HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 1. szám 125–141.
DOI: 10.32567/hm.2023.1.9

József Répás[1]

Definition of Forensic Methodologies for Autonomous Vehicles[2]

Digitisation is present more and more widely in the vehicle industry, the use of modern and increasingly self-driving vehicles is appearing more and more widely. Their use becomes more appropriate and necessary in industry, transport, military and logistics applications. The spread of these highly automated vehicles will have a direct impact on road accidents, violations and crimes. In the event of accidents, the determination of responsibility and the identification of the perpetrators of crimes will continue to be necessary in the future, for which tools and procedures are currently not available or not fully applicable. By connecting vehicles and infrastructure elements, the range of data related to events has been greatly enhanced. This information must be extracted and analysed during the investigations. The purpose of the investigations is to determine what, when, where and how it happened, who were involved, and to determine responsibility.

The basis of the expert investigation of self-driving vehicles and cooperative transport systems is the classical forensic procedure and digital forensics. On the other hand, the field requires specific knowledge, preparation, specific tools and approach. In this study, the existing, already used digital forensics examination methods are described, the applicability of some of them, some steps or tools that require further examination in the case of modern and increasingly autonomous vehicles.

Keywords: digital forensics, autonomous vehicles, autonomous vehicle forensics, C-ITS

Introduction

Through our various online activities and the use of our digital devices, we leave behind a so-called digital footprint. This can be a sent email, a photo uploaded to a social

[1] PhD student, University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military Engineering, e-mail: repas.jozsef@uni-nke.hu

[2] Prepared with the professional support of the Doctoral Student Scholarship Program of the Cooperative Doctoral Program of the Ministry of Innovation and Technology financed from the National Research, Development and Innovation Fund. The authors would like to especially thank the Management Director and staff of Alverad Technology Focus Kft. for their support for the research work.

network or the MAC ID of our laptop, which is recognised and stored by a server.[3] Our vehicles, which are becoming more and more modern, work in a similar way, the connectedness, the intelligent cooperative transport systems contain a large amount of information about drivers or passengers. For example, about what the user did, when and where she/he was, who he met, etc. Our vehicles process, transmit and store much more data than the average user thinks.

These data can be analysed during a forensic examination and can be interpreted as traces, with their help it can be determined what happened. With the help of the traces, the expert conducting the investigation can create a timeline of an event, which contributes to answering questions related to the purpose of the investigation. When examining the digital data available in vehicles, an important step is to filter relevant information from irrelevant information. As with all methods, forensic examination has its limitations, the understanding of which is important for its use, since critical decisions affecting life and freedom can be made as a result of the analyses. The key to success is ensuring that all relevant evidence, including digital evidence, is preserved in a timely and appropriate manner.

The purpose of forensic investigation is to create a timeline of the events or accidents, research relevant evidence, identify those involved and suspects, and discovering the methods and means of committing the crime. Tasks to be performed during the investigation include, for example, acquiring data (or providing access to it), ensuring data integrity, reconstructing and restoring deleted data, identifying relevant data, or compiling a narrative of the event. There is no developed methodology for performing these tasks, no universally suitable technique that can be used during all forensic examinations. There are many different, yet useful, subdomains of digital forensics. The purpose of this study is to collect the forensics sub-domains the steps or techniques of which can be used to obtain information that helps to understand the cases.[4]

These standard practices cannot be applied in case of autonomous vehicles, due to their specific operation. In order to be able to conduct the investigations and continuously develop the system, a timely collection of evidences may be essential. As technology advances and the range of tools grows, the efficiency of existing forensic solutions needs to be examined. New technology and increased data volume, new data sources require new forensic solutions, approaches, processes to answer previous and possibly new questions.

In-time collection of evidence may be essential for conducting investigations and continuously developing new systems. As technology advances and the range of tools grows, it is necessary to examine the usability of existing forensic solutions.

[3] Quadron s. a.

[4] Lyle et al. 2022.

Forensics

In forensic science, natural science methods and techniques are systematically applied, regardless of their type. Computer science, military, mechanical, chemical, civil and electrical engineering – as tools – help to explore the causes and the truth by collecting, extracting and examining evidences. Forensic science supports civil and criminal proceedings, reconstructs events, justifies lack of bias in a legal case. [5] As an applied science, forensic science serves as an investigatory tool.[6]

"The word forensic comes from the Latin word forensis: public, to the forum or public discussion; argumentative, rhetorical, belonging to debate or discussion."[7] Several definitions are used to define forensic science. One of these is the "application of a broad spectrum of sciences and technologies to investigate and establish facts of interest in relation to criminal or civil law"[8] and, according to a modern definition, the forensic "relating to, used in, or suitable to a court of law. Any science used for the purposes of the law is a forensic science".[9]

Today's modern forensic basics were already applied in the ancient times by the Greek inventor, mathematician and physicist Archimedes (287 to 212 B.C.E.). His Eureka legend could be regarded as an early use of forensic science. He examined the principles of water displacement in order to be able to prove whether the crown was made of gold or not only by its density and buoyancy. Another forensic approach was the establishment of identity-proof with the use of fingerprints in the 7th century just as the use of medical evidence to understand the mode of death in the 11th century in China and later on in 16th-century Europe. Already in the 12th century King Richard I introduced a so-called Office of the Coroner in England to combine the medical and legal approach for dealing with crimes. This approach is still applied in the United States and no federal law requires a coroner to be a licensed physician.[10]

The development of criminal litigation and the change in representation in litigation have enabled the parties to prove their truth. In the 19th century, the examination of Francis Galton's fingerprints was significant among modern examinations, which later evolved also due to the determination of blood groups. Outstanding achievements in the 20th century forensics were the design and conduct of ballistic investigations. The first forensic lab was founded in 1932 by the FBI. Due to the application of the technological achievements of the 19th century in criminal and litigation proceedings other disciplines and the establishment of new forensic laboratories had been involved as well. In 1984, the FBI's investigative practice first introduced computer forensics.[11]

Some studies still require the cooperation of different forensic areas, specialised experts such as medical experts, criminalists and other engineers. These areas overlap sometimes as well and are mostly applied in order to support and resolve legal cases.

[5] Siegel 2017; Vízi 2019; Calvert 2017.
[6] Legalbeagle 2019.
[7] Aafs 2022.
[8] Hüschelrath–Schweitzer 2014.
[9] Aafs 2022.
[10] Aboutbioscience 2022.
[11] Vízi 2019.

As each case is different, the primary task is to ensure impartiality and to protect the evidence (continuously from exploration to preservation), to reconstruct the timeline of the events. The events that have taken place have to be verified and made obvious by performing a deep examination, even if the case cannot be repeated.[12] In the course of forensic examination, from the discovery and exploration of the evidence, through the processes consisting of several continuously documented steps, we can get to the examination results, to their presentation and evidence storage.[13]

Generally, in case of investigation of traffic accidents, the aim is to reconstruct the events as accurately as possible, to determine the responsibility, to prove by whom the accident was caused by, collecting information such as skid marks, vehicle position, track and environmental conditions, vehicle, driver and passengers injuries and testimonies.[14] With the appearance of modern and increasingly automated vehicles, the range of evidence is expanding significantly. Information about vehicles, the track and the environment will be available in increasingly complex systems, creating a new challenge for digital forensic professionals. As technology advances, the techniques, solutions, tools and procedures applied should be improved and newer, more efficient methods and methodologies should be developed to record, analyse and preserve evidence.[15]

Digital forensics

The application running at a certain event and moment can also be determined such as the content consumed on the Internet. This information can be restored, even if the evidence is deleted. The development of vehicles, the proliferation of mobile communication devices and the emergence of cooperative transport systems result in a wide ranging array of complex evidences, and created many new potential source of evidence. There are many problems and complicating factors in the field of data availability, collection and evaluation, and currently there are significantly fewer solutions. A complex, effective methodology and a solution are not available yet.[16]

Digital forensics is "the science of identifying, preserving, recovering, analyzing and presenting facts about digital evidence".[17] According to the conceptual definition of the EC-Council, "digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events".[18]

According to the Interpol's approach, "digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on

[12] Calvert 2017.

[13] Vízi 2019.

[14] Siegel 2017.

[15] Calvert 2017.

[16] Stander–Barnard 2017.

[17] Stephens 2016.

[18] EC-Council 2022.

data stored electronically. […] The main goal of digital forensics is to extract data from electronic evidence, process it into actionable intelligence and present the findings for prosecution".[19] In a practical approach, digital forensics is about investigating crimes committed using digital devices, such as computers, mobile devices, cloud, network, etc.[20] Digital forensics thus can be interpreted in several approaches, depending on the subject of the investigation and the nature of the device (see Figure 1).

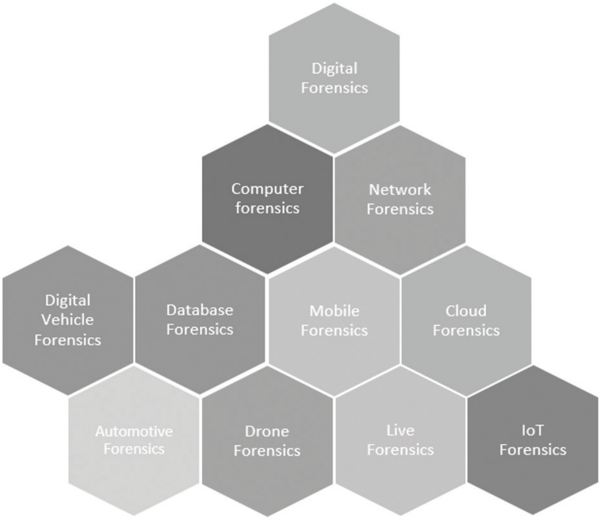

Figure 1: Digital forensics and others
Source: Compiled by the author

Highly automated and increasingly self-driving vehicles can be considered rolling computers, "data centres", which are connected to each other, to environmental and track elements, operators, service providers and supervisory organisations. According to this, in the further phases of the research, it is necessary to examine the methods and steps of both computer forensics and network forensics, in order to determine which elements of the methods can be implemented for the examination of future vehicles. Nowadays, it is common to connect our mobile devices to vehicles, or the vehicle itself provides network access, contains some kind of mobile internet connection, in this case the vehicle can be considered a mobile device, and the mobile forensics procedure can also be interpreted as one of the areas to be investigated. Thanks to the network access of the vehicles, the large amount of data collected by sensors (Lidar, radar, GPS, etc.) and cameras becomes available not only in the databases located inside the vehicle, but also in the management of some service provider (e.g. manufacturer, operator, etc.). This information is processed in information chains.

[19] Interpol 2022.

[20] Khanafseh et al. 2019: 610–629.

According to some approaches, satellites, GPS, SCADA are interpreted as a separate category of digital forensics,[21] however, in a military context, for example, in case of testing self-driving combat vehicles, information from these systems may also become necessary.

The aim of digital forensics are the followings:

- define the event
- provide authentic evidence
- finding and exploring evidence
- determine the source of evidence, extract information
- to give an answer to Who, Why, Where, When, What and How[22]
- preservation of evidence[23]

The principles of digital forensics are:

- securing the crime scene and keeping the evidence secure by prohibiting any access to the suspected digital evidence, documenting all processes and connections, disconnecting wireless connections, etc.
- limiting evidence interaction to "make sure that your evidence is having a limited interaction by capturing the ram and can also perform cold boot attacks on the evidence"[24]
- maintaining Chain of Custody, maintaining the sequence the evidence was recorded in with date and timestamps, identifying the investigator handling it[25]

The first step of the effective digital forensic process is always the 'Evidence Identification' preceded by the assignment, request, authorisation (by a legal authority, such as a search warrant or consent).

The identification and search of evidence, the identification of the elements of the system containing the information are an important part of every expert investigation. There is no documented method to perform the expert process for identifying modern vehicles or devices that implement increasingly complex self-driving functions, or a reliable tool for properly collecting the evidence that can be found.

Potential evidence collection may include computers, mobile devices, storage devices, copies of data from cloud accounts and other sources, and in case of vehicles, the vehicle's or data storage units. Data collection steps must ensure the integrity of the data acquired and provide a stable source for data analysis.

Acquiring digital data is the most basic task of digital forensics, the basic technique of which is to make a copy of the data to be examined. In the early days of digital forensics, the acquisition of digital data meant the acquisition of the contents of computer hard drives, floppy disks and CD-ROMs, from which an image was made. In case of vehicles, new challenges appeared in this area as well. By analysing the binary image of the vehicle's infotainment and telematics system, it becomes possible to

[21] Forensic Focus 2020.

[22] Bergholtz 2019.

[23] Årnes 2017.

[24] Chandel 2020.

[25] Chandel 2020.

extract data that can be used to determine, for example, the vehicle's route, timeline of events, and locations that can be connected to the vehicle.

After acquiring the data, they must be analysed during the forensic investigation. In the evidence analysis phase, special techniques and tools are applied (aggregation of evidences, correlating them, filtering, transforming and generating metadata, joining the bits and pieces of the pieces of evidence, retrieving deleted files).This is largely done with an interactive tool that must recognise and analyse the data structures and metadata embedded in the acquired data to display the content. The identification and extraction of data includes the identification and extraction of relevant information from the evidence, in order to create a timeline of the event and to answer questions that arise during the investigation.[26]

The penultimate phase is the detailed documentation of the steps of the investigation, the activities performed as well as the conclusions and results. The presentation phase deals with the presentation of the results, the opinion in the framework of the legal procedure, the representation of the opinion, which is not necessarily needed in each of the cases[27] (see Figure 2).

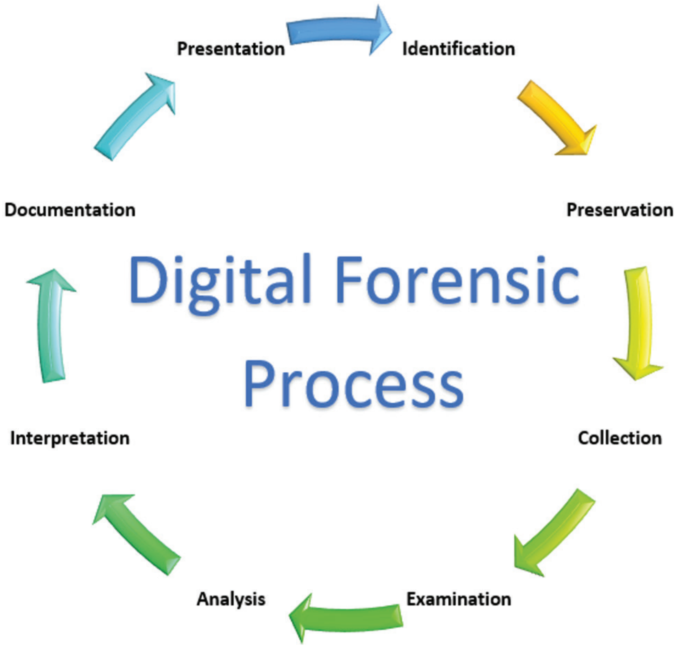

Figure 2: Digital forensic process
Source: Compiled by the author

[26] Lyle et al. 2022; Kävrestad 2020.
[27] Sule 2014; Stephens 2016; Chandel 2020; Vízi 2019; Gogolin 2021.

The 8-phase process of digital forensics can be interpreted in each of its areas. According to the specifics of the different areas, different procedures, tools and methods can be applied.

Computer forensics

Computer forensics is one of the basic elements of the digital forensics family, which consists of "the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data".[28] The purpose of Computer Forensics is to acquire, preserve, retrieve and present the stored data on a data drive device in a computer environment.

"As a forensic discipline, nothing since DNA technology has had such a large potential effect on specific types of investigations and prosecutions as computer forensic science."[29] At the same time, nowadays, most of the traditional forensic disciplines are different. Both the devices tested, and the techniques used are "products of a market-driven private sector", and tests normally performed under laboratory conditions, are often performed on site. Therefore, the result of the analyses will be direct information instead of interpretative conclusions, which is of high significance in a case".[30] Considering that vehicles are becoming more and more software-oriented devices, they can also be interpreted as rolling computers, computer forensic procedures and techniques will be an unavoidable part of future vehicle investigations.

Network forensics

As the number of IT systems and other networked devices has been growing and the prevalence of cybercrime and cyberattacks has been becoming more widespread, the investigation of events on networks is also becoming increasingly important. Capturing, recording and analysing network traffic, information, events in order to detect the source of network security attacks, locate and examine intrusions are gaining importance.[31] With the emergence and spread of cooperative intelligent transport systems, the network connectivity of vehicles becomes a fundamental factor. Not only will the vehicles communicate with each other, but also with their surroundings, the track and pedestrians, through various communication channels. The data transferred via such communication networks can also be used as an input for the expert examination of vehicles; therefore, it is necessary to examine the application possibilities of network forensic solutions and techniques.

[28] Chandel 2020.

[29] FBI 2000.

[30] FBI retired 2022; NIST 2015; FBI 2000.

[31] Kostadinov 2020; Liu et al. 2015.

Cloud forensics

Due to the spread of cloud-based solutions, digital transformation is also taking place. From software through platforms to infrastructure, we are increasingly using more and more services, where security and compliance are of primary consideration. More than 50% of personal and corporate data is stored in a cloud-based solution. In case of these systems and solutions, it may be necessary to analyse and examine the events afterwards, whereby one of the areas of digital forensics, cloud forensics is available.

At the definition level "cloud forensics is the application of digital forensic science in cloud computing environments",[32] using a hybrid approach, and virtual networks, thin and thick clients, remote access are examined in order to access the evidences. In order to be able to conduct the investigation and carry out the required analyses, information is needed from the side of the cloud provider, cloud consumer, cloud broker and cloud carrier as well, which needs to be interpreted in organisational, technical and legal terms, as well as addressing multi-jurisdictional issues.[33] The processing and storage of a large amount of information collected by vehicle sensors cannot be implemented in all cases or is not necessary for all data within the vehicle. The interconnectedness of vehicles also appears in case of different service providers, manufacturers and operators, so it must be taken into account that data related to the vehicle and the case under investigation are available at a cloud provider, or that processing and/or storage near the sensor takes place (fog computing). For this reason, the examination of cloud forensic techniques and solutions must also be taken into account for the examination of vehicle data.

Mobile forensics

With the proliferation of mobile phones, almost everyone owns their own device now. Nearly 70% of humanity can be considered mobile phone users. We spend a significant part of our lives online. Thanks to billions of "cellular subscriptions" worldwide, the mobile Internet traffic measured in exabytes and the growing number of device features and their increasing performance, mobile phones have become the most important data sources in digital forensics nowadays. It is not only an advantage but also a challenge for those working with mobile forensics mostly due to the rapid change in technology, wireless communication technologies, proprietary interfaces, mobile device platforms, etc. By definition, mobile forensics is the examination and analysis of stored information on mobile devices, identification, collection, examination, and analysis.[34] One of the basic functionalities of our modern vehicles is that they are suitable for communication with our mobile communication devices, or have a mobile communication channel themselves, typically for transmitting operating data sent to the manufacturer, for Software and Firmware Updates (Software Over

[32] Ruan et al. 2011.

[33] Forensics Colleges 2022; Ruan et al. 2011; Ruan et al. 2013; Joshi – Shubhakar Pilli 2016: 187–202.

[34] Hendricks 2022; Walsh 2021; Interpol 2021; Krasznay 2021; Munday 2021.

the Air – SOTA, Firmware Over the Air – FOTA) and to implement the eCall function. Examining the data received and transmitted by the vehicles over the mobile network can also contribute to the expert investigation, so mobile forensic techniques and solutions must also be taken into account.

Database forensics

The "database forensics is an emerging field" in relation to the growing number of illegal acts committed by electronic items and the critical data stored in databases.[35] Considering the large amount of data generated in the systems, the key aspect is the tracking of the related operations (modification, compromise), the reconstruction of damaged or deleted databases. Database forensics is responsible for examining the contents of databases, the related metadata, identifying incidents related to the database, as well as analysing and reconstructing related information.[36] Both the information within the vehicles and the information shared with the various environmental and track elements are stored in databases, the examination of which can contribute to the success of the procedure.

IoT forensics

IoT (Internet of Things) collects all sensory devices that are designed to collect and provide information and are able to share data over an Internet connection. The devices communicate with each other, the user, the central system, the cloud, and so on. A great part of the information generated and shared by IoT devices falls into some sensitive category. Data that is sensitive from the point of view of business, privacy and cybersecurity also account for an increasing share of network data traffic, and are also available from the Internet, and IoT devices and systems are becoming increasingly popular targets for cyberattacks.

The basic elements of the expansion of both Industry 4.0 and intelligent vehicles are the IoT and various cyber-physical devices, sensors, environments, the subsequent forensics, whereby the reconstruction of events is an essential element. The purpose of IoT forensics is to identify the sources of data generated, transmitted and stored by IoT-related events, devices connected to the Internet and sensors, and to identify, collect and analyse the data.[37] IoT and various cyber-physical devices, sensors and environments are the fundamental elements of the rise of intelligent vehicles, the subsequent forensic examination of which is an essential element for the reconstruction of events.

[35] Beyers 2013; Fowler 2008.

[36] Al-dhaqm et al. 2017; Al-dhaqm et al. 2020; Williams 2022;

[37] Gehlot et al. 2022; Flaglien 2017; Gillis 2022; Karthika 2022; LDSZ 2021.

Drone forensics

Millions of Unmanned Aerial Vehicles (UAVs) are registered worldwide, and nearly 50% of them are for commercial use. In addition to the registered UAVs, there are also plenty of devices in private use. These devices have a wide range of illegal uses, ranging from smuggling (e.g. drugs, etc.) to unauthorised surveillance, possible attacks, the transport of explosives and the disruption of aviation. Thanks to their continuous technological development, popularity and wide range of uses, they store a large amount of information about both the events they attended and their users. It is the responsibility of drone forensics to recover, obtain, process and analyse this information. Data generated by UAVs, such as flight path, time, images and videos greatly contribute to the reconstruction of the events.[38]

Live forensics

Live forensics is responsible for volatile data generated during the operation of digital systems, snapshots of information in memory during run, and data processing and analysis. It also makes available information not available in a post-mortem scan, such as a static disk image. This information can be the services run, event logs, registered drivers, etc.[39] If it is possible to access the vehicle in time, the examination can be started immediately, volatile data can also be a useful source of information.

Digital vehicle – automotive forensics

The transport ecosystem, one of the most important elements of individual transport is the automobile. Since 2010, the number of registered vehicles has almost doubled to 1.5 billion. These vehicles not only serve transport, they also contribute to our everyday life with more and more functions and services. Interconnected vehicles are becoming more intelligent, and within a few years, vehicles approaching in a completely autonomous way will also appear. By perceiving their environment and using advanced decision-making, they carry out their participation in transport and their planning processes more and more independently, without human intervention. In order to fulfil all these, advanced sensor networks, new communication channels, artificial intelligence and automatic control technologies are used to improve traffic safety. Ex-post peer review of data generated in vehicles and Cooperative Intelligent Transport Systems and Services is becoming an increasingly important area.

While previously vehicle forensics typically involved the collection of physical evidence (e.g. fingerprints, trace materials) and the physical inspection of a vehicle, digital vehicle forensics related to vehicles has emerged as vehicles become more intelligent. "Digital vehicle forensics is a branch of digital forensics that involves

[38] Digitpol 2022b; Forensics Colleges 2022; Singh 2022; QCC Global 2020.

[39] Adelstein 2006; Husain–Khan 2019; SciTech Connect 2013.

recovering digital evidence or data stored in a vehicle's modules, networks, and messages sent across operating systems."[40]

This area contributed to the success of forensic investigations by getting to know the route and destination of the vehicles and various driving information. Since drivers "interact with the vehicle" by the infotainment system, synchronise their mobile phones, personalise some of their functions, the vehicle has a large amount of information about the user. This information can be retrieved and analysed in a study.[41]

Considering the wide range of information that can be accessed, retrieved, extracted and tested by vehicles, Kevin Klaus Gomez Buquerin and his co-authors call the forensic analysis of modern vehicles "automotive forensics' in their study entitled "A Generalized Approach to Automotive Forensics".[42]

Today's vehicles contain a wide range of information:

- about the vehicle (e.g. serial number, part number, key ID, etc.)
- about installed apps (e.g. weather, navigation, Facebook, Twitter, etc.)
- about connected devices (e.g. media player, USB drives, SD cards, wireless access point, etc.)
- about navigation (e.g. history, saved locations, past destinations, active and inactive routes, speed logs, etc.)
- about mobile devices (e.g. device ID, call list, contacts, SMS messages, pictures, sounds, videos, access point information, etc.)
- other events (e.g. crash data, door opening/closing, lighting on/off, Bluetooth connections, Wi-Fi connections, USB restarts, GPS time synchronisation, speed, steering angle, mileage, gear change, strong acceleration deceleration, driving warnings, etc.)[43]

The Society of Automotive Engineers (SAE) J3016 defines the vehicle self-driving levels between SAE 0-6. The first three levels feature vehicles with different driver support, while the SAE Level 3 features self-driving capabilities and automated driving services. However, the driver supervision and intervention is still essential. In case of a vehicle signal, the driver must take control, thus the autonomous operation is limited. In the near future, vehicles equipped with SAE Level 4 automated driving services will no longer require intervention from the driver's part. In addition to this, the SAE Level 5 will mean fully autonomous vehicles with automated driving services able to drive the vehicle in all situations and conditions, in Cooperative Intelligent Transport Systems.

This way, the range of information generated in the vehicle and made available using appropriate procedures expands further. Such information could be, for example, information generated by the perception of the environment and information related to the exchange of data between vehicles, vehicle-to-track, vehicle-to-environment communication. These data related to vehicle detection and communication are available, required and to be examined during a forensic test. The necessary expansion

[40] Salvation Data 2021.

[41] Bates 2019; Salvation Data 2021.

[42] Gomez Buquerin et al. 2021; Forensics Colleges 2022; Répás et al. 2022; Parkinson 2022.

[43] Interpol 2021; Répás et al. 2022; Interpol 2022.

of the content and methodology of the term automotive forensics, the possibilities provided by the information available in the study justify the definition of a new concept.[44]

Autonomous vehicle forensics

Modern and increasingly autonomous vehicles will not only store "general" vehicle status information, connected device information, navigation data, call logs, images and videos, they will also have a large amount of information about their environment, the environmental and track elements in their environment, the vehicles nearby, the pedestrians, i.e. Cooperative Intelligent Transport Systems and Services. Access to this information, data extraction, processing and analysis cannot be implemented using the standard procedures and methodology of digital forensics. The development and application of new approaches, tools, technologies and methodologies are required. The following step after computer forensics could be the autonomous vehicle forensics with large potential effect on specific types of investigations and prosecutions as a computer forensic science.

Autonomous vehicle forensics is a branch of digital forensics that focuses on identifying, acquiring, processing, analysing and reporting on data stored in autonomous vehicles and the Cooperative Intelligent Transport Systems.

Autonomous vehicle forensics will be able to reconstruct events whereby the vehicle is the target of the attack, and the vehicle is the one committing the crime, and the vehicle and/or Cooperative Intelligent Transport Systems contains the evidence.[45] Autonomous vehicle forensics uses and integrates certain areas of digital forensics and provides a methodological basis for digital vehicle forensics.

Since forensic scans are typically post-mortem scans, live forensics appears at a lower rate. However, depending on the cases and the organisations acting, it may be necessary to scan live data. The autonomous vehicle forensic methodology should also ensure that testing objectives meet the live data. Drone forensics is a new area in digital forensic science providing additional information in terms of remote control, data storage and transmission solutions. As the vehicles of the future will be computers and IoT devices, autonomous vehicle forensics will rely heavily on computer forensic and IoT forensic solutions. As networked vehicles are forming complex networks, increasingly with their own mobile Internet connection, both network and mobile forensic solutions are considered to be an essential part of autonomous vehicle forensics. Cloud and database forensics and their contexts also contribute to the expert examination of data generated, processed and transmitted by vehicles to ensure the reconstruction of events according to the test objectives.

[44] Berla 2022; Digitpol 2022a; Digital Forensics Corp 2022; Moore 2021.

[45] Répás et al. 2022.

Conclusions

In line with the above findings we can see that we are on the verge of developing an area of digital forensics requiring a new approach. With the development of sensor networks and modern vehicles, the transformation of vehicle architecture, and the forthcoming emergence of software-oriented vehicle development, autonomous vehicles will require a new approach from research experts, as well. The aim will continue to be to determine what, when, where, why, under what circumstances has occurred, by whom was it caused and who was affected. Ex-post investigation of accidents suffered or caused by modern and self-driving vehicles or the reconstruction of events in official, legal and criminal proceedings is necessary. New technology and increased data volumes, new data sources require new forensic solutions, approaches and processes.

In this study, after summarising the basics and purpose of forensic science, the tools and relevant areas of the purpose of digital forensics were defined. The entire process of digital forensics has been presented, which is valid and applicable in all areas depending on the studied area. However, some process steps may be combined.

The use of different procedures, tools and methods depends on the purpose of the study and the form and manner in which the evidence is available. Digital vehicle and automotive forensics need to evolve within the development of Cooperative Intelligent Transport Systems (C-ITS) and Services. The range of in-vehicle incident data has been significantly expanding, environmental and track information is also added to the described C-ITS. In our view, the content and methodology of the term automotive forensics need to be expanded. We have defined the definition of autonomous vehicle forensics:

Autonomous vehicle forensics is a branch of digital forensics that focuses on identifying, acquiring, processing, analysing and reporting data stored in autonomous vehicles and the Cooperative Intelligent Transport Systems.

References

Aafs (2022): *What Is Forensic Science?* Online: www.aafs.org/careers-forensic-science/what-forensic-science

Aboutbioscience (2022): *Forensic Science.* Online: www.aboutbioscience.org/topics/forensic-science/

Adelstein, Frank (2006): Live Forensics: Diagnosing Your System without Killing It First. *Communications of the ACM,* 49. Online: https://doi.org/10.1145/1113034.1113070

Al-dhaqm, Arafat – Razak, Shukor – Othman, Siti H. – Ngadi, Asri – Ahmed, Mohammed N. – Ali Mohammed, Abdulalem (2017): Development and Validation of a Database Forensic Metamodel (DBFM). *Plos,* 12(2). Online: https://doi.org/10.1371/journal.pone.0170793

Al-dhaqm, Arafat – Razak, Shukor – Othman, Siti – Ali, Abdulalem – Ghaleb, Fuad A. – Salleh Rosman, Arieff – Marni, Nurazmallail (2020): Database Forensic Investigation Process Models: A Review. *IEEE Access,* 8, 48477–48490. Online: https://doi.org/10.1109/ACCESS.2020.2976885

Årnes, André ed. (2017): *Digital Forensics.* Oslo: Wiley. Online: https://doi.org/10.1002/9781119262442

Bates, Eoin A. (2019): *Digital Vehicle Forensics.* Online: https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf

Bergholtz, Stine (2019): *The Six W's of Investigation.* Online: www.brainspores.com/the-six-ws-of-investigation/

Berla (2022): *Vehicle Forensics.* Online: https://berla.co/category/vehicle-forensics/

Beyers, Quintus H. (2013): *Database Forensics. Investigating Compromised Database Management Systems.* MSc dissertation. University of Pretoria.

Calvert, Roz (2017): *Types of Forensic Tests.* Online: https://sciencing.com/types-forensic-tests-7551951.html

Chandel, Raj (2020): *Digital Forensics: An Introduction.* Online: www.hackingarticles.in/digital-forensics-an-introduction/

Digital Forensics Corp (2022): *Automotive Forensics.* Online: www.digitalforensics.com/digital-forensics/automotive-forensics

Digitpol (2022a): *Automotive Forensics.* Online: https://digitpol.com/automotive-forensics/

Digitpol (2022b): *Drone Forensics.* Online: https://digitpol.com/drone-forensics/

EC-Council (2022): *What Is Digital Forensics?* Online: www.eccouncil.org/what-is-digital-forensics/

FBI (2000): *Computer Forensics.* Online: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm

FBI retired (2022): *FBI Computer Forensics.* Online: https://fbiretired.com/skillset/fbi-computer-forensics/

Flaglien, Anders O. (2017): The Digital Forensics Process. In Årnes, André (ed.): *Digital Forensics.* Oslo: Wiley. 13–49. Online: https://doi.org/10.1002/9781119262442.ch2

Forensic Focus (2020): *25 Days, 25 Questions: Part 1 – Process And Practice.* Online: www.forensicfocus.com/articles/25-days-25-questions-part-1-process-and-practice/

Forensics Colleges (2022): *Modern Forensic Science Technologies.* Online: www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies

Fowler, Kevvie (2008): *SQL Server Forensic Analysis.* Upper Saddle River, NJ: Addison-Wesley Professional.

Gehlot, Anita – Singh, Rajesh – Singh, Jaskaran – Sharma, Raj N. eds. (2022): *Digital Forensics and Internet of Things. Impact and Challenges.* Hoboken: Wiley. Online: https://doi.org/10.1002/9781119769057

Gillis, Alexander S. (2022): *What Is the Internet of Things (IoT)?* Online: www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

Gogolin, Greg (2021): *Digital Forensics Explained.* Boca Raton: CRC Press. Online: https://doi.org/10.1201/9781003049357

Gomez Buquerin, Kevin Klaus – Corbett, Christopher – Hof, Hans-Joachim (2021): A Generalized Approach to Automotive Forensics. *Forensic Science International: Digital Investigation,* 36. Online: https://doi.org/10.1016/j.fsidi.2021.301111

Hendricks, Beth (2022): *Mobile Forensics: Definition, Uses & Principles.* Online: https://study.com/academy/lesson/mobile-forensics-definition-uses-principles.html

Husain, Shahid M. – Khan, Zunnun M. eds. (2019): *Critical Concepts, Standards, and Techniques in Cyber Forensics.* IGI Global. Online: https://doi.org/10.4018/978-1-7998-1558-7

Hüschelrath, Kai – Schweitzer, Heike (2014): *Public and Private Enforcement of Competition Law in Europe.* Berlin: Springer-Verlag. Online: https://doi.org/10.1007/978-3-662-43975-3

Interpol (2021): *Guidelines to Digital Forensics. First Responders.* Online: www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwih9_7tqsr8Ah-VK_7sIHYtRC64QFnoECA0QAQ&url=https%3A%2F%2Fwww.interpol.int%2F-content%2Fdownload%2F16243%2Ffile%2FGuidelines%2520to%2520Digi-tal%2520Forensics%2520First%2520Responders_V7.pdf&usg=AOvVaw30M-zwH6f3XZN9NGPNGT8Ag

Interpol (2022): *Digital Forensics.* Online: www.interpol.int/How-we-work/Innovation/Digital-forensics

Joshi, Ramesh Ch. – Shubhakar Pilli, Emmanuel (2016): Cloud Forensics. In *Fundamentals of Network Forensics.* London: Springer. 187–202. Online: https://doi.org/10.1007/978-1-4471-7299-4_10

Karthika, Dhanaraj (2022): IoT Sensors: Security in Network Forensics. In Gehlot, Anita – Singh, Rajesh – Singh, Jaskaran – Sharma, Raj N. (eds.): *Digital Forensics and Internet of Things. Impact and Challenges.* Hoboken: Wiley. 111–129. Online: https://doi.org/10.1002/9781119769057.ch8

Kävrestad, Joakim (2020): *Fundamentals of Digital Forensics. Theory, Methods, and Real-Life Applications.* Cham: Springer. Online: https://doi.org/10.1007/978-3-030-38954-3

Khanafseh, Mohammed – Qatawneh, Mohammad – Almobaideen, Wesam (2019): A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics. *International Journal of Advanced Computer Science and Applications,* 10(8), 610–629. Online: https://doi.org/10.14569/IJACSA.2019.0100880

Kostadinov, Dimitar (2020): Network Forensics Overview. *Infosec,* 14 April 2020. Online: https://resources.infosecinstitute.com/topic/network-forensics-overview/

Krasznay, Csaba (2021): Az adatok évezrede. *YouTube,* 10 February 2021. Online: www.youtube.com/watch?v=-0FvULEkpqw

LDSZ (2021): *IoT és biztonságtechnika – 1. rész.* Online: www.ldsz.hu/iot-a-dolgok-internete-es-a-biztonsagtechnika-1-resz-68

Legalbeagle (2019): *Forensic Science.* Online: https://legalbeagle.com/6498833-im-portance-fingerprints-forensic-science.html

Liu, Changwei – Singhal, Anoop – Wijesekera, Duminda (2015): *A Logic-Based Network Forensics Model for Evidence Analysis.* Online: https://csrc.nist.gov/CSRC/media/Projects/Measuring-Security-Risk-in-Enterprise-Networks/documents/logic_based_network_forensices_model-for_evidence_analysis.pdf

Lyle, James R. – Guttman, Barbara – Butler, John M. – Sauerwein, Kelly – Reed, Christina – Lloyd, Corrine E. (2022): *Digital Investigation Techniques: A NIST Scientific Foundation Review.* Online: https://doi.org/10.6028/NIST.IR.8354-draft

Moore, Sarah (2021): *What is Digital Forensics.* Online: www.azolifesciences.com/article/What-is-Digital-Forensics.aspx

Munday, Oliver (2021): *The World of Data We're Creating on the Internet.* Online: www.good.is/infographics/the-world-of-data-we-re-creating-on-the-internet

NIST (2015): *Digital Forensics.* Online: https://csrc.nist.gov/glossary/term/digital_forensics

Parkinson, Matthew J. (2022): *The Evolution of Vehicle Forensics.* Online: https://sytech-consultants.com/the-evolution-of-vehicle-forensics/

QCC Global (2020): *Drone Forensics.* Online: www.qccglobal.com/drone-forensics/

Quadron (s. a.): *Mi az a digitális lábnyom és milyen veszélyeket rejt a közösségi médiában?* Online: www.quadron.hu/blog-9

Répás, József – Schmidt, Miklós – Vitai, Miklós – Berek, Lajos (2022): *Mit árul el rólunk az autónk? – Modern járművek IT szakértői vizsgálatának kérdései és lehetőségei* [What Does Our Car Tell about Us? – Questions and Possibilities of Digital Forensic Analysis of Modern Vehicles]. Pécs: Szentágothai János Szakkollégiumi Egyesület. Online: https://doi.org/10.15170/PTE-TTK-XX.SZJMKHV

Rouse, Margaret (2022): Digital Forensics. *Techopedia,* 24 August 2022. Online: www.techopedia.com/definition/27805/digital-forensics

Ruan, Keyun – Carthy, Joe – Kechadi, Tahar – Crosbie, Mark (2011): *Cloud Forensics: An Overview.* Online: https://doi.org/10.1007/978-3-642-24212-0_3

Ruan, Keyun – Carthy, Joe – Kechadi, Tahar – Baggili, Ibrahim (2013): *Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability: An Overview of Survey Results.* Online: https://doi.org/10.1016/j.diin.2013.02.004

Salvation Data (2021): *What is Digital Vehicle Forensics.* Online: www.salvationdata.com/knowledge/what-is-digital-vehicle-forensics/

SciTech Connect (2013): *Incident Response: Live Forensics and Investigations.* Online: https://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Incident-Response-Live-Forensics-and-Investigations.pdf

Siegel, Jay A. (2017): *Forensic Science.* Online: www.britannica.com/science/forensic-science#ref310214

Singh, Anuraag (2022): Drone Forensics: An Unrevealed Dome. *Data Forensics,* 19 April 2022. Online: www.dataforensics.org/drone-forensics/

Stander, Adrie – Barnard, Hanlé (2017): *Digital Forensics and Electronic Evidence.* Online: www.udemy.com/course/digital-forensics-and-electronic-evidence/

Stephens, Blaine (2016): What Is Digital Forensics. *Interworks,* 05 February 2016. Online: https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics/

Sule, Dauda (2014): *Importance of Forensic Readiness.* Online: www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness

Vízi, Linda (2019): *A Computer Forensics jogi vonzata.* Online: https://netacademia.hu/courses/take/computer-jog/multimedia/8481853-figyelem-ez-egy-classic-tanfolyam

Walsh, Joe (2021): *Introduction to Mobile Forensics.* Online: www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/IntroToMobileForensics.pdf

Williams, Lawrence (2022): *What is Digital Forensics.* Online: www.guru99.com/digital-forensics.html