Ivan Cvitić
University of Zagreb, Faculty of Transport and Traffic Sciences
ivan.cvitic@fpz.hr

Dragan Peraković
University of Zagreb, Faculty of Transport and Traffic Sciences
dragan.perakovic@fpz.hr

Marko Periša
University of Zagreb, Faculty of Transport and Traffic Sciences
marko.perisa@fpz.hr

Siniša Husnjak
University of Zagreb, Faculty of Transport and Traffic Sciences
sinisa.husnjak@fpz.hr

s. 133-144

APPLICATION POSSIBILITIES OF DIGITAL FORENSIC PROCEDURES IN VEHICLE TELEMATICS SYSTEMS

Technological development has resulted in the possibility of implementing a large number of telematics systems and subsystems within the vehicle. Their purpose is to collect data through a number of sensors on the state of the vehicle as well as its environment. The result of the collected data processing is information that can be used to increase the passengers' safety inside the vehicle, but also to other participants of traffic network, and to optimize the desired resources such as fuel consumption, travel time etc. The use of vehicle telematics systems and collected data can be of great importance when an unwanted event occurs in which the vehicle is involved. The aim of this research is to identify vehicle systems that store data, data types and the possibility of their extraction using a digital forensic framework, for the purpose of timely reaction to the negative event occurrence.

KEYWORDS

data extraction, incident response, infotainment system, ECU

INTRODUCTION

The development of information and communication systems enabled their implementation within the vehicles. The result is the telematics systems whose purpose is to collect data from the vehicle and its surroundings with the aim of optimizing individual traffic processes, operating the vehicle and increasing the level of safety as well as the ecological and economic aspects of the transport system. A number of such systems implemented within the vehicle collects a large amount of data that are correlated and merged for the purpose of generating new information. Based on the obtained information necessary activities are carried out in order to achieve the final objective function.

The increase in the number of vehicles resulted in an increase in the number of accidents as well as numerous other forms of incidents in which the vehicle was used. Consequently grows the need for identifying the cause and other details of such incidents in which data from telematics systems within vehicles can serve as evidence in such proceedings.

The emergence of digital forensics as a relatively new field of forensic science has enabled the provision of support in detecting the causes of incidents in the environments of using information and communication technologies. The collection of digital evidence using the method of digital forensics involves the application of pre-established methodologies and scientific methods for the purpose of adequate extraction and data analysis.

The hypothesis of the research is that the procedures for digital forensics can be applied in the function of investigating the incidents in which the vehicle was involved. The aim of the research is to analyze the telematics systems implemented in the vehicle from the aspect of their mutual communication and the data they collect, process and store. Based on the analysis, the possibility of applying digital forensic procedures will be established as a new approach for the purpose of more effective detection of incident related details.

1. PREVIOUS RESEARCH

The possibilities of using digital forensics telematics systems are insufficiently explored, which is evident from a small number of existing research. Paper [1] shows a study of mobile devices digital evidence being used by drivers in traffic accidents. The authors used the procedures of digital forensics on mobile devices in order to prove their use while driving. As mentioned challenge is to establish a timeline of events and causal factors of the accident. The need for forensic analysis of other systems within the vehicle is also stated in order to precisely determine the activities that preceded the traffic accident. Paper [2] presents the research of the challenges associated with forensic analysis of telematics systems within the vehicle. In addition, a case study of the forensic analysis of the infotainment system in the Volkswagen Golf was shown. The first working framework for carrying out forensic analysis in the Internet of Vehicle (IoV) environment is shown in [3] in which a model of evidence collection within the distributed IoV infrastructure is proposed. One of the applications of telematics data is also visible in the optimization of auto insurance, where research [4] shows the architecture for the collection, processing and exploitation of telematics data.

The lack of existing research is reflected in the lack of defined methodology and description of the activities required for the implementation of the telematics systems digital forensics. In addition, no research (according to the authors' knowledge) does

not investigate the importance of the correlation of the collected data from the vehicle system for the purpose of investigating the incident. Mentioned deficiencies seeks to complement the research presented in this paper.

1.1. RESEARCH METHODOLOGY

The research presented in this paper is based on data of information and communication elements within the vehicle gathered from existing and current scientific and technical literature. Due to the lack of the possibility of using digital forensic procedures in the field of telematics systems research, data and knowledge of existing research in the field of digital forensics applied in other domains have been synthesized. For the purpose of formalizing the possibility of collected data correlation for the purpose of discovering new knowledge, sets theory was used.

2. CLASSIFICATION OF VEHICLE INFORMATION AND COMMUNICATION SYSTEMS

The effectiveness of applying the digital forensic procedures requires knowledge and classification of telematics systems implemented inside the vehicle. Equally, it is necessary to know and classify used communication technologies as well as data which is collected, processed and stored, but also exchanged between the systems inside the vehicle. Classification of telematics systems, communication technologies and collected data will enable more efficient identification, extraction and analysis of digital evidence about vehicle, driver or passenger activity inside the vehicle.

2.1. TYPES OF IN-VEHICLE CONTROL SYSTEMS

Vehicle manufacturers over the years of development implement an increasing number of sensors, actuators and electronic control units (ECU) inside the vehicle in order to collect more data about the vehicle and its surroundings.

Table 1. Examples of in-vehicle systems

System classes	System name
Braking management	Autonomous Braking System
	Anti-lock Braking Systems
	Electronic Stability Control
	Traction Control
	Stop-Start Technology
	Vulnerable Road User / Pedestrian Detection
	Collision Avoidance
Speed management	Adaptive Cruise Control
	Speed Warning Technology
	Intelligent Speed Adaption
Passengers' safety	Seat Belts Reminders
	Airbags
	Active head restraints
	Pre-crash Systems
Driver fitness	Alcolocks
	Driver Fatigue Monitoring Systems
Other	eCall
	Navigation
	Tyre Pressure monitoring systems
	Journey Data Recorders
	Event Data Recorders

The purpose of the implementation of such devices is to provide a greater number of services for the user with different objectives such as increasing safety and comfort and reducing travel time. Some of the available systems are shown in Table 1.

The most commonly used devices inside the vehicle are ECU devices which control the functions of the vehicle, i.e. which collect data from the sensors and, based on their processing, control the actuators inside the vehicle. Core modules based on ECU devices are [5]:

- Engine Control Unit,
- Junction Box,
- Multimedia Head Unit,
- Stability Control Unit,
- Tire Pressure Control Unit,
- Telematics Control Unit, and
- Body Control Unit.

Approximately 70 ECU devices have been implemented within modern vehicles. ECU devices are responsible for managing different elements of vehicle operations such as engine control, signalling system, braking system, telematics and other systems depending on the vehicle model [6].

Types of used communication technologies

The purpose of the ECU devices is to collect and process sensor data and control actuators based on the received information. In addition, it is necessary to exchange the sensor data between different ECU devices due to their mutual dislocation and the need for delivery of different services [7].

These ECU devices, for data exchange, use four most common types of communication networks [5], [7]:

- CAN (Controller Area Network) represents the core communication network dedicated for connecting all ECU devices for the purpose of mutual exchange of data and provides an on-board diagnostics interface.
- LIN (Local Interconnect Network) represents communication subnetwork used for services that do not require high speed data transfer.
- FlexRey represents communication subnetwork applicable for key messages such as information about the vehicle stability.
- MOST (Media Oriented System Transport) represents communication subnetwork used for multimedia services such as real-time music and video streaming which require high speed data transfer.

As it can be seen from Figure 1, the CAN communication network is the backbone of data exchange between the ECU devices. Telematics functionalities of the vehicle as well as OBD (On Board Diagnostics) are provided through a dedicated ECU device which is connected to other ECU devices through the CAN network.

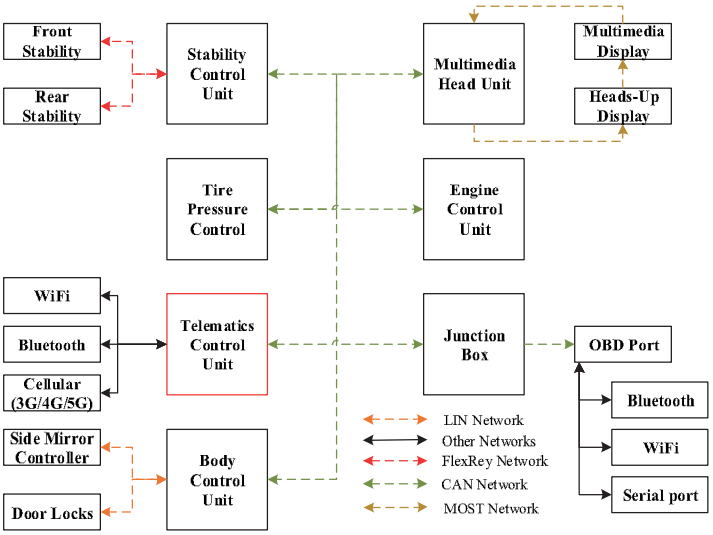

Fig. 1. Example of ECU devices interconncetions [5]

This implies the fact that telematics and OBD modules have access to all the data which other ECU devices inside the vehicle receive, process or pass. Implementation of vehicle telematics systems has enabled the data exchange between critical systems inside the vehicle.

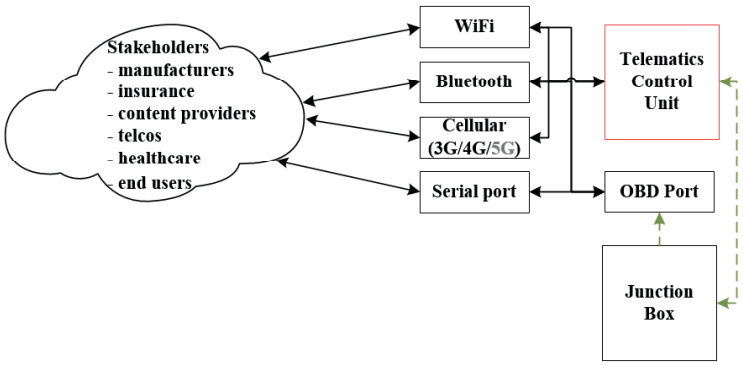

Fig.2. Stakeholders in vehicle telematics system [own study]

Data is exchanged via CAN communication network which also connects the vehicle telematics system and the OBD module. The purpose of such connectivity is to transfer data (generated inside the vehicle) with remote stakeholders, shown in Figure 2. By using the telematics system, stakeholders collect vehicle data for the purpose of remote diagnostics, insurance price calculation, reactions in the event of an accident or the provision of innovative information and communication service s [8]. This also implies the possibility of access to a large amount of data by using vehicle telematics and OBD interfaces for the purpose of digital forensic analysis, with the aim of collecting digital evidence related to the event of interest.

3. APPLICATION OF DIGITAL FORENSICS FOR VEHICLE INCIDENT INVESTIGATION

The current approach to investigation and reconstruction of the vehicle-related incident is based on a forensic analysis of physical evidence that is often unable to

identify certain events with the required level of accuracy. As common challenges of reconstruction of traffic accidents according to [9] are:
- inability to determine mechanical failure as the cause of the accident,
- speed of the vehicle at the time of the accident,
- driver identification, and
- vehicle contact point.

One of the growing risks of traffic accidents is the use of a mobile device while driving [10]. By forensic analysis of physical evidence of a traffic accident, it is difficult to determine the causal relationship between the use of a mobile device during driving and traffic accident.
Current challenges in reconstructing traffic accidents, as well as other vehicle-related incidents, require support for new evidence-gathering approaches. Digital forensics represents a new and rapidly growing field of forensic science in industrial and research environments. The goal of digital forensics is to retrieve and investigate data in digital devices, often for the purpose of proving certain activities related to a particular incident [11]. As mentioned in the previous chapter, today's vehicles contain a number of interconnected ECUs that have the ability to collect, process, store and transmit data [12]. Such functionalities provide the possibility of collecting digital evidence that can be supportive in investigating numerous incidents involving the vehicle.

3.1. CLASSIFICATION OF VEHICLE RELATED INCIDENTS

There are numerous incidents requiring forensic analysis in order to identify negative events, causes of incidents or other details related to the incident. Incidents associated with a vehicle can be classified into three basic groups as shown in Table 2. Primary vehicle-related incidents are those incidents in which the vehicle was directly involved. As an example it is possible to identify traffic accidents between two vehicles, vehicles and infrastructure, and vehicles and humans. Such incidents require a forensic analysis carried out at a physical level (calculation of vehicle speed at the moment of the accident, time-distance analysis, vehicle position, damages, etc.) [9]. Secondary incidents are those in which the vehicle was used to carry out illegal activities such as murder, robbery, smuggling, etc. Given the implementation of information and communication systems within vehicles, the trend of cyber-attack risks is on the rise [13].

Table 2. Vehicle related incident classification [own study]

Class notation	Incident class	Class description	Class member examples	Class member example notation
I_p	Primary	Incidents in which the vehicle was directly involved	Vehicle-vehicle	I_{pv}
			Vehicle - human	I_{ph}
			Vehicle-infrastructure	I_{pi}
I_s	Secondary	The incident in which the vehicle was indirectly involved	Robbery	I_{sr}
			Homicide	I_{sm}
			Smuggling drugs/weapons	I_{ss}
I_t	Tertiary	Incident in which one or more vehicle systems were attack target	Denial of Service	I_{tDDoS}
			Malicious code	I_{tmc}
			Unauthorized collection, modification / deletion of data	I_{tci}

Therefore, it is also possible to define a tertiary class of vehicle-related incidents. These are incidents in which the vehicle's information and communication system or its element are the attack target. In all of these classes of incidents, systems within the vehicle contain data that may be relevant in subsequent procedures for determining events and activities. Digital forensics has the potential to collect digital evidence of vehicle activity in all three listed incident classes [14].

Table 3. Vehicle incidents cause classification [15]

Class notation	Cause class	Class member example	Class member example notation
C_d	Driver related	Speed	C_{ds}
		Use of mobile phone	C_{dm}
		Inexperience	C_{di}
C_v	Vehicle related	Brake system malfunction	C_{vb}
		Engine malfunction	C_{ve}
		Tire malfunction	C_{vt}
C_e	Environmental and infrastructure related	Fog	C_{ef}
		Rain	C_{er}
		Road damages	C_{ed}

The causes of incidents according to [15] can be divided into driver (C_d), vehicle (C_v) and environmental (C_e). Wherein each mentioned set can have multiple elements where each element can represent new subset. Examples of each class of incident causes are presented in the table 3.

Data related to specific ECU devices

Vehicle ECU devices are handling numerous of data from large number of sensors implemented into vehicle. Each ECU is responsible for collecting data from a certain number of sensors and managing actuators for which it is competent. Thus ECU examples are ECU unit responsible for vehicles engine (ECU_{engine}), ECU responsible for vehicle airbags (ECU_{airbag}) and the ECU responsible for managing the vehicle infotainment system ($ECU_{infotainement}$). As mentioned, the number of ECU devices depends on the manufacturer and model of the vehicle [16].

Table 4. ECU and mobile device dataset examples [16], [17]

Set	Notation	Subset of (⊆)	Set elements	Unit
Engine speed	RPM	ECU_{engine}	0,..,5000	rpm
Engine coolant temperature	TMP	ECU_{engine}	-40,...,130	°C
Vehicle speed	SPD	ECU_{airbag}	0,..,200	km/h
Brake light switch	BRK	ECU_{airbag}	0,1	True/false
Mobile device connection	MDC	$ECU_{infotainement}$	0,1	True/false
Voice communication over infotainment	VCE	$ECU_{infotainement}$	0,1	True/false
Voice communication	MDVC	MD_{log}	0,1	True/false
Network activity	NTW	MD_{log}	0,..,1000	Mbit/s
Message sent/received	MSG	MD_{log}	0,1	True/false

A digital forensic investigation of a particular incident may often require the collection of data from other devices that are not implemented within a vehicle such as the driver's mobile device. The purpose of data collection is more efficient correlation of data and more precise determination of events and activities within the vehicle. Examples of data that can be collected from an ECU and mobile device are shown in Table 4.

Digital forensics methodology for vehicle digital evidence collection

When an incident belongs to one of the classes shown in Table 2, it is possible to use the methodology for implementing digital forensics to determine the details or activities that are related to the observed incident.

Figure 3 shows the methodology for the implementation of digital forensics as a support of physical forensic investigation of vehicle-related incidents. The methodology defines the activities that are necessary for the efficient collection of digital evidence. Forensic investigation is the result of a particular incident detection. Depending on the class of the incident, it is possible to conduct a physical and digital forensic investigation (primary and secondary) or exclusively digital forensics (tertiary). The implementation of a digital forensic investigation requires a legal basis and a permit for enforcement (court order). For the purpose of investigation efficiency, the necessary step is to identify the systems / devices as a potential source of digital evidence [18]. Interconnection of the system within the vehicle requires the knowledge and identification of the used communication technology for the purpose of planning the necessary resources for retrieving data from the observed environment. Data collection from the ECU vehicle system for further analysis and correlation can be carried out via telematics and OBD interfaces. The reason is their connection to all ECU devices within the CAN vehicle network, as shown in Figure 1.

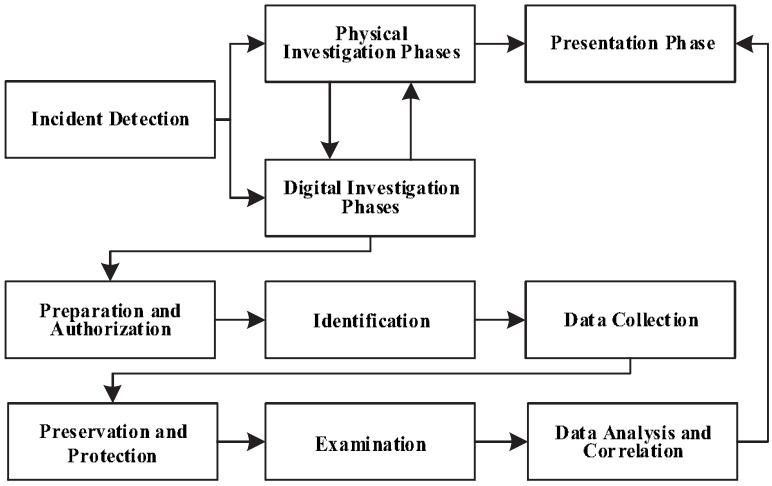

Fig.3. Digital forensics methodology for vehicle incident investigation support [19], [20]

After collecting data stored inside the vehicle's ECU, they must be transported in an appropriate manner to an environment suitable for further forensic processing. The key activity is to establish and maintain the chain of custody, or the documentation of metadata such as time, date, persons involved in the process of collecting and transport data [21]. The analysis and correlation of the collected data is the key and most complex phase in digital forensic analysis. Data collected from various ECUs combined and correlated can provide new information and evidence of vehicle-related events

and activities crucial to the incident being investigated. At this stage it is necessary to apply scientifically based methods on collected data, such as regression, classification method or set theory for the presentation of correlation data [22], [23]. These methods will allow relationship examination of two or more variables, or the effects of certain activities and events inside the vehicle on the occurrence of the incident which is being investigated.

Use case – digital evidence of using mobile device as potential cause of vehicle incident

Using a mobile device while driving is one of the drivers' distraction sources. During the investigation of the incident is necessary to collect and analyse data sets from the ECU units and correlate them to investigate whether, at the time of the incident the driver used a mobile device. In the aforementioned case, along with collecting data from the vehicle, it is necessary to collect the data from the driver's mobile device and correlate them with the data from the vehicle.

For the presentation and description of a specific problem it is possible to observe the incident I_{pv} (vehicle – vehicle) according to Table 2, where the incident I_{pv} is a subset of I_p, $I_{pv} \subseteq I_p$.

The causes of the incident I_{pv} can be varied, as can be seen in Table 4, and each of them represents a subset of the I_{pv}. Accordingly, the incident can be represented by Cartesian product of incidents causes sets:

$$I_{pv} = C_v \times C_d \times C_e = \{(c_v, c_d, c_e) \mid c_v \in C_v \wedge c_d \in C_d \wedge c_e \in C_e\} \quad (1)$$

The assumption of the incident cause requires an analysis of the collected data to confirm the assumption. For the observed case where the assumption of a cause or one of the causes of an incident is the use of a mobile device while driving, it is necessary to identify factors that can confirm or deny that hypothesis. For this purpose it is possible to use the data collected from the vehicle ECU's (ECU_{engine}, ECU_{airbag}, $ECU_{infotainment}$) and logs from the driver's mobile device (MD_{log}). Collected data needs to be correlated to determine user activity immediately before and at the time of incident.

The data of an individual ECU device and a mobile device log can be viewed as disjoint sets where the section of these sets is empty, $ECU_{engine} \cap ECU_{airbag} \cap ECU_{infotainment} \cap MD_{log} = \varnothing$. By displaying the Cartesian product of tuples, it is possible to correlate the data of disjoint groups in the time domain using the expression (2):

$$A_1 \times A_2 \times \ldots \times A_n = \prod_{i=1}^{m} \prod_{t=1}^{n} \left\{ (a_{11}, a_{22}, \ldots, a_{nt}) \middle| \begin{array}{l} a_i \in A_i \text{ for each } 1 \le i \le m \\ a_t \in A \text{ for each } 0 \le t \le n \end{array} \right\} \quad (2)$$

Observed sets are shown in Table 4, where for the purposes of determining the use of the mobile device during the incident can be used only certain sets like:

- RPM $=\{rpm_t \mid rpm_t \in RPM \text{ for each } 0 \le t \le n\}$
- SPD $=\{spd_t \mid spd_t \in SPD \text{ for each } 0 \le t \le n\}$
- MDC $= \{mdc_t \mid mdc_t \in MDC \text{ for each } 0 \le t \le n\}$
- VCE $=\{vce_t \mid vce_t \in VCE \text{ for each } 0 \le t \le n\}$
- MDVC $=\{mdvc_t \mid mdvc_t \in MDVC \text{ for each } 0 \le t \le n\}$
- NTW $=\{ntw_t \mid ntw_t \in NTW \text{ for each } 0 \le t \le n\}$
- MSG $=\{msg_t \mid msg_t \in MSG \text{ for each } 0 \le t \le n\}$

In this case, each set at time *t* contains a certain value of the element. Therefore, the Cartesian product of the presented sets is defined as:

$$\begin{aligned} &RPM \times SPD \times MDC \times VCE \times MDVC \times NTW \times MSG \\ &= \prod_{t=1}^{n} \left\{ (rpm_t, spd_t, mdc_t, vce_t, mdvc_t, ntw_t, msg_t) \middle| \begin{array}{l} rpm_t \in RPM \wedge spd_t \in SPD \wedge mdc_t \in MDC \wedge vce_t \in VCE \wedge \\ mdvc_t \in MDVC \wedge ntw_t \in NTW \wedge msg_t \in MSG \end{array} \right\} \end{aligned} \quad (3)$$

Inclusion

of exact values in expression (3) results in table 5. The table shows the data on vehicle speed, engine speed and the connection of the driver's mobile device and voice communication through the vehicle's infotainment system. In addition, the table also shows voice communication via driver's mobile device as well as the network activity of the mobile device at time *t*. The records displayed in the table represent simulated data and are used to visualize correlation of data and draw conclusions.

Table 5. Vehicle and user mobile device data over time

TIME	RPM	SPD	MDC	VCE	MDVC	NTW	MSG
1	2680	92	1	1	1	0.1	0
2	2750	98	1	1	1	0.6	0
3	3200	110	1	1	1	0.3	0
4	2930	103	1	1	1	0.2	0
5	2750	98	1	1	1	3.5	0
6	0	0	1	1	1	3.2	0

From the table it can be seen that in the moment t = 6 the speed of the vehicle and the engine speed have a sudden drop and are 0 in relation to t = 5 where the values are RPM = 2750 and SPD = 98. This indicates a moment of traffic accidents. At the moment t = 6 it is noticeable that the driver's mobile device is connected to the vehicle's infotainment system and that there is ongoing voice communication. An assumption is also confirmed by a log from the driver's mobile device within which it is apparent that the call was in progress at the observed time. In addition, according to the log records of the mobile device, there is an increase in network activity that can potentially indicate the interaction of user with the mobile device at times t = 5 and t = 6 where NTW = 3.5 and 3.2 respectively.

4. DISCUSSION

Telematics and OBD vehicle interfaces are a gateway for data exchange between vehicles and remote stakeholders. Therefore, they represent entry points through which it is possible to collect the necessary data for the implementation of digital forensic analysis. Although vehicle data analysis has the potential to detect vehicle events and activities, there are many challenges associated with the vehicle digital forensics. One of the challenges is a large number of separate ECU devices that have the ability to process, store and transfer data. Therefore, telematics systems within the vehicle often lack the ability to provide access to all the information required for investigation [2]. Because of the heterogeneity of the manufacturer and the vehicle there are differences in the operation of the ECU device and the data to be collected and the format in which they are stored, which can cause problems in the digital forensic processes.

The increase in the number of ECU devices implemented inside the vehicle for managing the numerous of vehicle functions also presents a challenge in terms of the increasing complexity of the system over which it is necessary to conduct an investigation. Accordingly, digital forensics will represent unquestionable support for investigating all types of vehicle-related incidents.

The telematics system also plays an important role in the development of cooperative intelligent transport systems that encompass the concepts of Vehicle to Everything (V2X) and IoV [24]. Investigations in such environments will require the use of digital

forensic procedures over vehicle ECU devices, as well as other elements such as the Cloud Computing environment, roadside units, etc.

CONCLUSION

This paper presents the research of digital forensics application possibilities for the purpose of event and activities detection in vehicle-related incidents. Digital forensic procedures have the ability to support standard forensic procedures in vehicle-related incidents. The reason is numerus ECU devices with the functionalities of collecting, processing and transmitting data associated with the vehicle. Often such data can represent evidence of a vehicle, driver or passenger events or activities, which may be crucial when conducting investigative conclusions.
Vehicle's telematics systems, due to the use of communication technologies (Bluetooth, WiFi, GSM), represent a gateway for accessing and collecting data from other vehicle subsystems. For the purposes of implementing digital forensics, knowledge of used data transmission technologies and the systems responsible for their collection and processing is necessary. Thus, the paper analyses the types of connection and communication between ECU device inside the vehicle as well as networks that are used for this purpose. In addition possible incidents and causes of incidents associated with the vehicle were identified and classified.
The sets theory was used for the purpose of presenting the correlation of vehicle collected data. Sets theory was used in a case study where vehicle and driver's mobile device data correlations were displayed for the purpose of gathering evidence of using a mobile device at a traffic accident.
Future research in this domain will focus on collecting real datasets from the vehicle and their correlation using scientific methods such as regression and machine learning with the aim of determining the interconnection of data.
Acknowledgment
This research is founded through project entitled The impact of mobile device usage on drivers' behaviour, within the National Road Safety Programme of the Republic of Croatia.

REFERENCES

[1] Horsman G., Conniss L.R.: Investigating evidence of mobile phone usage by drivers in road traffic accidents , Digit. Investig., vol.12, 2015, p. 30-37.
[2] Jacobs D., Choo K.K.R., Kechadi M. T., Le-Khac N. A.: Volkswagen Car Entertaiment System Forensics. IEEE Trustcom/BigDataSE/ICESS, 2017, p. 699-705.
[3] Hossain M., Hasan R., Zawoad S.: Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV), in 2017 IEEE International Congress on Internet of Things (ICIOT), 2017, p. 25–32.
[4] Husnjak S., Peraković D., Forenbacher I., Mumdziev M.: Telematics System in Usage Based Motor Insurance, in 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014, 2015, p. 816–825.
[5] Akalu R., Paving the way for Intelligent Transport Systems (ITS): The Privacy Implications of Vehicular Inotainment Platforms, Ontario 2016.
[6] Mansor H., Markantonakis K., Akram R. N., Mayes K., I. Gurulian, "Log Your Car: The Non-invasive Vehicle Forensics," in 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, p. 974–982.

[7] Navet N., Simonot-Lion F., In-vehicle communication networks-a historical perspective and review, vol. 96. Boca Raton, FL, USA: CRC Press, 2013.
[8] Lee J.-W., Choi K.-Y., Lee J.-W., Collecting Big Data from Automotive ECUs beyond the CAN Bandwidth for Fault Visualization, Mob. Inf. Syst., vol. 2017, p. 1–13, 2017.
[9] Kwasnoski J., Crash Reconstruction Basics for Prosecutors, St. Louis, USA, 2003.
[10] Peraković D., et al., Using mobile devices while driving in Croatia – preliminary analysis, in Proceedings of The 5th International Virtual Research Conference in Technical Disciplines (RCITD-2017), 2017, p. 56–61.
[11] Karie N. M., Venter H. S., Taxonomy of Challenges for Digital Forensics, J. Forensic Sci., vol. 60, no. 4, p. 885–893, 2015.
[12] KoscherK., et al., "Experimental Security Analysis of a Modern Automobile," in 2010 IEEE Symposium on Security and Privacy, 2010, p. 447–462.
[13] Pan L., Zheng X., Chen H. X., Luan T., Bootwala H., Batten L., Cyber security attacks to modern vehicular systems, J. Inf. Secur. Appl., vol. 36, p. 90–100, Oct. 2017.
[14] Bortles W., McDonough S., Smith C., Stogsdill M., An Introduction to the Forensic Acquisition of Passenger Vehicle Infotainment and Telematics Systems Data, 2017. [Online]. Available: http://papers.sae.org/2017-01-1437/.
[15] Agbonkhese O., Yisa G., Agbonkhese E., Akanbi D., Aka E., Mondigha E., Road Traffic Accidents in Nigeria: Causes and Preventive Measures., Civ. Environ. Res., vol. 3, no. 13, p. 90–99, 2013.
[16] Larson U. E., Phung P. H., Nilsson D. K., Vehicle ECU classification based on safety-security characteristics, IET Road Transp. Inf. Control Conf. ITS United Kingdom Members' Conf. (RTIC 2008), p. 102–102, 2008.
[17] Ilakkiya B., Vanitha V., A survey on engine control unit, Int. J. Adv. Res. Innov. Ideas Educ., vol. 2, no. 3, p. 21–25, 2016.
[18] Rana N., Sansanwal G., Khatter K., Singh S., Taxonomy of Digital Forensics: Investigation Tools and Challenges, Comput. Soc., 2017.
[19] Pilli E. S., Joshi R. C., Niyogi R., A Generic Framework for Network Forensics, Int. J. Comput. Appl., vol. 1, no. 11, pp. 1–6, Feb. 2010.
[20] Carrier B., Spafford E., An event-based digital forensic investigation framework, in Digital forensic research workshop, 2004, p. 1–12.
[21] Parate S., Nirkhi M. S. M., A Review of Network Forensics Techniques for the Analysis of Web Based Attack, Int. J. Adv. Comput. Res., vol. 2, no. 4, p. 2–7, 2012.
[22] Gandomi A., Haider M., Beyond the hype: Big data concepts, methods, and analytics, Int. J. Inf. Manage., vol. 35, no. 2, p. 137–144, 2015.
[23] Hauke J., Kossowski T., Comparison of values of pearson's and spearman's correlation coefficients on the same sets of data, Quaest. Geogr., vol. 30, no. 2, p. 87–93, 2011.
[24] Onishi H., Wu K., Yoshida K., Kato T., Approaches for vehicle cyber-security in the US, Int. J. Automot. Eng., vol. 8, no. 1, p. 1–6, 2017.