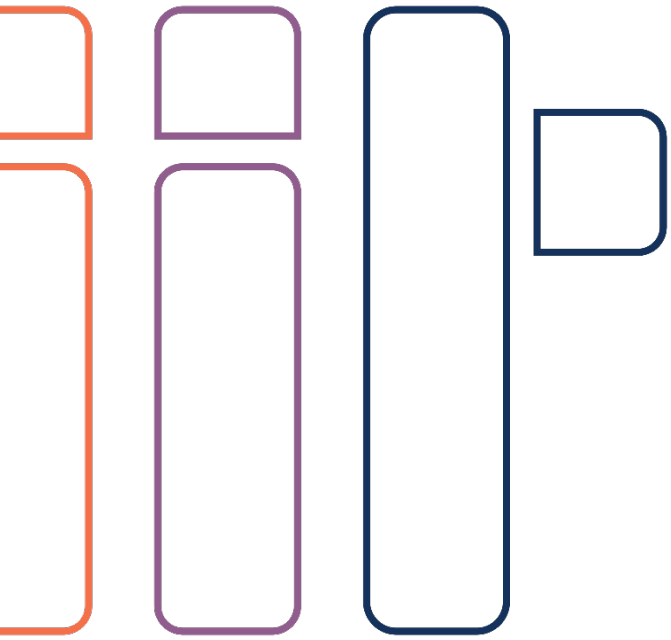

TECHNICAL REPORT

IIT TR-11/2021

Digital Vehicle Forensics: challenges and opportunities

A. Del Soldato

ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche

Index

1 Introduction

Modern vehicles are becoming an important source of evidence in digital forensic investigations, and forensic analysis of systems installed in vehicles, is an emerging area of research.

Connected and assisted-driving cars are becoming more common, and self-driving cars are becoming more widespread, along with supporting infrastructure such as smart cities. Vehicles are equipped with a large number of sensors that collect data about the vehicle itself and its immediate environment, as well as the behavior of the driver. These can be an important source of digital evidence in investigations where there is a need to clarify the dynamics of a road accident and the behavior of a vehicle and its crew before, during and after the accident, when the vehicle is involved in a crime scene or in a terrorist attack. Among the data that can be stored inside our cars are recent destinations and favorite places and some personal data such as call logs, contact lists, SMS messages, pictures, etc., as well as electronic control unit faults and, in some cases, events such as when and where the vehicle's lights came on and which doors are opened and closed at specific points. The forensic analysis of vehicles has assumed an important role in Italy, also following the introduction, of the law of 23 March 2016 n. 41, of the case of road homicide (Art. 589-bis[1]) under which the driver of motor vehicles is punished whose culpable conduct causes the fatal event, or personal injury with violation of the rules on road traffic (Art. 590-bis[2]). Digital forensics however has not yet been applied to vehicles in a regulated manner.

This paper was created to help the digital forensics community understand the application of digital forensics to major electronic systems in vehicles. The theory of this research can be used by investigators to gain a methodology for where and how to look for specific information in a vehicle-specific electronic module, when attempting to extract digital evidence so that it can be relevant to an investigation once it is collected and analyzed. The paper describes the main challenges associated with forensic investigation on vehicle data in the various main phases that characterize digital forensics, making reference to both traditional digital forensics tools and also some specialist equipment, that can be used to find the evidences from vehicles.

The rest of this document is organized as follows: Section 2 introduces the main concepts of digital forensics with particular reference to its main phases; Section 3 considers forensic analysis on

1 Vehicular homicide: “whoever causes by a negligent act the death of a person in violation of the rules of road traffic shall be punished with imprisonment from 2 to 7 years”.

2 Serious or very serious road injuries: “whoever culpably causes bodily injury to another with violation of the rules of road traffic shall be punished with imprisonment from three months to one year for serious injury and from one to three years for very serious injury” [17].

vehicles by highlighting the challenges to be faced in the different phases described in the previous section; subsequent sections look at digital forensic on the main sources of evidence on a vehicle such as Infotainment Systems, on-board Electronic Control Units (ECUs), Event Data Recorders (EDRs), black boxes, and eCAll unit.

2 Digital forensics and its main phases

The concept of digital forensics originated as a generalization of the concept of computer forensics at a time when the focus of forensic science shifted from the personal computers to the world of digital data more generally. As a unitary technical definition that can encompass both concepts, we can consider the one given by G. Ziccardi, who defines Computer Forensics as "*that science that studies the value that a piece of data related to a computer or telematics system can have in a social context, juridical, or legal, as it may be*" [24]. Meaning in this case as "value", from an exclusively technological point of view, the "*ability to resist any disputes and ability to convince the judge and the parties to the proceedings or other subjects regarding the genuineness, non-repudiation, imputability and integrity of the given itself and of the facts demonstrated by it*". Much like the older and more traditional field of forensics, digital forensics is about identifying, collecting, preserving, analyzing and presenting evidence. The difference between the two disciplines is the nature of the evidence being processed. Similarly, digital forensics, while originally intended for computer systems, is now applicable to any device or system that contains computing ability. This includes mobile phones, tablets, smart TVs, game consoles, cloud computing systems, smart vehicles, etc. In recent years, therefore, sub-disciplines of digital forensics have emerged, such as Mobile Forensics, Cloud Forensics, Vehicle Forensics, etc. in order to provide specialized investigators for the different types of devices following different approaches. In all these disciplines, however, the fundamental principles of digital forensics must be respected such as the relevance of digital evidence for the investigation, its sufficiency to allow a correct investigation, the verifiability of the actions carried out and the justifiability of the methods used to manage the potential tests, as well as the repeatability or reproducibility of the test results[3]. The diagram in Figure 1 shows the various phases, followed by a brief analysis of each of them in order to better understand the actions and problems to be addressed in the context of vehicle forensics.

[3] Art. 359 and Art. 360 of the c.p.p.

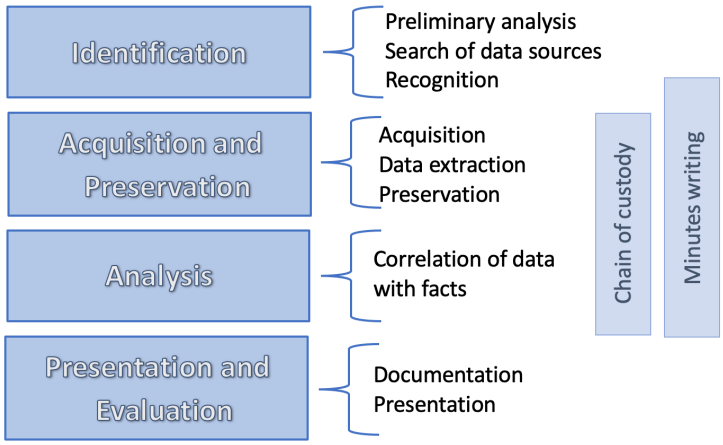

Figure 1 - The 4 main steps of digital forensics

2.1 Identification

The *identification* phase is the first stage of the entire digital evidence life cycle and is made up of the *preliminary analysis* phase, in which the investigator tries to obtain the basic information to understand the extent of the incident, and the *evidence source search and recognition* phase, in which the areas affected by the fraud are examined and an attempt is made to understand where the evidence might be located. This may seem to be the simplest phase, because it is "only" a matter of identifying and cataloguing the potential "container" of the information sought (source of evidence), but this is not the case, given the enormous amount of tools capable of storing data that we normally have at our disposal.

To recognize evidence it is necessary, first of all, to know where to look, then to know the architecture of the apparatuses (also in relation to their typology), which usually consist of different elements that contribute to the functioning of the system and can contain information useful for the reconstruction of the dynamics of an offence. These include:

- The type of *computer system* (laptop, desktop, smartphone, GPS, infotainment system, etc.) defines the main use of the device and therefore the approach for acquiring the data;
- *Operating System* typology identifies memory areas of interest that may contain evidence, and determines subsequent steps;
- The type of *file system* specifies how the data is organized within the memory supports, therefore allowing access and interpretation of the data, and often recovery in cases of inaccurate deletion;
- *The type of file* which allows to recognize which ones can be useful for the investigation and which ones are not;

- The *presence of interfaces* and their typology which allow to identify the possible interconnection between the analyzed system and the various external or removable storage devices and the network.

2.2 Acquisition and preservation

After identifying the evidence source, data acquisition follows. Data acquisition is a very delicate phase of digital forensics with regard to repeatability/unrepeatability of activities. At this stage, all material deemed necessary for the investigation is acquired: hardware, forensic copy of the data, data extraction from a network, etc... It is therefore of particular importance to recall what is stated in one of the guidelines for digital evidence collection RFC 3227 [23], which provide the universally recognized and applicable guidelines and technical procedures for dealing with digital evidence, regardless of the regulatory environment of the individual nation, and allow digital evidence to have evidentiary value.

This stage also depends on the type of computer system and its state, on or off, so the investigator will perform a *Live* or *Post-mortem analysis*. Live analysis requires care as it can lead to alteration of the system, and consequently, possible destruction of significant data. It is important, therefore, that the analyst knows the possible alterations and that these can be documented. It is clear that live analyses will not be repeatable. Post-mortem analysis requires that the analyst secure the crime scene, document in detail all operations performed, and make a low-level copy of the original data medium through the use of specific software tools such as for example DD (Data Duplicator), EnCase (commercial), SafeBack (commercial), DEFT and CAINE or the use of HDD Duplicators and/or Write Blocker devices. This is necessary to preserve the original data and ensure its authenticity and integrity.

The acquired source of evidence must then be kept intact for the duration of the investigation, then secured and stored for the next phase of analysis. Captured data are stored on secure media, sealed appropriately and stored in locations accessible only to authorized personnel. Destruction of digital evidence may, in fact, change the assessment at trial.

2.3 Analysis

In the analysis phase, data are analysed in order to prove or disprove the truth of an allegation or evidence for a defence. At this stage, a timeline of device usage is usually constructed so that possible operations performed over time by the suspect can be documented. The forensic analyser uses analysis software that can be either proprietary or open-source, which, if sufficient, is preferable to the former. In order to certify the operations performed at this stage, it is preferable for the analyst to

use tools accepted by the scientific community. In this regard, the NIST (National Institute of Standards and Technology), for years, has been carrying out the testing and validation of computer forensics software and hardware tool[4].

2.4 Presentation and evaluation

The presentation and evaluation stage involves the preparation of a forensic report in which all the information must be gathered that will enable the investigator to answer the questions posed by the trial bodies, prove the hypotheses, and evaluate the results. The forensic report is used in the trial by the forensic expert who, throughout the trial, testifies in court and must provide evidence to the court, as well as withstand opposition from the opponent both during direct questioning, in which evidence is provided to prove the case, and during cross-examination, which is conducted by the opposition. At this stage, the validity of the testimony is evaluated: evidence is presented to the judge or employer, depending on who commissioned the investigation, and evaluated in order to determine the outcome of the investigation.

The ***Recognition***, ***Acquisition*** *and* ***Preservation*** phases are accompanied by a ***Crystallization*** phase of the evidence, which is the most delicate management process of digital forensics as regards the concept of Reproducibility. This activity is aimed at freezing the contents in the system in order to attribute to them, as much as possible, the characteristics of integrity required by international standards. It is carried out through forensic copying of the data and correct conservation of the evidence. During the *Acquisition, Preservation and Analysis* phases, the so-called ***Chain of Custody*** and a ***Reporting*** must also be implemented. It is necessary for the correct attribution of responsibilities throughout the life cycle of the evidence source and to ensure its *verifiability*. The chain of custody certifies the originality, integrity and manner in which the source of evidence has been treated. All changes of hand of evidence must be traced and there must be a person responsible for the entire life cycle. Furthermore, all the activities carried out during the acquisition and analysis, systematically, must be reported in a report, followed by the motivation of the activities carried out and photos identifying the key information. The minutes also contain the time references of the activities (date and time), with any deviation from the time reported on the systems, and the reference to all the people who attended.
The following section looks at vehicle forensics by highlighting the challenges faced in the different stages of digital forensics described above.

[4] Computer Forensics Tool Testing Program: https://www.cftt.nist.gov

3 What is digital vehicles forensics

Digital vehicle forensics primarily involves the acquisition and analysis of digital data (digital evidence) from motor vehicles. The current state of vehicles forensics is quite new considering how the field of digital forensics is fresh as a whole compared to the already established traditional forensic methodologies, which have been around for much longer.

Vehicles can be viewed as a typical computer system with several electronic modules connected to and controlled by different computing devices that generate process, transmit, and store digital data in various formats. From the perspective of forensic and criminalistics disciplines, therefore, every modern vehicle creates a large amount of digital evidence. In fact, nowadays, each connected car contains about 100 ECUs, 150 million lines of code handling them, and 25 GB of data for every hour the vehicle is in operation [14]. By 2030, many observers expect them to have roughly 300 million lines of software code. To put that into perspective, a passenger aircraft has an estimated 15 million lines of code, a modern fighter jet about 25 million, [22]. A vehicle can thus be seen as a computer with wheels, the on-board data are stored in different devices, in different data formats, and are generally not internationally standardized. Similarly, and consequently, some tools for analysing this data for forensic purposes within the European Union are not standardized [21].

This draws attention to two main problems that need to be addressed during forensic analysis: the heterogeneity of data, which necessitates the modelling of the data so that they can be valid from a forensic point of view; and the adherence to the principle of relevance in identifying, collecting, analysing, and preserving only those data that are essential for digital forensics, in the enormous amount of data available. Moreover, in this ecosystem, maintaining and respecting the chain of custody is another major challenge to be faced since most nodes do not store any metadata, particularly temporal information.

Also from the point of view of the data contained in auto components, these are often produced abroad, and therefore, in the event that there is a need to have support from the manufacturers, there would be this kind of problem. Finally, very often, manufacturers are unwilling to provide open access to the data collected in their vehicles (e.g., because of intellectual property or competition issues), which introduces a major concern regarding the collection, analysis, and preservation of forensically sound evidence. In the future, we can expect increasingly autonomous vehicles, supported by communication systems with all objects involved in driving and with the vehicle and road logistics, including elements of artificial intelligence. Vehicles will use their "experience," learn and exchange information with other vehicles (v2v - Vehicle to Vehicle), traffic infrastructure such as intelligent traffic lights (v2i - Vehicle to Infrastructure), parking lots, etc., creating what could be

called the Internet of Vehicle (IoV). At that point, it will be entirely possible and essential to use this information heavily for forensic work as well.

This data has become an increasingly valuable source of digital evidence. The ability to access this data may vary depending on who is looking for the data and the purpose for which we are looking for it. An insurance company may share this information with its internal investigators. In other cases, the data may be made available to law enforcement through appropriate court approvals and production order requests to telecommunications, automakers, insurance companies, or other third parties. Unlike traditional digital forensics, the challenges for investigators in vehicle forensics include:

1. Where and what information each module stores?
2. What software tool(s) can be used to forensically acquire the data of interest, without affecting its integrity?
3. What software tool(s) can be used to interpret the acquired data correctly?

The complexity and variety of systems in vehicles exacerbate the above challenges. For example, to investigate a modern vehicle, investigators may also need to understand the operation of 20 or more electronic modules, their configurations and their interactions. The main questions to focus on should be:

1. What are the types of electronic components and devices of interest, both embedded and stand-alone devices (e.g., radio navigation system, such as RNS-XXX devices) and how can they be forensically recovered?
2. What types of personal information (e.g., call history and social media data) are stored in vehicles, how are they stored?
3. What is the supporting infrastructure in the sense that there are additional sources of evidence (e.g. smart traffic lights and CCTV in a smart city/country)? How do vehicles interact with the supporting infrastructure, what types of data are stored, where is this data stored and how can it be retrieved?

Once we have identified potential sources of evidence, we will need to determine how to forensically recover the data. For example, can we reliably retrieve the data using the vehicle's gateway via the OBDII connector, or do we need to remove the electronic module from the vehicle? In the latter scenario, forensic investigators are likely to need to work with individuals with the right skills (e.g. vehicle technicians) to remove the module, without damaging it and/or corrupting the data. At this point questions such as:

1. What are the implications of power loss for data stored on the device?
2. Is the data stored on RAM, flash, EPROM (erasable programmable read-only memory), other volatile data, removable storage devices (e.g., USB), etc.?

Similar to cloud forensics a few years ago [3] there is a lack of guidelines and frameworks related to the digital investigation of a vehicle. Therefore, urgent challenges for vehicle system forensic analysis also include determining a viable forensic approach to conducting digital investigation of a vehicle and identifying tools that can be used to retrieve forensic evidence from the vehicle and the various modules (or components) and possibly from the supporting infrastructure and various components (e.g., nodes or "things" in the smart city/nation architecture).

3.1 Identifying the Source of Evidence

As regards the identification of sources of evidence, it is necessary identify the types of electronic components and devices of interest, both incorporated in the vehicle and autonomous. Among them may be sources of evidence:

- Control units related to **infotainment systems**.
- Control units with **Event Data Recorder** (EDR) functionality, which are the most widely used source of digital data (evidence) during forensic road accident investigations;
- The Data that come from the **black boxes** that insurance companies mount;
- The eCall Units for calling emergency services.

Once the components have been identified, it is necessary to know what information each component stores and where, as well as what types of personal information is stored in the vehicle and how it is stored (Ex: call histories and social media data). In a more complex system, it is necessary to understand if there is a supporting infrastructure, to be used as an additional source of evidence that forensic investigators can rely on, such as smart traffic lights and video surveillance system in a smart city or nation. Next, understand how vehicles interact with the supporting infrastructure, what types of data are stored, where they are stored, and, finally, how they can be retrieved.

3.2 Data Acquisition

Once potential sources of evidence have been identified, we need to determine how to forensically acquire the data.

It is possible to reliably acquire the data using special tools connected to gateways in the vehicle via an On Board Diagnostic (OBD) connector or USB port. In this scenario, it is likely that forensic

investigators must work with people with the right expertise (such as vehicle technicians) to avoid misinterpretation or loss of data.

In the absence of the right equipment, it is possible to try to recover the data by removing the module from the vehicle, trying not to damage the module and/or alter the data itself. In this case, the investigator needs to know what the implications of a loss of power are on the data stored on the device when the connectors are removed from the battery. It would be helpful to know the types of memory on which the data are stored (RAM, flash, EPROM) and whether there are other volatile data. In this context, before leaving the vehicle, the investigator must ensure that there are also no removable storage devices (e.g., USB) or external connections to other devices or infrastructures. This methodology leads to issues with regard to proper management of evidence, particularly with regard to maintaining the chain of custody. In addition, IT systems often have active external connections (cell phones, wi-fi, Bluetooth) so in order to prevent data loss or modification it is necessary, if possible, to isolate the vehicle from connections to external networks (e.g., disconnect antennas and modems, remove SIM cards, etc.). With the removal of the system, data acquisition will take place in the laboratory. The lab should be equipped with a power generator, a vehicle network simulator, to replicate the network traffic and make the system work, and various appropriate cables and connectors.

If the types of acquisitions defined above are not possible, other types of acquisitions are used that are extreme and invasive and which are usually carried out only if there is a need.

One way is to use **JTAG**, a standard for design verification and testing of printed circuit boards that is basically used by the investigator to read data from a memory. However, some manufacturers may take countermeasures to make it difficult to use the JTAG interface in the final product, adopting countermeasures such as obfuscation (cutting rails, removing resistors, etc.), reconfiguring JTAG pins in software, or encrypting and validating the firmware image signature. Other manufacturers go further and completely disable the JTAG interface via certain fuses: internal bits of the chip that, once programmed, can no longer be changed.

The most invasive method is **chip off**, which involves identifying the memory chip on the motherboard (which is sometimes hidden or protected by resin or metal) and removing it from the motherboard itself unsoldering it with a heat gun (250° to 300°). After that, the contents of the chip are read with a socket reader and a bit-by-bit copy is made. The success of this procedure is also related to the forensic analysers' experience in dosing the right temperature, which must be high enough to unsolder the chip but not too high to introduce bit errors that may prevent the data from being read correctly. In addition, once the memory chip is removed, the examiners must clean it thoroughly and replace any solder balls damaged or removed during the removal process. During this

process, the memory chip is reheated, increasing the likelihood of reintroducing bit errors into the flash memory. In addition, the presence of epoxy on memory chips often requires both increased exposure to heat during the removal process and the subsequent application of strong chemical epoxy solvents to remove it so that the flash memory chip will fit the adapter properly. Finally, if chemical removal is not completely successful, examiners must physically scrape the remaining epoxy resin from the chip further risking damage to the flash memory chip and affecting the ability to successfully read the chip [12].

Unlike JTAG, chip-off is a destructive process and the device will no longer be usable. It may require a process called MicroRed, which involves the use of powerful microscopes to obtain a physical view of the memory cells.

3.2.1 JTAG standard

JTAG is a standard used as a tool for programming and debugging the device in production. As printed circuit boards (PCBs) became more complex, it began to become difficult and complicated to design a bed of nails to perform testing. For this very purpose, in 1985, the Joint Test Action Group (JTAG) interface was created, a standard (IEEE 1149.1) for testing printed circuit boards during production. Over time, JTAG has become one of the most popular interfaces for testing electronic circuits, gaining other capabilities such as debugging and burning flash devices.

Currently, this interface is available in most processors and microcontrollers of different architectures such as ARM, x86, MIPS and PowerPC.

These are the four main steps to extract firmware from a device using JTAG:

1. Identify the JTAG connection pins;
2. Test the connection with a JTAG adapter;
3. Gather information on the memory mapping of the chip;
4. Extract the firmware from the flash memory.

Next we need a j-tag adapter and communication software. The adapter connects the device with the JTAG interface, which in turn is usually connected to the PC via a USB. The communication software communicates with the JTAG through the adapter.

Through a text console and with special commands, the investigator identifies what the memory space is by identifying the starting address of the flash memory and its size. Then through the interface it reads the identified memory space and downloads it to a file. The file is finally analysed in order to analyse the firmware and extract the file system (for example with binwalk[5]).

[5] https://github.com/ReFirmLabs/binwalk

3.2.1.1 Functioning

Although there are some variations of the standard, the JTAG interface is usually implemented by the chip manufacturer via four mandatory pins (TDI, TDO, TCK, TMS) and one optional pin (TRST):

- *TDI* (Test Data In): data input.
- *TDO* (Test Data Out): data output.
- *TCK* (Test Clock): clock whose maximum frequency depends on the chip (usually from 10MHz to 100MHz).
- *TMS* (Test Mode Select): pin to control the JTAG state machine.
- *TRST* (Test Reset): optional pin to reset the JTAG state machine

The pins of the JTAG interface are connected internally to the chip via a module called TAP (Test Access Port). The TAP interface implements a finite state machine (16 states) that provides access to a group of registers (IR, DR). Through this state machine, it is possible to select an operation via the IR (Instruction Register) register and pass parameters or check the result via the DR (Data Register) register. Basically, with the JTAG interface it is possible to:

- Identify hardware information (processor, memory, etc.);
- Download RAM and gain access to sensitive data such as passwords and cryptographic keys;
- Change the behaviour of programs at runtime to gain privileged access to the system;
- Acquire sensitive data from hardware devices, such as information stored in an EEPROM;
- Activate peripherals and change their behaviour, such as setting or resetting an I/O pin;
- And, of course, download flash memory to extract device firmware;

As we can see, the JTAG interface is perfect for inspecting firmware execution, finding vulnerabilities, and exploiting the device.

3.3 Challenges

Once the acquisition methodology has been established, the investigator needs to figure out what tools can be used to forensically acquire evidence from the various components without affecting their integrity and from the supporting infrastructure, such as the nodes or "things" that make up the architecture of the smart city or nation.

In the event that the investigator does not have the right tools at his or her disposal, he or she may still have difficulty obtaining proprietary information from the various manufacturers of the vehicle

components. Sometimes it may also be impossible because a vehicle is generally assembled using parts from many suppliers and located in different countries. Another problem may be intellectual property. Reputational and legal risks for sharing information are also to be considered. By sharing information about the inner workings of the modules, in fact, researchers may find that the modules can be exploited to track individual drivers or discover previously unknown vulnerabilities that could be used to compromise vehicle safety. All of this could result in serious financial, legal, and reputational implications for manufacturers.

At a legislative level, the European Community is working on this issue also because car manufacturers want to protect themselves and want to be able to demonstrate that any road accidents are not caused by vehicle malfunctions. The idea is to force manufacturers to install devices that record the vehicle's operating parameters. In America the EDR (Event Data Recorder) functionality is mandatory on the ECUs while in Europe we are still working on it, especially as regards self-driving cars.

Should the investigator opt for the more intrusive solutions, however, he or she would have to deal with the cybersecurity solutions that manufacturers are installing on vehicle components. These include the use of a centralized gateway that divides the trusted part (body: air conditioner, doors, transmission, suspension) from the untrusted part (infotainment, telematics) with protection policies for the trusted part, such as through the use of encryption features that provide protection from attacks. On the control units, specific hardware has also been adopted to enable secure on-board and off-board communications, among them: access via JTAG with access to debugging features via passwords; introduction of security systems on the network to ensure authenticity and integrity of data passing over the CAN; strengthening the security of networks communicating with mobiles using protocols such as TLS; introduction of systems to authenticate the software running on the ECUs during update (compare with hash received during update); access to diagnostics from authorized tools via servers, etc.

Continued research needs to continue by both law enforcement and digital forensic communities to come up with viable solutions to defeat the new security features introduced by manufactures.

Moreover, collaborative efforts between private and government agencies must continue into the future to ensure continued access to legally authorized data obtained from the legal system so that data privacy and related regulations are complied with.

3.4 Best practices

Forensic Investigators must be aware that the digital systems contained in a vehicle are like any other digital device or system and therefore must be managed appropriately to prevent data destruction.
Modern vehicles contain multiple electronic components and/or networks and therefore, especially during the collection and processing phase, the investigator should take appropriate measures at least to isolate the vehicle from wireless networks [10]. This is to avoid any loss or modification of data.
Whenever possible, the car should be kept in an area with little or no GPS signal reception in order to avoid changes to the last known location and other related information (e.g., GPS fix). Better would be a garage that serves as a faraday cage. Unlike typical mobile device forensic investigations, however, it is unlikely that most law enforcement agencies have a faraday cage (i.e., designed to block any static electrical signal) large enough to contain a forensic case vehicle. Therefore, in this case study, an underground garage can be used as a Faraday cage. In any case, the investigator should locate any nearby devices or vehicles with Bluetooth enabled and record their MAC addresses including the investigative team's devices.
Also, whenever possible, it would be wise not to start the car since some cars overwrite or change data with each turn of the ignition key. If the car is to be started, any potential data changes should be documented and explained.
There is something to keep in mind, however, that electronic control units (ECUs) constantly draw power from a vehicle's battery, even when the ignition switch is in the off position. Many ECUs, such as infotainment and telematics systems, use key events such as unlocking or opening/closing doors as signals to enter low-power mode or initiate the ignition procedure. Thus, minimizing the number and duration of power cycles helps preserve volatile data stored on ECUs.
Finally, the investigator should ensure that the navigation unit does not start to avoid changes to information (e.g., last known location). If necessary, he or she might consider using a signal jammer to avoid interference with other signals, being careful to follow relevant legislation to ensure admissibility of evidence[6].
To avoid the loss of volatile data contained in the ECUs as much as possible, the investigator should document the data on the infotainment system screen, document the date and time, and properly shut down the vehicle to allow the ECUs to shut down properly. In order to turn off properly the vehicle to preserve evidence, the following steps should be performed [10]:

[6] The jamming device is a frequency jammer. Jammers are devices little larger than a cell phone whose GPS jamming radius can be up to tens of meters away. The use of a signal jammer is regulated by law in some countries, therefore, it is important that forensic investigators follow the relevant legislation to ensure the admissibility of evidence.

- Turn off the vehicle remove the key and exit;
- Close all doors;
- Open the driver's door for 5 seconds;
- Close the driver's door and wait about 2 minutes;
- Disconnect the vehicle's power supply, such as disconnecting the battery;

To verify that the vehicle has been completely turned off, make sure that the vehicle's centre light, as well as the instrument cluster, and interior/exterior lights are turned off for 30-45 seconds after all doors have been closed. After all components have turned off, wait 60 seconds before removing power to any of the ECUs.

In addition, before running the tests, consider the current legal authority to avoid violating any regulations or note any restrictions. If necessary, also request additional authorizations essential for data access.

Finally, if physical forensic investigations of the vehicle, such as fingerprinting or DNA, are required, it is imperative to discuss the order in which the investigations are conducted with the investigator and crime lab personnel to avoid inadvertent destruction of physical and digital forensic evidence.

The following sections contain a brief overview of the possible data acquisition methodologies on the sources of evidence that we listed in section 2.1 as well as the forensic analysis of the evidence itself. The various issues to be addressed in different cases will also be considered.

4 Forensic Analysis of Infotainment Systems

Infotainment systems are defined as all those systems in motor vehicles that serve to provide information and entertainment to the driver and the inhabitants in the vehicle.

The term infotainment is a neologism of Anglo-Saxon origin; the word is derived from the fusion of two pre-existing terms: information and entertainment, which mean information and entertainment, respectively. In the automotive field, infotainment is used to refer to the complex of in-vehicle technological equipment (software and hardware) capable of combining entertainment and information functions.

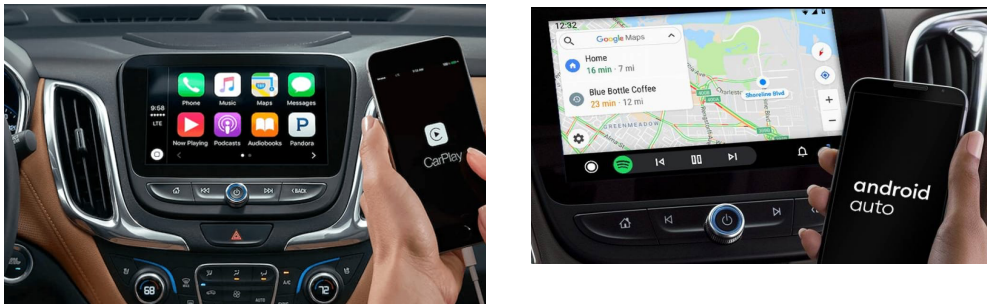

Figura 2 - Infotainment systems

The goal is to provide occupants with the simplest and most intuitive information environment closely related to the car's location and enable them to control both information and entertainment systems (radio transmissions), communicate with the environment (cell phone control), and orient themselves in space (navigation systems). Today infotainment systems can be controlled by touch screens, steering wheel controls, or 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 geographic movement of a vehicle (routes taken, favourite routes, frequently visited destinations, etc.) and the telecommunication activities of vehicle occupants (phone calls, text messages, Internet activity, social network activity, and so on). The combination and correlation of these activities, in time and places of implementation, gives additional insight into the course and consequences of certain events.

Infotainment systems are increasingly widespread and comprehensive, especially on newer models, and embrace an ever-widening range of features and applications on which automakers are pushing in order to differentiate them from car to car.

4.1 Identification of evidence

Among the information that the investigator may find interesting in the context of forensic analysis in infotainment systems are:

- Vehicle and system information:
    - Serial Number (VIN[7]), Part Number[8]. This information links an infotainment system to a specific vehicle and is useful for confirming the VIN of the vehicle or to find out if the infotainment system was sold as a stand-alone unit (extracted from the original vehicle).
- Data relating to installed applications:
    - Meteo, Traffic, Social

  This information can facilitates analysis in that it can give an investigator an idea of what to expect and look for when analysing information extracted from the system.

- The lists of the currently and previously connected devices:
    - Phones and media players, USB and SD cards, Wireless access points.

  This usually displays the name of the device but this holds relevance as it helps corroborate evidence (for e.g. suspect or victim's name as the name of the device) by linking said device to a potential owner.

- Data related to navigation:
    - Active and inactive routes, saved locations, previous destinations.

  This information shows "favorite" GPS information and exact coordinates of specific locations such as "home," "work," or custom saved locations. This data can be particularly useful in identifying the vehicle owner and places he or she may regularly frequent, placing the person of interest in specific locations in case he or she denies ever having been there.

- Cell phone data:
    - Device ID, SMS and calls, address book, audio and video recordings.

  This data can show that potentially interesting people have connected with this device and can help refute any claims that the owner does not know a person who is associated with this data.

[7] VIN (Vehicle Identification Number) known to everyone as the chassis number. It is the identity card of any car. A code consisting of 17 characters, including letters and numbers, that distinguishes that car from any other.

[8] Part number is used to classify and catalog an object. It identifies the company, manufacturer or outside supplier.

The call list can also show that two people have come into contact at a certain instant of time and in any case certify the activity of a user and help to corroborate the identity of the vehicle's owner.

- Vehicle-related events:
    - Odometer reader, gear indication, door open/close, lights on/off, Bluetooth, WI-FI and USB connections, GPS time synchronization. This information can help investigators in further assessing and corroborating the overall vehicle trip and thus the possible movements of the suspect.

Even for these systems, as for the traditional systems covered during forensic analysis, if we want to identify and take data from them, it is necessary to know the Operating System and consequently the File System. The main Operating Systems contained in infotainment systems are [25]:

- *BlackBerry QNX* [7] - found on vehicles of the automakers BMW, Ford, Acura, VW, and Audi. The file system supported is QNX4 and 6. Originally, QNX provided a usable user license for non-commercial developments (QNX NC), but this was discontinued in 2003 and now provides only the ability to download the complete system with a temporary 30-day license.
- *Automotive Grate Linux* [6] - present in vehicles from automakers Volkswagen, Jaguar Land Rover, Nissan, Toyota Honda, Mercedes, and Tesla. With Linux at its core, AGL is developing from the ground up an open platform that can serve as a de facto industry standard to enable the rapid development of new features and technologies.
- *Windows embedded* [WINEMBEDDED] – present on Ford, Fiat, Nissan and Kia vehicles that support the FAT, FAT32, User Defined File System (UDFS).

Then there is *Apple CarPlay* [4] and *Android Auto* [2], which are not operating systems, but are systems that allow the infotainment to talk to smartphones, making all of their cell phone apps available on the car's touch screen or through voice commands. These systems were created with the aim of zeroing out or otherwise minimizing any kind of potentially very dangerous distraction while driving.

Google then introduced Android Automotive, a version of Android that will run on infotainment systems. With this system it will be like having another phone: a user will be able to customize (by logging in with a Google account) the interface with favourite screens and download apps and make automatic updates if they have a built-in Internet connection. The substantial difference, even from a forensic point of view, between Android Automotive and Android Auto is that the dedicated

integrated version (Automotive) can control vehicle functions such as air conditioning, heating, heated seats, and audio functions. Also, with the Google Assistant, you can control most vehicle functions using only your voice, which is super neat because you never have to take your eyes off the road. In addition, Android Automotive is open source, so manufacturers can customize it to their liking with all that goes with it.

4.2 Data Acquisition

To understand the various systems from a digital forensics perspective, it is first necessary to gain an understanding of the underlying technology. This is done in order to initially understand what types of memory storage are being used and consequently have an idea of the possible methods of acquisition.

Each infotainment unit should be photographed as an entire device, before being deconstructed at the PCB (Printed Circuit Board) level. During the entire acquisition process, it is also good practice to note down the various steps performed in order to comply with best practices and to be able to create the chain of custody.

As with traditional systems, acquisition methodologies on infotainment systems vary depending on the analysis systems the expert has at his disposal (see previous sections) and the level of analysis required by the investigation. The investigator should always opt for the least destructive ones first and comply with best practices, but the choice of methodology also depends on the time available. Data may be acquired directly in the vehicle or on the bench.

4.2.1 Manual Approach

A simple examination approach consists of leaving the unit in the car and manually going through the different menus. This allows the investigator to view and document, including by taking a picture of each screen, the data in the device's memory. Using this approach allows time and date settings to be obtained from the display.

A visual analysis of the physical interface of the system, however, can give us a trace of the systems within the device and consequently the type of digital evidence to look for. A 'Nav' and 'Map' button could confirm that this is indeed a satellite navigation system and, as users are often able to save locations, input new destinations for a journey and save contacts, underlying data from this could become an artefact. Likewise, the presence of the Bluetooth symbol could confirm that some level of interaction with mobile phones is possible and that related data could be used.

Scrolling through the interface, however, it is possible to learn information that could be useful for the investigation, such as:

- The names of the devices that are or have been connected to the device, useful in case a device name is found to match the name of a suspect or victim;
- The list of contacts that might contain people involved in the investigation;
- The call list, to show that the suspect had contact with the victim or otherwise showing the activity of the driver or owner of the vehicle (including the timestamp);
- The GPS information, which can give the geographical coordinates of locations washed out by the user and the system such as 'home' and 'work';
- The version and type of the infotainment system from which the system's specifications can be inferred and the possible compatibility with forensic tools.

There is, however, a limitation with such an approach: the GPS module is attached to the device and turning on the device will cause the last GPS fix to be overwritten with its current position. Therefore, crucial data will be lost.

4.2.2 Using instruments connected to the OBD or USB port

Another approach is to exploit the vehicle's OBD II port or the USB port connected to the infotainment system and download the data using ad hoc tools that, connected with cables to these ports are able to read the data and present them in the form of reports. The most used tool at the moment by digital investigators for this purpose is iVe, created by Berla Corporation which is a software-hardware tool designed for the acquisition and decoding of evidence from infotainment and telematics systems [20]. This is one of the biggest challenges as the capture process requires a custom third party hardware and software solution and iVe only works for very specific vehicle makes and models. This tool extracts information from infotainment systems and presents it in a report structure, similar to mobile forensic tools. iVe is able to extract vehicle information such as serial numbers, part numbers and VINs as well as user related data such as navigation data, information from car kits and user events such as open doors, Wi-Fi connections and Bluetooth, points of interest, track logs and previous destinations, as well as installed applications, Wi-Fi connections and telephone data such as calls. The problem is that the extraction and parsing method are proprietary and it is not clear what file system it supports. Berla iVe had limited support for the extraction process. Only the file system extraction can be performed. One problem with extracting data with this tool is that the extraction method and analysis are proprietary and therefore it is not clear how the information is extracted and what file types are supported. iVe currently supports a limited number of car brands [20]. Furthermore, it is not capable of performing a complete extraction and decoding of VxWorks and QNX type file systems [25]. There is a possibility that the investigator may be in a situation where the USB connections are not working as they are only enabled for mass storage mode: debugging is

disabled and re-enabling cannot be done unless source code/reverse-engineer access is completed. Especially aftermarket system required creative solutions versus supported forensic acquisition tools provided for OEM systems. There are methods that have been tested to enable debug mode on USB or other interfaces. This allows for data mining on systems that initially have debugging functionality disabled. For example, sometimes, ADB (Android Debug Bridge) can be enabled by accessing developer mode through the systems menu on the device. However, it could happen that device did not have developer options enabled and ADB could not be turned on for USB ports. It has been discovered that, Android-powered infotainment systems, root access can be achieved through the infotainment system's factory settings, after entering a special command. As root, the investigator can enable debug mode, accessing root directories of the device, which gives access to the entire system, as well as running the "dd" utility for data extraction. For other systems, it was discovered that during the boot process of the device, any inserted USB stick, could trigger the system to boot in a "testmode". This mode enabled debugging by default and the ability to run system scripts but specific file was needed on the USB device. The extracted data could be viewed using open source forensic tool as Autopsy[9]. Some systems are still not forensically accessible due to malformed files and in unspecified formats or because some files are not allowed, by the Operating System, to be copied out of the system. More standardized capture methods should be developed to attempt to capture as much data as possible, although built-in features may prevent certain personally identifiable information from being stored on infotainment devices [28].

4.2.3 Physical removal of the module from the vehicle

The third approach is the more invasive physical one, which consists in acquiring data by physically removing the infotainment module to gain access the circuit boards. For this type of operation, the investigator will need not only the appropriate software equipment (both traditional tools used and specialized tools) but also common equipment such as a set of screwdrivers, including the "T-head screwdriver", usually used in mobile device investigations, and a unsoldering tool in case the chip-off technique is used, also derived from mobile forensics [13].

Once the module is extracted, different types of ports such as mini USB may be present on the PCB and by looking at the connection points on the PCB itself, it is possible to recognise the JTAG or similar connectivity points used for testing by the manufacturer. In this case, the investigator can plug in a card, provided by the manufacturer of the extraction software, and proceed to download the data. This could be an alternative and non-destructive route for data extraction.

[9] Autopsy is an end-to-end open source digital forensics platform that allows efficient hard drive investigation solution (https://www.autopsy.com/).

Infotainment systems have various configurations, e.g. some use traditional hard disks and others use flash-based storage devices. For example, it might be good news for the investigator to find an eMMC (electronic Multimedia Card) chip on the PCB. The eMMC is a non-volatile memory system used as a storage component by most devices such as smartphones and mobile devices dedicated to Internet browsing and therefore analysable with the known methodologies of mobile forensics.

If, within the module, the investigator finds a micro-USB card, it can be forensically imaged using the FTK Imager[10] and subsequently its MD5 and SHA-1 hash can be calculated to ensure crystallisation of the evidence. This can be done using USB write blocker software and a USB adapter for MicroSD cards. It is also possible to do data carving for the recovery of deleted data, for example using PhotoRec[11].

If the investigator finds a hard disk inside, however, he or she can perform a standard acquisition following the methodologies and tools used in computer forensics. The simplest approach is to leave it in the system and connect a write blocker device with an IDE/SATA connector. Another approach is to remove the hard drive from the system, for instance when a drive crash occurs.

Once the data has been accessed, the file system supported by the system must be identified and then analysed. It may happen that the file system is not recognisable or proprietary or contains unknown file formats. In this case, we proceed to read the hexadecimal with an editor like Winhex[12] and, if we are lucky, something written in plain text comes to us so that we can deduce data, for example the name that tells the map type or the coordinates [25]. If it is a QNX[13] system, a QNX Virtual Machine (VM) environment can be used to correctly interpret the data on the hard disk. On the other hand, you can use the open source digital forensics platform Autopsy, but reading the OS is difficult and often indecipherable. What one can do is guess the type of data contained by directory names, but for the contents, it is a problem. Attempts have been made to install toolkits such as Autopsy and Sleuth Kit in the QNX environment to assist analysis, but this has not been possible due to the inflexible nature of the operating system [13]. Another approach is to locate the JTAG port and read the data with that.

---

[10] FTK Imager quickly assess electronic evidence by obtaining forensic images of computer data, without making changes to the original evidence (https://www.exterro.com/ftk-imager)

[11] PhotoRec is a tool that allows you to restore lost files from all digital devices such as computers, digital cameras, mobile phones, tablets, memory cards, external hard drives, CDs and more. The program can also recover corrupted photos (https://photorec.it.softonic.com)

[12] WinHex is a universal hex editor, particularly helpful in the realm of computer forensics, data recovery, low-level data editing (http://www.winhex.com/winhex/hex-editor.html)

[13] Details can be found at: http://www. qnx.com/products/

The JTAG also provides the memory structure and the file system that the investigator can analyze with the classic digital forensics techniques. Again, however, the file system may contain files in a proprietary format that the investigator may not be able to decipher, as well as files in hexadecimal that he or she can try to decipher. By reading the technical manual of the system, you can find information on the type of chip that stores the information. For example, the HMI NG 1.1 has a 32 GB Electronic Multimedia Card (eMMC) chip as a storage method, which boasts features such as Bluetooth, Wireless Local Area Network (WLAN) and support for CDs, DVDs and SD cards, and this is the same chip found in mobile phones, and therefore known. The advantage of this approach is that it avoids damaging the device by ensuring the integrity of the data. Unfortunately, a device received as part of an investigation may be physically damaged, or the device may not provide an interface for data acquisition and, as a result, its data may be inaccessible using the automated software-based approach. In this case, the investigator must opt for the third approach: the chip-off.

The memory chip-off is an even more invasive approach, which consists of removing and reading the memory chips in the system on which the expert then conducts the analysis (see section 3.2).
To perform chip-off analysis, forensic investigators follow the best practices used by electronics manufacturers for their rework process, in which manufacturers remove and replace defective components in their products. This procedure uses hot air to heat the chip just enough to melt the solder that connects the chip to the PCB, which allows for the safe removal of the chip. We refer to this technique as thermal-based chip removal. At this point, the chip can be read via an adapter and analysed at a low level as an unprocessed data dump [13].
Chip-off is a risky procedure because there is a possibility of burning the memory during the extraction process. Unfortunately, it has been shown that even if the temperature used during chip removal is the minimum temperature required for the soldering to reach its melting point (usually above 200 C), this temperature is still high enough to introduce a very high number of new raw bit errors into the chip. Unfortunately, since the ECC data stored on the chip has a fixed error correction capability, newly introduced errors are often able to render much of the data on a NAND flash memory chip unrecoverable using traditional low-level analysis techniques [19].

In all the approaches described above, the safety systems installed by the manufacturer have to be taken into account (see section 3.4 the challenges to be faced). Through the Judiciary it is possible to ask for the support of the car manufacturers by sending the control unit to the manufacturer, but this approach is difficult to implement and can cause problems in maintaining the chain of custody.

5 Forensics Analysis on on-board control units (ECU)

Unlike forensics analysis on infotainment systems which are used in investigations where the vehicle is used as a means to perpetrate a crime, the data from the control units are used to reconstruct the dynamics of an accident.

The electronic control units or ECUs (Electronic Control Units) are microcontrollers that manage the functions and mechanics of the vehicle. Each ECU is responsible for controlling certain specific processes such as engine, gearbox and airbag activity status, fuel levels, general vehicle condition, number of doors closed and seat belts fastened, etc. These are equipped with memories and are connected to each other so that data can be exchanged.

5.1 How ECU work

An ECU is like a small computer that receives incoming analogue or digital signals from sensors that are the ECU's connection to the outside world. The sensors monitor certain parameters that the ECU then processes and uses to do things. The ECU is connected to a communication network through which it exchanges data with the other ECUs on the vehicle. The ECU, (see Figure 3) processes the signals taken from the sensors and the network and, on the basis of these, generates output variables that will be used to provide the signals to activate the actuators that make up the physical arm of the ECU, such as electric motors, window lifters or anything that is capable of transforming an electrical signal into a mechanical movement. The control programme, the 'software', is stored in a special memory and implemented by a microcontroller. Finally, there is the connection to the power supply [8].

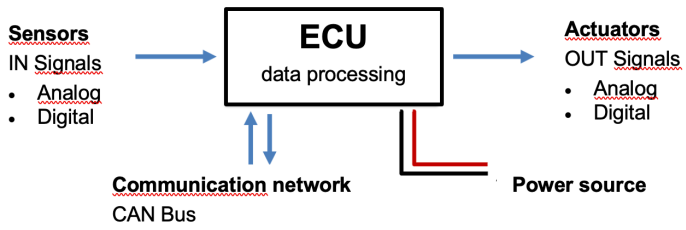

Figure 3 – Electonic Control Unit

One of the requirements on electronic systems is real-time capability. This means that control procedures must react to in- put signals within an extremely short time. For example, a wheel that has a tendency to lock must be detected so quickly that the ABS control algorithm in the control unit can reduce the brake pressure via the hydraulic modulator quickly enough. Brake slip is therefore reduced before the wheel can lock.

The electrical and electronic systems of motor vehicles are often not independent of each other, but influence and complement each other. For this reason, the individual components must be interconnected with networks or sub-networks so that the information managed by the individual systems can also be used by the system as a whole. Different communication systems are used depending on the requirements. The type of network depends on the type of data travelling over it, and thus on the reliability, tolerance and speed required: for example, the management of signals for opening windows will have different requirements to that for brake management.

The CAN bus is now the standard for communication between electronic control units within the different areas of electronics (transmission, suspension, body electronics and infotainment) and is a powerful backbone for networking these areas with each other. Additional bus systems (e.g. LIN bus, MOST bus) are used as sub-bus or for high-speed data transmission with relatively low real-time requirements in the vehicle (see Figure 4).

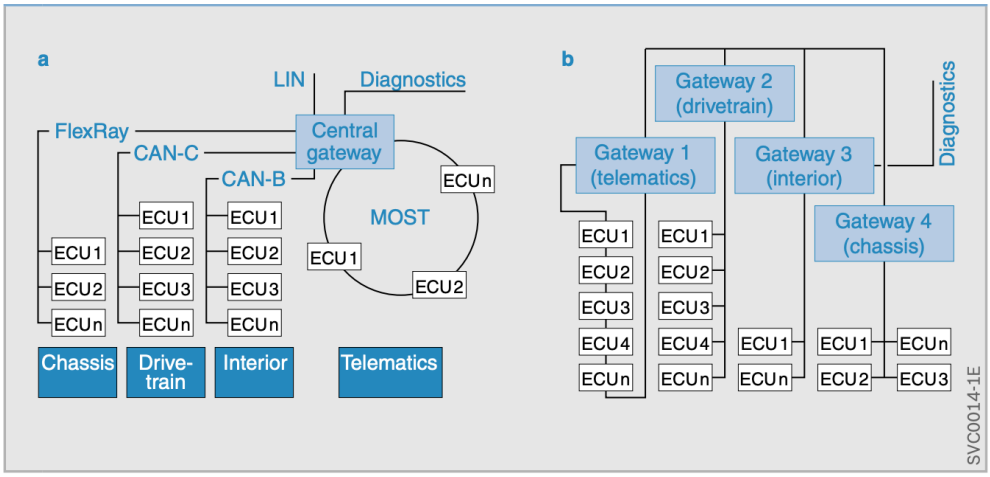

Figure 4 - The ECUs connections [8]

However, the different network protocols are incompatible, which means that data cannot simply be exchanged between networks. In this case, help is provided by a gateway. A gateway can be compared to an interpreter that receives 'data' from one interlocutor, translates it and passes it on to another interlocutor. Technically, a gateway is a computer that reads data transmitted by networks and converts it into another format. The use of gateways thus enables the exchange of information between different networks. The network topology can provide for a central gateway (Figure 4 a) or several distributed gateways (Figure 4 b) can be used to interconnect bus systems. The diagnostic interface is connected directly to the engine and gearbox control unit via the serial K-line. All other ECUs are connected to the diagnostic interface via a simulated virtual K-line on the CAN bus.

5.2 ECU and failures

Almost all ECUs, especially engine ECUs, are equipped with a fault memory.

The fault memory stores data from a function called self-diagnosis that ECUs have. Monitoring functions are implemented in control-unit hardware (e.g. “intelligent” out- put-stage modules) and software to ensure that the control unit functions correctly at all times. The monitoring functions check each of the control-unit components (e.g. micro- controller, flash EPROM, RAM). Moreover, the CAN protocol contains control mechanisms to detect malfunctions. As a result, transmission errors are even detectable at CAN-module level.

The ECU can make a diagnosis of two types:

- the **electrical** type, if it notices if, for example, some sensors are malfunctioning, or if a component is consuming too much current, or if it is broken;
- **functional diagnosis,** if from a comparison of the signals arriving from various sensors it understands whether those values are compatible with each other, for example if the speed sensors on the wheels indicate that the car is travelling at a certain speed and instead some other sensor is sending data that is inconsistent with this type of information.

Each fault is stored as a fault code in the non-volatile area of the data memory. The fault code also describes the fault type (e.g. short-circuit, line break, plausibility, value range exceeded). Each fault-code input is accompanied by additional information, e.g. the operating and environmental conditions (freeze frame) at the time of fault occurrence that were running on the CAN network (e.g., engine speed, engine temperature) [8].

All this data can be accessed to understand what caused an accident. The next session will deal with the methodologies for acquiring this data.

5.3 Data acquisition from ECUs

In order to facilitate the reading of fault memory information from the ECU, a standardised diagnostic socket, called OBD-II (On-Board Diagnostics) (see Figure 5), is mounted in an easily accessible location in every vehicle (easily accessible from the driver's seat). The socket is used to connect a scan tool. The interface may vary depending on the make of vehicle.

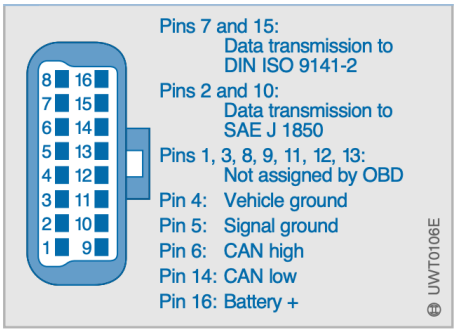

Figure 5 - Presa ODB socket [8]

The port is defined by a standard that allows access to the gateway and control unit and allows reading vehicle parameters, identifying control units, downloading fault memory or clearing fault memory and controlling actuators (e.g. controlling the activation of a windscreen wiper motor). The OBDII hardware interface includes a 16-pin (2 × 8) female J1962 connector. Each pin in this J1962 connector has a different function: pins 1, 3, 8, 9, 11, 12 and 13 are vendor-specific, while pins 2, 4, 5, 6, 7, 10, 14, 15 and 16 always have the same standard function (see Figure 5).

The data acquired from the modules can be examined with the official dealer's diagnostic tools, if available to the investigator, or alternatively, with appropriate third-party hardware/software (see Figure 6). This will depend on the type of investigation being performed and the nature and importance of the data.

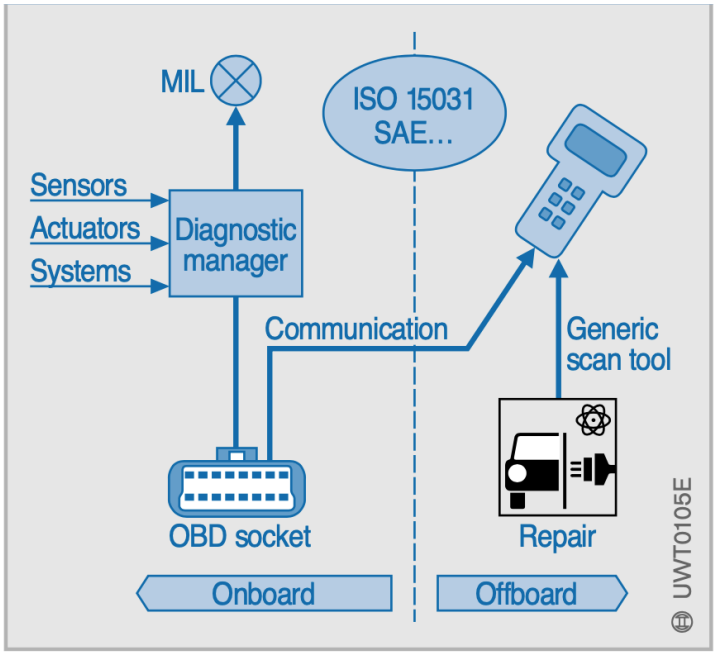

Figure 6 - ODB system [8]

The diagnostic tool shows the modules on the car, tells you if any are corrupt, and provides information such as the version of VCDS, the VIN/chassis number of the car; the licence plate (input by user); the mileage; the chassis type; modules scanned by the software and repair order.
When the programme completes the module check, it will display additional information on each module. The reason for the malfunction is recorded in the 'frozen' frame data. In an investigation, it may be useful to determine the errors and their causes [25].

On some occasions, e.g. when a car is damaged, it may be necessary to remove one or more modules from the car for forensic examination. In this case, it is recommended to have the removal attempted by a professional technician in order to minimise the risk of module damage or data corruption. Data acquisition in this case will be done using j-tag or chip-off (see section 3.2).

6 Forensic analysis on Event Data Recorder (EDR)

An Event Data Recorder is a feature or device installed in a motor vehicle to record technical information about the vehicle itself and the occupant when a collision event is detected [15]. Examples of EDRs, installed in most vehicles, are in the airbag control unit, which has sensors that monitor the vehicle's acceleration, but also in the pedestrian collision modules. The development of EDRs can be traced back to 1990, when General Motors introduced the diagnostic energy reserve module (DERM) to record data about airbag systems. Indeed, it is rare for automobiles manufactured nowadays not to have some module of EDR. There is no standard location for the positioning of an EDR however, it is usually located inside the vehicle cabin, close to the centre line of the vehicle or under/in one of the front seats. The physical removal of an EDR usually requires the disassembly of a vehicle's interior. EDR data, which varies according to the make, model and year of vehicles, can support the physical evidence used in crash investigations [5]. Consequently, the majority of studies related to EDRs have focused on using data after it has been recovered and decoded.

The EDR continuously monitors the data from the sensors, checks the vehicle's speed and if it changes with a certain threshold, the ECU realises that a collision has occurred and starts storing the data travelling on the CAN network. The relevant data predetermined for crash analysis is sent to the EDR from an ECU located inside the vehicle in a specified format and specified time sequences. The ECU also stores the data travelling on the CAN 5 seconds before and after the event and records and stores the data throughout the event.

In the 5 seconds before the collision it stores, vehicle speed, percentage of acceleration pedal opening, brake application (pressure in the brake system that determines the extent of braking), wheel speed, roll and steering angle. In the next five seconds, it records, from the state of the seat belts and airbags, the accumulation of pressure on the seats, the presence of the occupant and its size, the deployment of the airbags and pre-tensioners, and the ignition cycle of the ignition from start to memory.

An important, and often useful element to look at on the report, is the ignition cycles. Most control units, in fact, do not give time references, and if the investigator wants to cross-reference them with data from a mobile phone for example, the only reference you can get is the number of ignitions of the dashboard. If the data retrieved at the accident scene comes from the accident under investigation, the ignition cycle must be equal to or less than one from the ignition cycle at the time of the investigation (ignition cycles at deployment and at investigation are given).

From the change in speed during impact, the corresponding deformation energy can be determined. Sometimes even with just one EDR it is possible to trace the parameters of the other car without a photo doc.

The EDR stores data for both **deployment** and **non-deployment** events, that is, both those events that result in the activation of safety systems (airbags) but also those if they are not severe enough to do so. The *deployment* data are stored permanently and are non-rewriteable, while the *non-deployment* data are recorded but can be overwritten. If an additional *non-deployment* incident is detected maybe that one will overwrite a previous one for me. Memory space is limited to about 3 events, so the fourth one overwrites the first one.

Data collected by EDR ECUs are used as a source of evidence during forensic road accident investigations to ground or correct an accident reconstruction, be of assistance in accident reconstruction when traditional information (photos, brake marks, etc.) is lacking, give evidence of driver error, or give evidence of device malfunction.

The data are not suitable, however, for forensic investigations of various acts of fraud, manipulation of the VIN identifier stored in the vehicle in digital form, odometer fraud (restoring the number of kilometres driven), and detection of other vehicle activities (including automated activities), as well as the behaviour of vehicle occupants and their communications with the environment outside the accident event.

6.1 Data Acquisition

As with other ECUs, the investigator has several ways to download data at his disposal. The method to retrieve the data will depend on several factors such as damage to the vehicle, weather conditions, and available power sources.

The best method is to access the data through a CDR (Crash Data Retrieval) device attached to the vehicle's OBD-II diagnostic socket. The CDR module interface is used to download and display the data stored in the EDR. The CDR tool connected to a computer with CDR software through an RS-232 cable will display the data on a computer without changing the data stored within the EDR, which will remain on the module (see Figure 7).

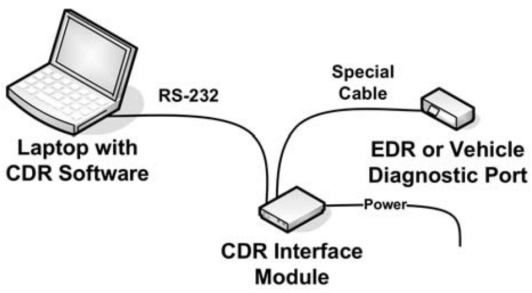

Figure 7 - Data recovery System connection

At the first connection, that is, when the case is opened, the investigator is asked to enter case-specific information such as the vehicle information number (VIN), its name, case number, date of investigation and date of accident plus some comments. Next, the CDR, through an EDR model-specific dump command, dumps the non-volatile memory from the EDR onto the non-volatile memory of the CDR Interface Module. At this point, the CDR dumps the stored data to analyse it in three sessions. Finally, a temporary file is generated with the report. Three sources of data are contained in the dump: user-entered data, CDR-supplied data and hash values used to ensure the data has not been altered.

Methods for retrieving data stored in EDRs are generally proprietary in nature. The data stored on the EDR is normally retrieved by crash investigators using the Bosch Crash Data Retrieval Tool (CDR) [15]. The **Bosch CDR Toolkit (formerly Vetronix)** is a commercially available system is a reliable, versatile, and increasingly powerful industry-standard platform that retrieves EDR data from the vast majority of modern vehicles. After EDR data are downloaded from a vehicle and saved in a secure file format, the CDR Tool software generates a detailed report that can be used by investigators in a variety of ways [9]. See Figure 8 for an example of parameters contained in the Report provided by Bosch CDR.

Other CDRs that can be used are [11]:

- **The Tesla Vehicle Kit** is now available for the North American market. This kit contains all the hardware needed to download EDR data that can be stored in Tesla Model 3, Model S and Model X vehicles [26].
- **The Hyundai and Kia GITs, Event Data Recorder (EDR)** tool released by the manufacturers have developed by Global Information Technology (Global IT) provides access to data stored in Hyundai and Kia vehicles have been developed only for vehicles produced after September 12, 2012 [18].

Pre-Crash Data -5 to 0 sec				
Time Stamp (sec)	Vehicle Speed (MPH)	Engine Speed (RPM)	Service Brake (On, Off)	Steering Wheel Angle (degrees)
-5	92	3574	ON	-2
-4	86	3382	ON	0
-3	82	3190	ON	4
-2	79	3190	OFF	-12
-1	79	3062	OFF	-48
0	72	2788	ON	-37

System Status at Deployment	
Airbag Warning Lamp Status	ON
Driver's Belt Switch Status	Buckled
Passenger's Belt Switch Status	Buckled
Passenger's Seat Position Switch Status	Rearward
Ignition Cycle Count at Deploement	2767
Ignition Cycle Count at Download	2769
Maximum Recorded Velocity Change (MPH)	-35.98
Event Recording Complete	Yes

Figure 8 - Example Bosch CDR Report parameters [9]

The reports generated by the tools (*.CDR files) are 4-5 to 20 pages long, but in all cases, careful examination of the data by a certified technical analyst is required to validate the content.

The method used by the system to select and enter the data is unknown, making it difficult to verify the repeatability of the extraction process and results. In fact, the *.CDR file does not contain the original data collected during the three passes. This implies that the CDR software transforms the data read from the EDR (possibly by performing certain calculations on the data) before being displayed in the CDR report. Without additional translation techniques and tools, it must be assumed that all available data are translated. However, it would be very useful to have an alternative HTT to compare results.

A module may contain more than one recorded event; many have the capacity to record up to three events, so it is necessary to determine whether the events are related to the incident being investigated or possibly to an earlier event.

Another problem could be inconsistent data to interpret depending on the dynamics of the accident, such as a negative or non-zero speed at the time of impact. In this case, the investigator has to take into account the other factors that could affect the recorded speed such as: the wheels of the vehicle not being in contact with the ground (in flight); yawing (wheels rubbing sideways); the vehicle in reverse; or even (if the module has not been reprogrammed) the size of the tire, if they do not have the size recommended by the manufacturer. Also, because the vehicle speed sensor actually measures the rotation of the drive shaft and not the actual speed, the speed of a vehicle that is sliding sideways on ice is not reported correctly in the EDR [5]. The data may be inconsistent even if the full scale of values is reached. In addition, I might be in the presence of partial data if the ECU is damaged or

overwritten in the case of multiple collisions, especially if the ECU has recorded data for non-deployment events that, unlike deployment events, can be overwritten.

Finally, in the case of a serious accident where the vehicle has been destroyed, the communication network may be compromised or the device difficult to access. In the case where it is necessary to pull out the ECU, the investigator must keep in mind that the ECU does not realize that it has been disassembled. Capacitors, in fact, allow the control unit to record events even if the blow of the accident disconnects the power supply, so for example in the case of a fall the accident could be recorded and could go on to overwrite the recorded data. In any case, extracting the ECU and acquiring the data by direct instrument connection at least allows the ECU as evidence.

EDRs provide vital data for traffic accident reconstruction. They are not suitable, however, for the forensic investigation of various acts of fraud, manipulation of the VIN identifier stored in the vehicle in digital form, odometer fraud (restoring the number of kilometres driven), as well as the behaviour of vehicle occupants and their communications with the environment outside the accident event. Nevertheless, during accident reconstruction, it is important to also consider the physical evidence that is always present instead of relying solely on digital evidence. To prevent the evidence from losing legal value, the investigator should maintain a detailed record of the chain of custody of an EDR. This specifically includes documentation of all physical extractions from the module because there are no unique identifying marks on the EDR that tie it to the vehicle. In addition, it should retain the original human readable report provided by the EDR because this document becomes the evidence used in the legal context. This is because, as we mentioned, the original data in the EDR device could be erased (the memory is erased after the unit has been turned on a number of times), overwritten, or corrupted.

6.2 Regulations

In the U.S. and Canada since 2010, EDR is not mandatory, but the legislation requires that if the vehicle is equipped with this feature, the data must be accessible i.e., there must be commercial availability of the necessary tools to enable accident investigators to retrieve data from the EDR. In addition, manufacturers are required to include a statement in the manual of the presence of the EDR and the data being stored [15].

Legislation is being worked on in Europe, but some automakers do not agree to provide the data. Some are giving access.

The draft Regulation on the specification of these systems, which will become mandatory from 2022, calls for a black box that can tell what is happening, but not where, for privacy reasons *(We are very*

concerned about the proposed EDR requirement that it should not be able to capture and store data elements about the location, date and time of events). VolVo and Toyota have it.

In terms of regulation, in some countries the government has mandated that all vehicles be manufactured with an event data recorder (EDR), or "black box", which continually captures data points that include speed, reliability of brakes, seat belt usage and many other important metrics.

7 Black Boxes (RCA) and eCall Units

Black boxes are installed by insurance companies that bring discounts on the policy if they deem the driving style appropriate. They are useful in making it easier to find a car if it is stolen and lead to a reduction in fraudulent actions against insurance companies.

Black boxes can be used in appraisal to prove and certify one's car's condition, location, and possibly serve as a probative element or evidence for the defence or prosecution.

Connected to the car's battery, they are capable of recording a great deal of data pertaining to the driver's conduct and driving style, including claims. The recorded data also helps the owner find the vehicle in case of theft and can also be used to contest a traffic ticket. In order to provide a fairly specific and comprehensive driving style overview (E.g. an aggressive type – speeding, abrupt braking, intensive braking and so on) a black box usually records: the location of the vehicle via GPS; any impacts of the vehicle (location, speed, impact); driving and stopping times; accelerations and decelerations and braking relative to the routes taken, activation of safety devices and the gears gradually engaged, etc.. The amount of the vehicle's insurance premiums then depends on these parameters.

A black box generally consists of a triaxial accelerometer and gyroscope, a satellite navigation system (GNSS[14]) and a GSM module to send data to black box companies.

The appraisal of the black box installed in cars for insurance purposes, but also in other motor vehicles such as motor vehicles or trucks, must be carried out with the authorization and with the support of the insurance companies in such a way as to be able to guarantee the integrity of the acquired data.

Limitations may include incorrect installation or detachment of the control unit due to impact.

An eCALL Unit, on the other hand, is a device designed to call emergency services in the event of a car accident or in the event of an emergency determined by an occupant of a vehicle.

This device is mandatory in every new car sold within the EU, including vehicles imported from outside Europe destined for the European market, as of April 2018 [1].

eCALLs are energy-independent, high-strength and long lasting, and are activated automatically (by special sensors that register a vehicle crash or airbag deployment), or they can be activated manually by vehicle occupants. Upon activation, the nearest 112 emergency telephone line operations centre is located, and data describing the accident location, circumstances, and basic vehicle characteristics

[14] GNSS (*global navigation satellite system*) is a system that provides a geo-spatial positioning service with global coverage that enables small, dedicated electronic receivers to determine their geographic coordinates (longitude, latitude, and altitude) at any point on the earth's surface or in the atmosphere with an error of a few meters.

are transmitted from the telematics systems. In general, the following data are transmitted: GPS coordinates of the vehicle's location, direction of travel, VIN identifier, vehicle category, fuel type, number of passengers (i.e., number of people wearing a seat belt), an indication of how the unit was activated (manually or automatically), and various other information about the credibility of the accident. This data is transmitted via a mobile phone through a Bluetooth connection or a device equipped with a SIM card to an emergency line operations centre that will use it primarily for organizing and carrying out rescue operations [1]. However, the data sent can also later be used for forensic and other security investigations to investigate fraud such as vehicle identity changes, simulating a traffic accident, and so on [27].

8 Conclusions

In just a few years, both the cost of mobile data has dropped dramatically and the penetration of computers in cars has increased. Vehicles are becoming more complex and it is increasingly difficult for a forensic investigator, including those in government and law enforcement agencies, to gain insight into the design of digital vehicle components and their interactions that would facilitate forensic investigations. This paper has outlined some of the challenges associated with digitally investigating various systems on a vehicle, looking at the various stages of digital forensics on key sources of evidence. Both traditional digital forensics tools and some specialist equipment for finding evidence from vehicles have been described. Hardware and software solutions that can be used to find evidence from vehicles were then discussed.

This document can also be used to train investigators on where to look for specific information in a specific module when attempting to extract information from a vehicle and how to handle the data in a way that it can be relevant to an investigation if collected and analysed.

In terms of future work, more research can be done on CAN and MOST bus interactions and whether infotainment system data can be accessed and downloaded via CAN: it would be interesting to know if it is possible to develop an acquisition method using the CAN bus as a means of connection. This would provide a standardized approach to data acquisition as CAN buses are universal in modern vehicles. Another research might be on automated real-time capture of the target vehicle or intercept stream based on their IP or other unique information. Integrating forensic readiness into the design of future vehicles, a term coined forensic-by-design, will facilitate future forensic investigations of such vehicles.

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 forensics on the other. There will undoubtedly be a need for accessible, sufficiently general and certified forensic technologies that are relatively easy to use in forensic investigations, as well as suitable forensic methods and methodologies. These activities will be closely associated with the training of entirely new types of specialists, forensic engineers and forensic workplaces, the subject matter of which will be highly multidimensional.

9 References

[1] EUROPEN COMMISSION, MOBILITY AND TRANSPORTS - AN AUTOMATED ECALL SYSTEM - HTTPS://EC.EUROPA.EU/TRANSPORT/SITES/DEFAULT/FILES/PROJECT-AN-AUTOMATED-ECALL-SYSTEM.PDF

[2] ANDROID AUTO - HTTPS://WWW.ANDROID.COM/INTL/EN_CA/AUTO/ - *ANDROID* - SEPTEMBER 2021

[3] A. DEL SOLDATO - ATTIVITÀ DI ANALISI FORENSE SU SISTEMI DI CLOUD COMPUTING - CIBERSPAZIO E DIRITTO VOL. 14 N.49 (3-2013) – 2013

[4] APPLE CARPLAY - HTTPS://WWW.APPLE.COM/IT/IOS/CARPLAY/ - APPLE INC. – SEPTEMBER 2021

[5] N. SINGLETON, J. DAILY, G. MANES - *AUTOMOBILE EVENT DATA RECORDER FORENSICS* –ADVANCES IN DIGITAL FORENSICS IV, CHAPTER 21, SPRINGER PROFESSIONAL "TECHNIK" 2008

[6] *AUTOMOTIVE GRATE LINUX* - HTTPS://WWW.AUTOMOTIVELINUX.ORG – THE LINUX FOUNDATION PROJECTS – JULY 2021

[7] QNX NEUTRINO REAL-TIME OPERATING SYSTEM (RTOS) - BLACKBERRY - HTTPS://BLACKBERRY.QNX.COM/EN/SOFTWARE-SOLUTIONS/EMBEDDED-SOFTWARE/QNX-NEUTRINO-RTOS - JULY 2021

[8] K. REIF (ED.) - *AUTOMOTIVE MECHATRONICS, BOSCH PROFESSIONAL AUTOMOTIVE INFORMATION* - DOI 10.1007/978-3-658-03975-2_2, © SPRINGER FACHMEDIEN WIESBADEN 2015

[9] BOSH DIAGNOSTIC – BOSH, HTTPS://CDR.BOSCHDIAGNOSTICS.COM/CDR

[10] SWGDE - SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE - *BEST PRACTICES FOR VEHICLE INFOTAINMENT AND TELEMATICS SYSTEMS VER.2.0* – 23 JUNE 2016

[11] CRASH DATA GROUP, *TOOLS TO HELP YOU UNDERSTAND THE CRASH* - HTTPS://CRASHDATAGROUP.COM/

[12] C. ENCE, J. RUNS THROUGH, GARY D. CANTRELL - CHIP-OFF SUCCESS RATE ANALYSIS COMPARING TEMPERATURE AND CHIP TYPE – JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW, VOLUME 13, NUMBER 4, ARTICLE 7, FEBRUARY 2019

[13] J. MOOS, G. DAVIES, E. LEWIS, N. WILLIAMS, B. GICHOHI, R. LANE, A. BELLAMY - *DIGITAL FORENSICS FOR AUTOMOBILE SYSTEMS: THE CHALLENGES AND A CALL TO ARMS* - INTERNATIONAL JOURNAL OF FORENSIC SCIENCES ISSN: 2573-1734, VOLUME 1, ISSUE 1, JUNE 2016

[14] E. A. BATES - *DIGITAL VEHICLE FORENSICS* - HTTPS://ABFORENSICS.COM/WP-CONTENT/UPLOADS/2019/02/INTERPOL-4N6-PULSE-ISSUEIV-BATES.PDF, FEBRUARY 2019

[15] SENIOR TROOPER STEVEN T. KEAN - *EVENT DATA RECORDER, AN OVERVIEW* – VIRGINIA STATE POLICE

[16] S. PRADO - *EXTRACTING FIRMWARE FROM DEVICES USING JTAG - HTTPS://EMBEDDEDBITS.ORG/2020-02-20-EXTRACTING-FIRMWARE-FROM-DEVICES-USING-JTAG - FEBRUARY 2020*

[17] GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA - HTTPS://WWW.GAZZETTAUFFICIALE.IT - FEBRUARY 2020

[18] W. R. "RUSTY" HAIGHT, S. GYORKE, S. HAIGHT - *HYUNDAI AND KIA CRASH DATA, THE INDISPENSABLE COMPENDIUM* - COLLISION MAGAZINE - VOLUME 8 ISSUE 2, 2007

[19] A. Fukami, S. Ghose, Y. Luo, Y.Cai, O. Mutlu - Improving the reliability of chip-off forensic analysis of NAND flash memory devices - Part of special issue: DFRWS 2017 Europe: Proceedings of the Fourth Annual DFRWS Europe, Pages S1-S11

[20] Berla Corporation - *The iVe Ecosystem* - https://berla.co

[21] B. Kopencova, R. Rak - *Issues of Vehicle Digital Forensics* - 2020 XII International Science-Technical Conference AUTOMOTIVE SAFETY, Kielce, Poland, Oct. 2020

[22] J. Deichmann, B. Klein, G. Scherf, R. Stützle - *The race for cybersecurity: Protecting the connected car in the era of new regulation* - McKinsey Center for Future Mobility – October 2019

[23] D. Brezinski, T. Killalea - Guidelines for Evidence Collection and Archiving - https://www.rfc-editor.org/rfc/pdfrfc/rfc3227.txt.pdf - February 2002

[24] G. Ziccardi - *Scienze forensi e tecnologie informatiche: la computer and network forensics* - Informatica e diritto, XXXII annata, Vol. XV, n. 2, pp. 103-125, 2006

[25] N. Le-Khac, D. Jacobs , J. Nijhoff , K. Bertens , K. K. Raymond Choo - Smart vehicle forensics: Challenges and case study - Future Generation Computer Systems (International Journal of Future Generation Computer Systems Grid Computing: Theory, Methods & Applications), Vol. 109, pp. 500-510, 2020

[26] Tesla Event Data Recorder (EDR) Resources – Tesla, https://edr.tesla.com/

[27] D. Kopencova, R. Rak - Issues of Vehicle Digital Forensics - 2020 XII International Science-Technical Conference AUTOMOTIVE SAFETY - October 2020

[28] J. Lacroix - *Vehicular Infotainment Forensics: Collecting Data and Putting It into Perspective* - University of Ontario Institute of Technology, MSc Computer Science Thesis, 2017

[29] Ab Rahman, N. H., Glisson, W. B., Yang, Y., Choo, K.-K. R. (2016) - Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing, 3(1), pp. 50–59.

[30] European Parliament, Official Journal of the European Union - Autonomous driving in European transport European Parliament resolution of 15 January 2019 on autonomous driving in European transport - (2018/2089(INI)) - 15 January 2019

[31] EDPD, Europen Data Protection Board - Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications - Version 2.0 Adopted on 9 March 2021