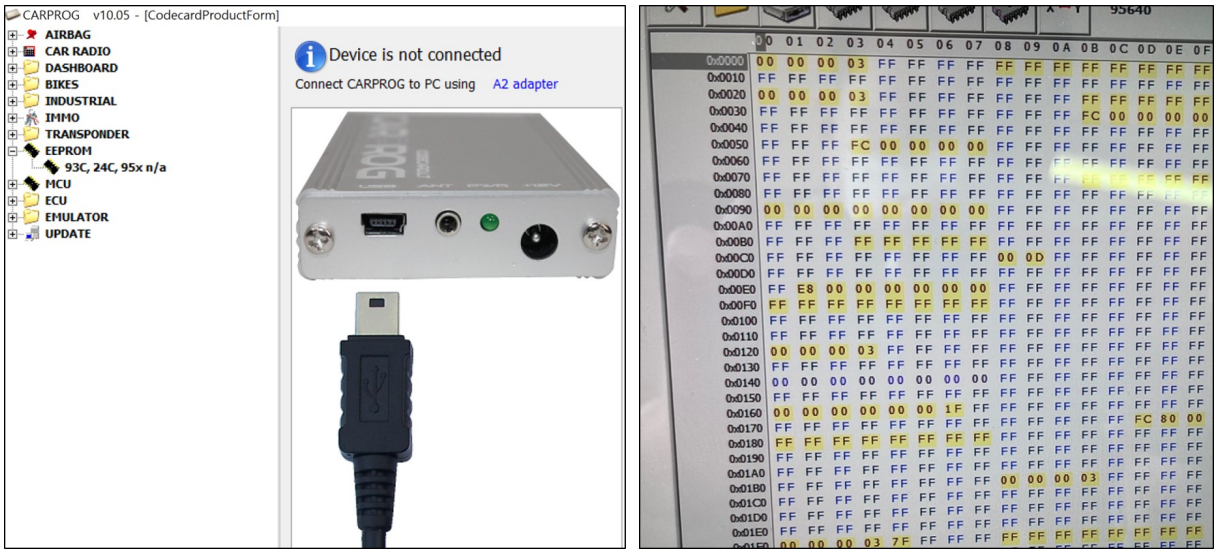

Figure 7: The result of the data acquisition

they are embedded, the EDR data can be converted and displayed in a readable form using dedicated software, such as the Bosch CDR and the manufacturer's dedicated diagnostic device. However, if we do not know the specifications and do not have a dedicated diagnostic device, as identical with the case of using UDS, we cannot understand the data officially. In general, non-canonical methods are applicable in this case. The manufacturer's specifications are its own intellectual property and are not disclosed to the public. Thus, reverse engineering is required for the specification to understand. Reversing is beyond the scope of this study and therefore, we did not explore it.

5 Conclusion

In this study, we have demonstrated the method to collect and analyze the data to understand the vehicle behavior. EDR, which is an essential device to reenact an accident, can be analyzed through commercial tools such as Bosch CDR; however, 11% of the model year 2016 and newer vehicles are supported by other EDR tools, which means that there are no standardized retrieval tools and methods [16]. In this case, the proposed analysis method can be an alternative solution.Unfortunately, we could not analyze

DSSAD in this study because there are no vehicles equipped with DSSAD so far. In addition, analyzing the EDR helps to recreate the accident situation, but it is insufficient to find the cause of the accident. For this reason, it is absolutely necessary to collect and analyze logs of other security-related devices such as IDS, V2X OBU, firewalls, and Ethernet switches. In the future, we will develop a vehicle forensic framework, which establishes methodologies and processes for data collection and analysis, and develops tools that analysts can easily understand by organizing the results.

Acknowledgments

This work was supported by Institute of Information & communications Technology Planning & Evaluation(IITP) grant funded by Korea government(MSIT) (No.1711170476, Development of Collection and Integrated Analysis Methods of Automotive Inter/Intra System Artifacts through Construction of Event-based experimental system)

References

[1] E. A. Bates. Digital vehicle forensics, November 2019. `https://abforensics.com/digital-vehicle-forensics/` [Online; Accessed on August 1, 2022].

[2] H. Mansor, K. Markantonakis, R. N. Akram, K. Mayes, and I. Gurulian. Log your car: The non-invasive vehicle forensics. In *Proc. of the 2016 IEEE Trustcom/BigDataSE/ISPA(TrustCom'16), Tianjin, China*, pages 974–982. IEEE, August 2016.

[3] O. Henniger. Evita: E-safety vehicle intrusion protected applications. *EVITA*, November 2011.

[4] W. Bortles, S. McDonough, C. Smith, and M. Stogsdill. An introduction to the forensic acquisition of passenger vehicle infotainment and telematics systems data. In *Proc. of the SAE World Congress Experience (WCX'17), Detroit, USA*, page 28. SAE Technical Paper, March 2017.

[5] M. M. Hossain, R. Hasan, S. Zawoad, et al. Trust-iov: A trustworthy forensic investigation framework for the internet of vehicles (iov). In *Proc. of the 2017 IEEE International Congress on Internet of Things (ICIOT'17), Honolulu, Hawaii, USA*, pages 25–32. IEEE, July 2017.

[6] K. K. G. Buquerin, C. Corbett, and H. J. Hof. A generalized approach to automotive forensics. *Forensic Science International: Digital Investigation*, 36(1):301111, March 2021.

[7] M. Dibaei, X. Zheng, K. Jiang, S. Maric, R. Abbas, S. Liu, Y. Zhang, Y. Deng, S. Wen, J. Zhang, et al. An overview of attacks and defences on intelligent connected vehicles. arXiv:1907.07455, July 2019. `https://doi.org/10.48550/arXiv.1907.07455` [Online; Accessed on August 1, 2022].

[8] Europe Union. Un regulation no 160 – uniform provisions concerning the approval of motor vehicles with regard to the event data recorder. *Publications Office of the European Union*, July 2021.

[9] United States of America. 49 cfr part 563 - event data recorders, October 2011. `https://www.nhtsa.gov/` [Online; Accessed on August 1, 2022].

[10] Europe Union. Un regulation no 157 – uniform provisions concerning the approval of vehicles with regard to automated lane keeping systems. *Publications Office of the European Union*, January 2021.

[11] BOSCH. Bosch diagnostics. *BOSCH*, 2022.

[12] ISO ISO. Road vehicles — unified diagnostic services (uds) — part 1: Application layer, February 2020. `https://www.iso.org/obp/ui/fr/#iso:std:iso:14229:-1:en` [Online; Accessed on August 1, 2022].

[13] SsangYong Motors. Korando heritage. *SsangYong Motors*.

[14] J. P. Zeitler, J. Palmer, and C. Smith. Validation of eeprom chip removal and reinstallation for retrieval of electronic crash data-destructive and non-destructive methods. Technical report, SAE Technical Paper, 2021.

[15] M. Marchetti and D. Stabili. Read: Reverse engineering of automotive data frames. *IEEE Transactions on Information Forensics and Security*, (4):1083–1097, September 2018.

[16] C. Grasso, S. Vartak, and E. D. Jackson. Enhancing connecticut's crash data collection for serious injury and fatal motor vehicle collisions. Technical report, rosap, 2018.

Author Biography

Yousik Lee received his Ph.D. degree in information security from Korea University, Seoul, South Korea, in 2020. He has been in the cyber security industry for over 22 years, especially ten more years in automotive security. He specializes in consulting, development, and standardization for application security, PKI, cryptography, and automotive security. As a Korean ITU-T SG17 member, he has contributed to developing automotive cybersecurity standards. He is currently responsible for the cybersecurity business of ETAS Korea as a director and Chief Information Security Officer. His research interests include in-vehicle network security, V2X, security risk analysis, cybersecurity management system (CSMS), and evaluation methodologies for automotive security.

Samuel Woo received his Ph.D. degree in information security from Korea University, Seoul, South Korea, in 2016. He was a senior researcher with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea. He is currently an Assistant Professor with the Department of Software Science, Dankook University, Jukjeon, South Korea. His research interests include cryptographic protocols in authentication, security and privacy in vehicular networks, and controller area network security.