Internet of Things and Cloud Computing
2020; 8(1): 12-16
http://www.sciencepublishinggroup.com/j/iotcc
doi: 10.11648/j.iotcc.20200801.13
ISSN: 2376-7715 (Print); ISSN: 2376-7731 (Online)

Actual Issues of Modern Digital Vehicle Forensic

Roman Rak[1], Dagmar Kopencova[2]

[1]Department of Criminalistic and Forensic Science, University of Finance and Administration, Prague, Czech Republic
[2]Department of Security and Law, Ambis University, Prague, Czech Republic

Email address:
Roman.Rak@irisident.cz (R. Rak), Dagmar.Kopencova@seznam.cz (D. Kopencova)

To cite this article:
Roman Rak, Dagmar Kopencova. Actual Issues of Modern Digital Vehicle Forensic. *Internet of Things and Cloud Computing*. Vol. 8, No. 1, 2020, pp. 12-16. doi: 10.11648/j.iotcc.20200801.13

Received: April 17, 2020; **Accepted**: May 26, 2020; **Published**: June 3, 2020

Abstract: Today, the development of the automotive industry is associated with the phenomena of electromobility, autonomous vehicles, digitisation and telematics. New vehicles contain a large number of electronic control units which process and preserve digital data on the vehicle's activity and its occupants, including communication with the external environment. This data can also be used for forensic purposes, as described in this paper. Attention is also paid to current trends, problem areas and safety risks. The paper deals with sources, classification, characteristics and uses of digital information in vehicles for forensic purposes from various perspectives, paper describes main problematic issue of Digital Vehicle Forensic. The present-day development, advancement and operation of vehicles is inseparably linked with the introduction of electronic devices and digitisation. As a result of this trend, vehicles process, transmit and save a large quantity of operational data and data connected with the activities of the vehicle's occupants. This trend has a sharply rising character, especially in connection with the development of electric engines and an effort to create and put into operation entirely autonomous vehicles that do not require the active involvement of a driver in order to reach their established destination.

Keywords: Control Unit, Data Recorder, Digital Records, Forensics, Vehicle

1. Introduction

Electronic processes are carried out in the vehicles themselves, which, in addition, also communicate with other vehicles and traffic and telematics infrastructure. Data from a number of devices, which are a part of the vehicle or which connect to the vehicle (mobile phones, tablets and computers of its occupants, etc.), are saved to a cloud environment.

From the perspective of forensic disciplines and criminalistics, every modern vehicle creates a large quantity of digital evidence. On average, a contemporary, newly manufactured passenger car contains more than 75 electronic control units which store over 150 million lines of source codes of support programs and which generate over 25 GB of data [1] for every hour for which the vehicle is in operation!

2. A Vehicle as a Subject of Forensic Investigation

Vehicles can be involved in accidents (or other negative events) and may subsequently be subject to a forensic investigation [2]. They can also be an instrument (means) for committing or a target for criminal acts or other events or activities with a negative impact on safety (other than in the context of road traffic). In the first case, forensic and traffic engineers or forensic experts in the field of construction, maintenance and operation of vehicles or related fields are involved in clarifying the course of events and their consequences. In the latter case, the vehicle is of interest to criminalistics units and other security-oriented institutions which deal with a variety of criminal activities and guarantee general security as such at various levels.

In any case, every modern vehicle today turns out an enormous volume of data/information which can provide digital evidence that help to explain the course of negative events and their consequences.

3. Vehicles as a Source of Digital Data

Every modern vehicle contains a range of devices which generate, process, transmit or store digital data in various formats, which can be used as digital evidence to help in forensic investigations of incidents.

Typical data sources of digital evidence are:

a) Black boxes (Event Data Recorders - EDR)

b) Telematics and infotainment systems

c) Electronic Control Units (ECU)

d) eCALL units

e) Key fobs

f) Dash cams (front and rear)

g) Aftermarket technologies

3.1. Black boxes (Event Data Recorders - EDR)

Black boxes are the most widely used source of digital data (evidence) during forensic investigations of traffic accidents. They have been well-known in professional practice since the 1990s, when they were first used in the USA. Also known as Event Data Recorders (EDR), they are activated at the “moment” that a vehicle heads for a collision (traffic accident) [3]. The EDR records events 5 seconds before the traffic accident and subsequently records and stores data over the course of the entire event; this data can then be analyzed. Predetermined relevant data for accident analysis are sent to the EDR from an Electronic Control Unit (ECU) located inside the vehicle in a specified format and specified time sequences.

Single-purpose black boxes are primarily intended for accident analysis. They are not suitable, however, for forensic investigation of various acts of fraud, manipulation of the identifier of the VIN stored in the vehicle in digital form, odometer fraud (rolling back the number of kilometers travelled) and detecting other vehicle activities (including automated activities), as well as the conduct of the vehicle’s occupants and their communications with the environment outside of the accident event. A number of events outside of the accident have an extremely varied course and nature, and are often useful for forensic purposes during running investigations of serious criminal acts. This information or data are found elsewhere than in the black box.

3.2. Telematics and Infotainment Systems

The term “telematics” is derived from the words “telecommunication” and “informatics”. Telecommunications involve wire and wireless transfers of data between individual components of a vehicle, between different vehicles, and potentially external components and traffic infrastructure. The term informatics can be simply defined as a method of processing and storing data, including transmitted data. The terms “telematics” (just like the term “infotainment”) therefore expresses an ability to generate, send, receive and process data.

The term “infotainment” is a combination of the words “information” and “entertainment”. The word originated in the USA, primarily with the advancement of cable television as a type of news, where the choice of topics and their processing is intended to evoke emotions and to entertain. In the original sense of the word, infotainment was perceived as an insufficiently serious source of news.

The term infotainment was first introduced into the automotive industry and vehicle design in connection with the arrival of mobile phones and with video, CD/DVD players, screens (tablets) for entertaining occupants (usually children), particularly in the rear seats, and later with the use of touchless tablets on the central panel of the dashboard. The aim is to provide the occupants with the simplest, user-friendly information environment closely related to (and sometimes triggered by) the car’s location, and to enable them to control information and entertainment systems (radio broadcasts), to communicate with the environment (mobile phone control), to search for information on the internet, and to orient themselves in space (navigation systems). Today, infotainment systems can be controlled by touch screens, controls on the steering wheel, or by human voices. Data can be transmitted through various communication protocols and interfaces, such as Bluetooth, WiFi, USB devices, SD data cards, etc.

Infotainment systems in vehicles are an excellent source for analyzing the geographical movement of a vehicle (routes travelled, favorite routes, frequently visited destinations, etc.) and telecommunications activities of the vehicles occupants (phone calls, text messaging, internet activity, social network activity, and so on). The combination of these activities in terms of time and place of implementation gives a qualitatively new idea of the course and consequences of such events.

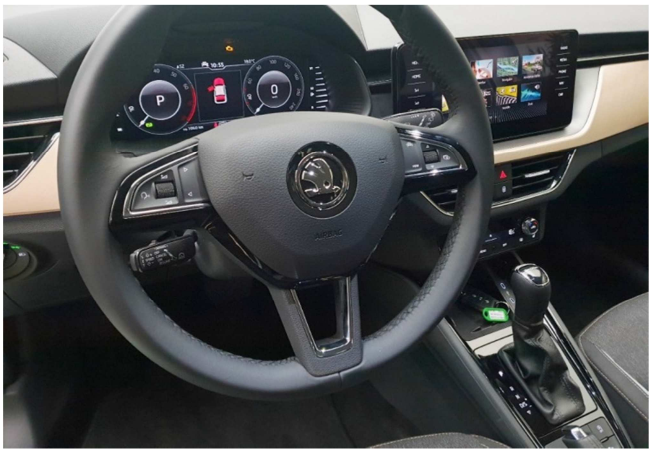

Figure 1. *Driver's seat of a modern vehicle. Škoda Kamiq. Photo R. Rak.*

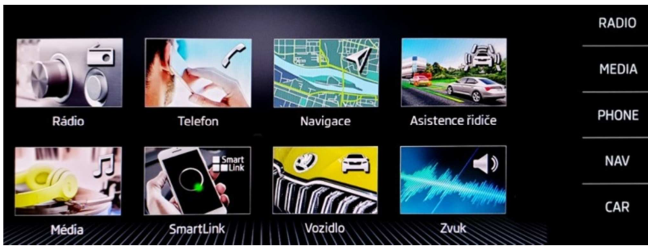

Figure 2. *Example of infotainment panel. Photo R. Rak.*

3.3. Electronic Control Units (ECU)

An electronic control unit (ECU) is a digital microcontroller which controls activities and operations in a vehicle. Modern vehicles usually have more than 75 ECUs which manage and control partial key processes and “operations” in the vehicle.

Every ECU is responsible for controlling certain specific processes, such as the status of engine, gearbox and airbag activity [4], fuel levels, the overall vehicle status, the number of closed doors and fastened seatbelts, etc. ECUs are closely connected to the vehicle's telematics and ensure data transmission and exchange. Data connectivity is ensured by various data protocols and standards, e.g. LIN (*Local Interconnect Network*), CAN (*Controller Area Network*), MOST (*Media Oriented Systems Transports*), FlexRay, WiFi, Bluetooth, etc.

Access to control and management units (to their data) inside a vehicle is provided by an external interface called OBD-II (*On-Board Diagnostics*), which makes it possible to connect to individual ECUs and to obtain required data or information.

Vehicle data is usually obtained through OBD connectors from ECUs or through a black box (EDR); this includes physical extraction of data. Data from such devices frequently have diverse, non-uniform and non-standard content across individual motor vehicle manufacturers.

3.4. eCALL Units

An eCALL unit is a device which is designed to call emergency services in the event of a car crash or an emergency involving an occupant of a vehicle. This technology has been used since 1st April 2018 in all new homologated vehicles in the European Union, including vehicles imported from outside Europe intended for the European market.

The energy-independent units with high resistance and long life are activated automatically (thanks to special sensors which register an impact of the vehicle or expansion of the airbags), or can be activated manually from the front seats. Next, the closest operating center of emergency phone line 112 is located, and data describing the location of the incident, the circumstances and the basic characteristics of the vehicle is transmitted by telematics systems. The following data is transmitted: part of the incident, the coordinates of the vehicle's location, the direction of travel, the VIN identifier, the vehicle category, the type of fuel, the number of fastened seatbelts (i.e. the number of persons wearing a seatbelt), an indication of how the unit was activated (manually or automatically) and various other information on the credibility of the incident. This data is displayed at the emergency line operating centre and serves primarily for organizing and carrying out rescue operations. However, the sent data can also subsequently be used for forensics and other security tasks for investigating fraud (e.g. changes to the vehicle's identity, faking a traffic accident, and so on).

3.5. Key Fobs

Key fobs (smart keys) to modern vehicles are another source of valuable information of forensics investigations. They serve as an external storage device for selected important vehicle data. Key fobs contain a globally recognized unique identifier (*Vehicle Identification Number* - VIN), a key transponder ID number, time data stamps indicating the last time that the key was used, the status of the odometer (counter of distance travelled by the vehicle) corresponding to the time stamp, the number of paired keys to the vehicle, the amount of fuel in the tank, other paired data as of the time that the key to the vehicle was last used, and more. Data from key fobs for unlocking a vehicle can generally be read by authorized service centers or specialized forensics instruments.

3.6. Dash Cams (Front and Rear)

Vehicles are equipped with cameras that capture and record movement and events occurring in front of and behind the vehicle in the form of digital time loop recordings. These video sequences are a welcome source of information when investigating traffic accidents. They provide visual information on the scene around the vehicle and the conduct of other road users. Recordings can clarify the conduct of certain road users (so-called brake tests, tailgating, failure to give way, improper driving in parallel lanes, dangerous overtaking, running a red light, passing over a level crossing when the warning signals are activated, and so on).

3.7. Aftermarket Technologies

Other digital (usually recording) devices can be installed in a vehicle. These relatively often include journey logs in so-called fleet vehicles (company vehicles used either entirely for business purposes, or for combined purposes – business/private). The operators of such vehicles are provided with real-time information on the movement and other activities of the vehicles. The aim is to reduce paperwork (manually filling in a logbook), to optimize operation costs, to streamline vehicle movement logic, to provide information on the current status of the vehicle, and to prevent fuel theft and abuse of the vehicle for private purposes, etc.).

Devices of this type obtain information not only from their own navigation systems, but often from the vehicle's ECUs. A specific feature of such devices is intensive telematics operation, where monitored characteristics are transmitted to the vehicle operator and then stored in the operator's own information systems or in a cloud (virtual) environment. This fact heavily affects (in a certain sense of the word, significantly complicates) forensic methods [5] of obtaining such data which is not stored and preserved in the vehicle's equipment, but in third party systems, to which it is then necessary to acquire authorized access.

Data from telematics applications like journey logs can be derived from applications intended for insurance companies. Data from selected vehicle ECUs are then transmitted to remote data repositories (clouds) and various characteristics of the vehicle's operation are assessed. These include the nature of the driver's driving style (e.g. an aggressive type – speeding, abrupt braking, intensive braking [6]. The amount of the vehicle's insurance premiums then depends on these parameters.

4. Forensic Use of Digital Evidence

In forensics practice (engineering and criminalistics), it is possible to use digital data (evidence) for determining, analysing, clarifying, etc. the following:

a) the vehicle's identity (Vehicle Identification Number and serial numbers of individual vehicle components) [7]
b) the driver's conduct while driving and operating the vehicle (e.g. defensive versus aggressive driving)
c) the behaviour of the vehicle and/or driver over the course of an accident, and the cause and consequences of the accident
d) activity around the vehicle
e) (un)justified ((un)authorised) interventions into the vehicle's technology (e.g. rolling (i.e. clocing) back the number of kilometres travelled)
f) (un)authorised exchanges of vehicle components
g) use of telecommunications by the vehicle's occupants - their "digital activity" inside the vehicle
h) the vehicle's geographical location
i) the economy of the vehicle's operation

In the future, we can expect much greater vehicle autonomy, coupled with very strong information support and telecommunications with all objects involved in driving and road logistics, including artificial intelligence elements. Vehicles will use their "experience", learn, and exchange information with other vehicles (v2v - *Vehicle to Vehicle*), traffic infrastructure (v2i - *Vehicle to Infrastructure*), parking spaces, etc. It will subsequently be entirely possible and essential to use much of this information for forensics work.

5. Problem Areas to Be Resolved

The automotive industry is one of the most intensively developing fields. Commercial pressure is enormous, and manufacturers and individual brand names strive to outdo each other in their ranges. Anything that is new and innovative quickly finds customers, meaning that things that prove successful for one brand will usually appear in one form or another in other brands. With changes occurring at an extremely rapid pace, time intervals between individual changes are very short and constantly decreasing.

Trends in electromobility and vehicle autonomy are clear to see. In practice, however, this results in certain paradoxes in terms of security, and in substantial threats [8, 9]. The highly dynamic nature of development and production often overtakes safety practice, especially as regards vehicle information and telecommunications systems. In many cases, manufacturers pay insufficient attention to these concerns [10].

Modern trends of information and communications technology also find a use in the automotive industry. The result is a logical integration of ECUs and their CAN buses, as well as infotainment systems inside a vehicle (which contain a considerable quantity of sensitive data) with the external environment by way of internet interfaces to remote data repositories and to various remote third-party applications. The vehicle becomes a part of the Internet of Things.

In the case of insufficient security measures, the opposite path can therefore be used to access the data and functionalities of a vehicle: to use the internet to gain unauthorized control of individual ECUs inside the vehicle. In recent years, various scientific conferences [11], have demonstrated ways in which hackers can gradually gain control of vehicle systems all the way to steering the vehicle, operating the brakes, etc.

Standardizing new technologies in practice is a tough nut to crack. When innovating, it is not necessarily possible to know exactly how things will turn out, what the consequences might be and whether innovations become established in practice [12]. As a result, different manufacturers or groups of manufacturers achieve their goals after a time by various means, technologies or their own data standards. In practice, it is therefore no easy task to carry out diagnostics, to examine the content of black boxes, to monitor various processes or to read data from ECUs across all brand names. From the perspective of diagnostics by independent service centers, government institutions (technical and emissions control stations, checks for unauthorized interference with systems, etc.) and forensics institutions, every manufacturer or group of manufacturers uses its own technology, readers, etc. Therefore, if any institutions wish to work with all brand names, they must obtain multiple devices which are only compatible with the systems of certain brand names. Universal instruments essentially do not exist, which increases not only costs, but also demands for technical equipment and software, expert knowledge, ongoing training, etc.

Standardization of processes within the EU is progressing very slowly. The adoption of a standard for eCALL [13] technology alone took over 8 years, and the first requests or ideas for transmitting information from a stricken vehicle to rescue operation centres are more than 30 years old.

Figure 3. *A digital dashboard is capable of displaying much more information than traditional analogue dashboards. Drivers can set up several appearances and choose the one that suits them best. Dashboard of an Audi Photo R. Rak*

6. Conclusion

The examination of digital data relating to the operation of motor vehicles (*Vehicle Digital Forensics*) is one of the widest fields of digital data (evidence) analysis, which is typically referred to as *Digital Forensics* or *Computer Forensics*. Today, examining data and digital evidence ensuing from the use of computers, mobile phones and other components of equipped processing units is a relatively stable field which has gone through a somewhat difficult history.

Vehicle Digital Forensics is a field that is just emerging and is still waiting to be put into extensive use. Key issues are the standardization of data interfaces, recording units and in-vehicle data storage on the one hand, and their use and application in forensic activities on the other. There will undoubtedly be a need for affordable, sufficiently general and certified forensic technologies that will be relatively easy to use in forensic investigations, as well as adequate forensic methods and methodologies. These activities will be closely associated with the training of entirely new kinds of specialists [14, 15], forensic engineers and forensic workplaces [16], whose subject matter will be highly multidimensional.

References

[1] E. A. Bates, “Digital Vehicle Forensics” [online]. [cit, 2019-11-17]. Available at https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf

[2] L. Moravcik and M. Jaskiewicz, M. “Boosting car safety in the EU”. 11th International Scientific and Technical Conference on Automotive Safety, 2018, Location. Casta Papiernicka, Slovakia

[3] “Event Data Recorders” (US National Higway Traffic Safety Administration regulation) (NHTSA), 2018 edition, updated as of May 29, 2018, The Law Library, printed by Amazon, ISBN 9781729754900

[4] P. Posuniak, M. Jaskiewicz, K. Kowalski and F. Dabrowski, F. “Child restraint systems: problems related to the safety of children transported in booster seats (without integral safety belts)”. 11th International Scientific and Technical Conference on Automotive Safety Location. Casta Papiernicka, Slovakia, Date: Apr. 18-20, 2018

[5] T. Hajdukova. Research Methodology, In: “Application of Scientific Methods to Cases from Police Practice”. 2016, ISBN 978-80-8054-766-0 (2018), pp. 8–35.

[6] K. Pavlica, R. Kaiser and E. Jarosova, E. “Balanced Leadership; Managerial Skills Dynamics”. Prague: Management Press, 2015. ISBN 978-80-7261-289.

[7] R. Rak, P. Kolitschova and P. Kerbic P. “Forensic and technical aspects of vehicle identification labels.” 11th International Scientific and Technical Conference on Automative Safety, Casta Papernicka, 2018, Slovakia, Proceedings Paper.

[8] M. Felcan, D. Kopencova and R. Rak. “Objects and systems - Basic analytical security features”. Proceedings of the 14th International Symposium of 14 March, 2019 in international Security expo Bratislava 2019, Academy of Police Force in Bratislava, Bratislava, pp. 212, ISBN 978-80-8054-795-0, pp. 41–55

[9] M. Felcan, “Implementation of European Union legislation and regulations on road safety standards of the Slovak Republic” In: Security of transport on the road. 2008, pp. 122-132, ISBN 978-80-232-0292-2.

[10] L. Moravcik and M. Jasksiewicz, “Boosting car safety in the EU”. In: Automotive safety 2018: proceedings of the XI International Science-Technical Conference: Kielce University of Technology, 2018, ISBN 978-1-5386-4578-9, Web of Science 2018-07-09, 345 E 47th ST, New York, USA, ISBN 978-1-5386-4578-9, IDS Number: BK3OJ, Accession Number: WOS: 000435296000013.

[11] H. Mansor, K. Markantonakis, R. Akram, K. Mayes and I. Gurulian, “Log your car: The non-invasive vehicle forensics”. 2016 IEEE International Conference Trustcom/BigDataSE/ISPA, Trust, Security and Privacy in Computing and Communications, [online, cit, 2019-11-26], Available at https://ieeexplore.ieee.org/document/7847047/authors#authors

[12] P. Augustin and R. Odler, “The mission of the police in a democratic state in the context of globalization”. In: Securitologia: czasopismo naukowe, pólrocznik. Vol. 18, Nr. 2, 2013, ISSN 1898-4509, pp. 55-64.

[13] I. Matouskova, L. Moravcik, R. Rak and A. Tallo, “eCall, intelligent transport system (legal, technical, informational and psychological aspects)”. Slovakia, Bratislava: Magnet Press Slovakia, 2015, 189-215 pp., ISBN 978-80-89169-31-3

[14] D. Kopencova, “Secondary education with security focus”. INTED 2020 Proceedings, pp. 2477-2481. 14th International Technology, Education and Technology and Development Conference. 2nd-4th March, 2020, Valencia, Spain. ISBN: 978-84-09-17939-8, ISSN: 2340-1079

[15] F. Vlach, “Evaluation of Cooperation between Educational Institutions of the Armed Forces”. New trends in police training III. International conference. Holesov: Higher Police School and Secondary Police School of the Ministry of the Interior in Holesov, 2018, pp. 121–124. ISBN 978-80-7616-008-8.

[16] R. Rak and R. Zrubak, “Project eCALL – Car in Emergency Situation”. 7th Scientific International Conference Crisis Management: Envirenmental Protection of Population – Conference Proceedings. Edited by Horak, R; Juricek, L; Schwarz, R. pp. 251-258, 2012. Proceedings paper.