Investigating modern cars

D. Sladović[1], D. Topolčić[1], K. Hausknecht[1],G. Sirovatka[2]
[1]INsig2 d.o.o., Zagreb Croatia
[2]Zegreb university of applied science, Zagreb Croatia
Danijel.Sladovic@insig2.com, Davorka.Topolcic@insig2.com, Kresimir.Hausknecht@insig2.com,
goran.sirovatka@tvz.hr

***Abstract* - Car forensic is one of the branches of digital forensics that is recently becoming more and more popular and important. Because of the accelerated growth of technology and its implementation in various industries, modern cars have additional features to raise the level of security, improve the driving experience, and now add the advanced option to connect the car to the internet. The possibilities today are much more advanced, which means that today's cars can drive autonomously, read the email, respond to messages, automatically receive software updates over the internet that provide new features. Today "smart" cars can even be controlled over the key fob or mobile app. This paper will show common information that can be found in the car; who drove it, how he drove, where and in what state did he drive, information that is related to the car and its mechanics, all the synchronized information etc. It will also explain the extraction process, software used for the extraction, and which difficulties the forensic examiner can encounter during the extraction. Furthermore, the information extracted may prove to be useful in resolving different types of crime, and it can show the importance of digital forensics of cars.**

Index Terms - Car, forensics, digital forensics, investigating cars, modern cars, car forensic, information technology, information

I. INTRODUCTION

In this paper the reader will be introduced to the field of car forensics. Another focal point will be the cars onboard systems which will explain what security features can be found on car systems, and how they can be manipulated with. The next thing that will be explained is the digital evidence that can be found in a car during a forensic investigation and how the car's systems can be accessed to find as much evidence as possible. After that, each phase of the forensic process will be covered and explained, and what a forensic investigator has to do and what procedure to follow during the acquisition process. The final part of this paper will explain a use case for the car forensic process and how to acquire evidence or data from a car's system, what tools and methods for the acquisition process can be required. Then the data acquisition of a car's infotainment system will be explained and what tools can be used for the procedure. Additionally the connection between the car's system and infotainment system will be explained.

The main goal of this paper is to introduce the field of car forensics to the reader and especially to forensic investigators and ultimately to raise awareness of the importance of car forensics.

II. CAR FORENSICS

Today we have all kind of smart things like; smartphones, smart television, smart watches, smart bracelets. These technological gadgets are very common these days. But today the common public does not realize that modern or "smart" cars can also store a lot of data and even have the capability to be connected to the internet. On top of that, cars store all the data about situations that happen around and inside them, and this is the reason why modern cars are considered to „know more" about their owner or driver than a smartphone does. Car forensic is a newer and less known branch of digital forensics. Vehicles are becoming more important sources of digital evidence in criminal investigations. Traditionally if a car is connected to a crime, the investigators focus more on DNA, fingerprints, and other physical materials that are not of digital nature. Cars have just recently become interesting for attackers, but the most important fact of all that has made car forensics more popular is that the older cars did not save data that can be of use for the investigators. Because modern cars have more and more security and entertainment features, this paper will describe some of the challenges that an investigator may come across. Some case studies on the forensic acquisition and data analysis of an entertainment system of a modern car will be described.

III. EMBEDDED ONBOARD CAR SYSTEMS

First, it is important to mention embedded car systems which come in a huge variety of shapes and functions and serve in a specific purpose. Because of the low cost of equipment that is used to produce these kinds of systems, they are now included in many devices used today. These systems have an extremely varied degree of technical quality especially regarding systems which are important for safety while driving. These systems can often be overlooked by an unaware observer. Embedded car systems can also be problematic for the examiner. This can occur because some systems need to be connected to the car they are made for and the components of the car that they control, in order to enable the examiner to extract data saved on them. Another thing specific to the car systems is the fact that the data and the state of the system are susceptible to the environment with which the system interacts. For example, if the car door is opened, or the

engine is turned on, it can delete the records saved in the recent history. Modern cars are also equipped with all kind of sensors which can create a lot of information that can be found in the car's system. [1]

A. *Security related to car's onboard system*

The security system of a car is very important because not only can it affect the car, it can also affect the people that are resident in the car. This means that in case of some event or crime law enforcement officers from multiple departments can have jurisdiction. It is interesting to mention that the security aspect was not always so important, because the older cars did not have the ability to connect to the internet or to the outside world. Today car manufacturers must take in consideration the vulnerability of modern cars to hacker attacks, because the more features are added to a car, the bigger the chances are that some attacker will find a "weak-point" and compromise the car system in order to steal the data, steal the car or take control of the car which can endanger the passengers. The danger for the passengers can be even higher if the car is remotely driven, because signals or commands sent from the attacker to the car go through network, which causes a delay from the time the attacker inserted a command to the time when the car reacts.

The improvement can not only be seen in the car systems, but also in the attacks that are becoming more advanced which makes the system manufacturers job harder. The attackers can also target the vehicle system by compromising the entertainment system. But there is also a chance of that attackers will compromise data that is collected from mobile devices connected to the entertainment system. Since the threats are getting more and more serious, the company Arxan has published information about the threats to modern cars with connectivity features and how the drivers can protect themselves from these risks. [11] There are multiple ways that cars can be connected to the outside network:

- vehicle to vehicle using wireless standard WAVE environment (802.11p),
- vehicle to the device using USB, Bluetooth, WIFI, NFC,
- vehicle to the environment over the GSM network and 802.11p (WAVE).

Essentially, if car has an onboard computer it creates new security vulnerabilities. The Center for Automotive Research (CAR) stated that modern, connected cars have 16 possible points of vulnerability. Some of these points are already stated above. There is also car system called CAN-BUS which is a bus standard designed to allow microcontrollers and devices to communicate with each other in implementation without a host computer that manages their communication. It is used as an internal network for the car's system that controls the car or its actuators using packets or signals sent from ECU to other parts of the car. The CAN-BUS or BUS-system is also used for automotive diagnostic and to flash applications. It operates according to ISO 11898, ISO 11898-1, ISO 11898-2, ISO 11898-3 standards. [12] On top of that, the modern cars can have several other systems that are used and have their own purpose:

- K-Line is one of the first mechanisms that enable access to the ECU (replaced by the CAN) [3]
- LIN is an inexpensive and slow communication that enables the control of less independent systems like door modules, window control, seat control which are connected to the cars main system
- SAE J1850 is used to provide access to vehicle networks for onboard-diagnostics (ODB) [4]
- FlexRay is a very fast network bus system for security-critical applications (drive by wire)
- Media-oriented system transport (MOST) is a large data transmission for infotainment and other data-intensive systems
- Ethernet is used for diagnostic and flash programming at high bandwidth

As stated above, these systems are included in the car system that can be compromised and allow control of locks, breaks, airbags, steering wheel sensor, stability control, engine, and more. To reduce the risk of a car being hacked, the owner or driver can keep the car's software updated, not connect a smartphone device that is jailbroken or rooted, check the outlets (USB, ODB2 Port) periodically, verify that the pre-installed or third-party apps used in the vehicle are hardened [1][2].

B. *Digital evidence in a car's onboard system*

Digital evidence in a car's onboard system is similar to the digital evidence which can be found in a classic forensic scenario. In this case digital evidence can be found in the car computer system. The data in car systems seem to be volatile because the important information when car is in working mode (such as acceleration, speed, etc.), are saved in the RAM.[1] This does not mean that a skilled attacker will leave no traces or evidence, but this evidence will be harder to collect. As mentioned before, some data is constantly being saved in car's volatile memory (RAM), and in case of a collision, the last 5 seconds are saved to permanent memory (EEPROM) and can be further examined to clarify the circumstances of the accident. This device is called the "Event Data Records" (EDR).

Evidence that can be saved on the EEPROM permanent memory is:

- The status of various vehicle systems
- What seats were occupied in the vehicle
- If, and how was the individual safety equipment used
- The position of the vehicle controls that were actuated by the driver or passenger
- The speed, direction, position and spatial attitude of the vehicle

The device called CDR (Crash Data Retrieval Tool) shown in Figure 1 which consists the "box" or CDR

hardware and of software that operates on Windows operating system can be used by the investigator directly in the field or in the laboratory. It is used to retrieve the data that was recorded before the crash into the car's embedded system. This device can also be directly connected to the EDR module of the vehicle in a situation when the vehicle is too damaged and the EDR can't be accessed through the diagnostic port of the vehicle.

Figure 1. Module interface of crash data retrieval (CDR) [10]

The difficulties that can occur during the extraction of data are the differences in this system from one car manufacturer to another and from one model of vehicle to another. This is because every car model of one make can have different d*at*a saved to *its* system. Which is common because these embedded systems are not standardized. Today's infotainment systems are found to have complex software - these systems can run programs that contain more than 2 million lines of code.[1] And as for all complicated systems goes, the more they are complicated the more room for errors they leave.

Data that can be found on the infotainment system (infotainment system hard disk) can also be very useful in situations where it is required to place a suspect in the vehicle used to commit a crime. Data that can be found in these infotainment systems are:

- GPS data which can be recorded even if a car doesn't have a navigation system. That is possible because some manufacturers create the same navigation/GPS module for a car model, but they enable them for customers only if the car is supposed to have the equipment package that includes a navigation system.
- The information that can be retrieved from the navigation system are tracklogs and track points, saved location's, previous destinations, active and inactive routes.
- List of established connections (devices) using the Bluetooth to connect the smartphone or some other device to the car, if the system is set up to do so, which is the case in most of the newer cars. This way the car can collect the make, model, Bluetooth name of the device, IMEI number, and serial number.
- All connected devices that were connected via USB port or memory card slot to the car i.e. listening to music from a USB flash drive if the car is configured so, will have record that this USB flash drive or SD card was connected.
- Data that can be found from installed applications or multimedia system: information about applications that were run, contacts, messages, emails, credentials, weather information, social networks, browse history, traffic, multimedia files (music, video, images) etc.
- Wi-Fi Access Points (AP's) where the car was connected and it can include information of a smartphone device if it was used for internet teetering.
- Key fobs can also be the source of forensic evidence because they can contain information about the vehicle which is: VIN number, mileage, fuel level, last time the vehicle was driven, GPS data [5] [9].

IV. CAR FORENSICS PROCESS

The car forensic process, in general, is similar to the traditional approach for systems that are inactive at the time of analysis, because the analysis is done on a copy of the systems state in the specific time. To do an examination of embedded and infotainment systems it is important to have extensive knowledge of electronics, digital systems, automation, and control. It also requires the specific skill of field research that needs to be constantly updated by professionals. Like the process of computer forensics, the process of car forensics can also be divided into five stages shown in Figure 2 that were created for the analysis of a car's onboard computer of the embedded system [1].

Figure 2. Stages of digital forensics

A. *Preparation*

At this stage of the forensic process, the investigator has to know all the potential sources of evidence that can be stored in the car system, as well as any other system in the car that can be connected to the car system and can reveal new evidence from those separate systems. This also includes the knowledge of access to the computer board [1].

B. *Identification*

At the beginning of the identification process, the investigator has to identify the type of system that is present during the investigation. The main objective is to separate and recognize data and information that is relevant to the case before starting the process. It is also required that the tools that are going to be used to examine this data, are defined and updated. It is important to use appropriate techniques, so that the files are accessible to forensic analysis in the next phase. In case of car forensic, the vehicle identification number (VIN) can be helpful for finding the right forensic tools to do the acquisition with. The VIN number consists of letters and numbers which all have their own meaning. The data that can be found just

by reading the VIN number (left to right, respectively) is: the country, manufacturer, vehicle type, body type, engine, series, model, check digit, model year, plant, and the last six numbers are the serial numbers. The next step is to identify the used operating system and the type and manufacturer of the computer board. This identification process can include reviewing the manufacturer's documentation, reviewing the design specifications, diagrams, and the human-machine interface [1]. The VIN number can also be helpful during this process if the vehicle examined is destroyed or unrecognizable.

C. Collection

This phase includes the collection process of evidence or data from the systems which have memory and contain digital evidence. During this process, it is recommended to maintain the chain of custody that is basically a generated report containing information about seized evidence, and it also creates the complete documentation about the people involved in the evidence handling.

In this phase, the traffic, that is sent between the car computer board system and the car's infotainment system, is identified and captured. That process also captures the traffic between the car's infotainment system and the Internet. Because these two systems make a closed network it is important that the investigator captures that traffic to gather as much evidence as possible.[1]

D. Analysis

When the process of identifying and collecting is done, the analysis process begins. In this process the data that was previously seized, will be analyzed in order to find useful information that can be helpful for the investigation. The next step is to find a connection or correlation between the found data, so if there is a need to reconstruct the event to establish a link to the suspect and create a conclusion, it is possible to do so. This can be done if the investigator wants to use data from the EDR and infotainment system to prove that a person was in the exact vehicle at the exact time the incident happened, so the suspect can't deny his or someone else's presence in the vehicle.

Analysis of results is the process of gathering all collected, examined, and analyzed evidence so they can be presented in the report that will contain all the truth about the analyzed data and to prove the link to a crime so that irrefutable proof can be presented. During this process, it will also be required to provide information about the tools, and techniques used to prove the integrity of the information. The report should point to the result and conclusion based on the found evidence, but it also should present all the techniques used to preserve, extract, and analyze the content of digital media [1].

E. Documentation

It is crucial that each analysis step has in-depth documentation which includes detailed notes, chain of custody, recording the time, date, and name of the person responsible and other essential information. The documentation is important because the evidence can be compromised during the post-incident analysis, and the documentation can also serve as a reference for future incidents with a similar situation [1]. After everything is analyzed and documented the investigator has one more step to do - write the report. The report is the final document in which the investigator states the facts and conclusion of the entire investigation. The report has to be clear, concise, and enable the non-technical readers to understand it. The report can also be a document that is submitted to a police unit or to the court.

V. CAR FORENSICS USE CASE

As mentioned in the introduction, this paper will describe what possibilities does the investigator have while carrying out the investigation or the recovery of data, which methods can be used to recover the data that is stored in the car infotainment system or the embedded car system.

A. Recovering the data from the vehicle system

The acquisition of data from the car's internal system can be done in three different ways, depending on how the car is designed and what information can be collected:

- Connecting to the OBD-II port
  Using this method the investigator gains access to the standard vehicle network interface. Connection to the OBD-II port can be established via cable or by a wireless connection. Often the data retrieved via this method are data packet identification number (DPID) which is a representation of the NVRAM data but not the actual data. For the access to the actual NVRAM data, there is usually a special mode and security feature incorporated into the serial access protocol.
- Umbilical-to-ECU
  In this case the investigator is connected directly to the ECU using a cable, and this method incorporates the security feature. This method is not forensically sound because the data in the ECU can be changed if the ECU recognizes an incompatible environment, and it can also wipe the data.
- Umbilical-to-EPROM
  Using this method the investigator makes a direct connection to the printed circuit board (PCB) within the EDR assembly. This method requires the disassembly of the ECU to gain access to the printed circuit board (PCB), cleaning the contacts for the EPROM with solvent and operates by using a direct connection of the EPROM device. Using this process, it is possible to retrieve the raw binary data in hexadecimal format. This process is much more time-consuming than methods mentioned above, but the plus side is that using this method the investigator can overcome the serial security access control by avoiding it completely. Now the actual raw NVRAM binary data is recovered in hexadecimal format [6].

B. Recovering data from a vehicle infotainment system

The data that can be recovered from the vehicles infotainment system is the most useful data for an investigator. The reason why is that the car's computer system stores the information about all the devices that were connected to the vehicle, and the data from their memory such as contacts, emails, call records, application data, GPS locations and more. Even the changes in some sensors like open/closed doors, gear shifts, force of acceleration and breaking are being stored to the cars computer system. Using this data, the investigator can easily place a suspect to a car at a specific place, time, and date only by looking at connected smartphone devices via Bluetooth and other activities logged through the vehicle's infotainment system. For the process of acquiring data from the vehicle infotainment system, the "Berla iVe" forensic software and the forensic toolkit that comes with the software is used. After that, the first step is to disassemble the vehicle to gain access to the vehicles infotainment system. This can be done easily because the previously mentioned software (iVe) is equipped with detailed instructions. After the disassembly is finished and the investigator gains access to the infotainment system, starts the process of connecting the infotainment system or the vehicle's hard drive (which depends on the vehicle) to the forensic station. Before the extraction starts, it can be required to open the infotainment housing to gain access to the PCB where the specific pads covered with insulating material are located (by following the instructions from the iVe software and using a specific fiberglass brush). After the contact pads are exposed, it is required to connect the iVe "Device interface board" (DIB) to the PCB and align it properly on the exposed pads. The next step is to power the PCB with the variable power supply that is included in the kit. It is very important to adjust the voltage to 12V prior to connecting the leads to the PCB power connector.

If the infotainment system has a hard drive built in and the investigator has extracted it, the hard drive needs to be connected to the iVe tool to be mounted because it is encrypted and cannot be mounted, examined or imaged otherwise.

The iVe tool has a built-in acquisition wizard that goes through the setup of the acquisition process to make sure everything is set up properly. When the iVe DIB is connected to the forensic station and the infotainment PCB, the connection has to be tested through the acquisition wizard by pressing the "Detect" and "Test" buttons shown in figure 3. The next step is to start the logical image extraction from the human machine interface (HMI) module. After the extraction is completed, the analysis can be performed. iVe's data export functionality supports CSV, tab-delimited, and KML file formats for GPS data. Reports can be exported in HTML or PDF format.

During the investigation, the investigator can come across all kinds of data from the connected smart devices. Fortunately, iVe forensic tool has functionality to search through system folders of the infotainment system, content (applications, connections, devices, events, navigation), search tab, and the timeline which includes filters that enable the investigator to visually show the results and connections to the suspect. In the figure 4 is an example of the GPS positions that were recorded during the use of the car. Every circle in the figure represents a GPS location that contains some events of opening/closing the doors, engine state, gear change (from drive to reverse). Figure 5 shows details about the devices that were connected to the vehicle [7] [8].

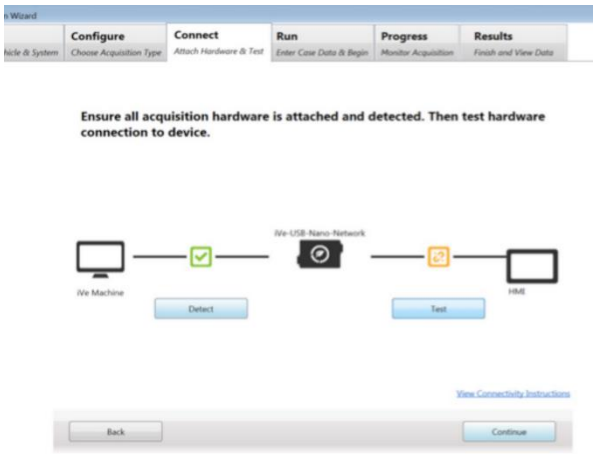

Figure 3. iVe Acquisition wizard [7]

Figure 4. iVe analysis (GPS tracking)

Flags	Device Name	Device Type(int)	Device Type	Unique Number	Unique Number Type	Manufacturer	Model	InterfaceTyp
	BLACKBERRY-1ED2			A4E4B86C5A5B	Bluetooth Address	BlackBerry Limited, MAC-> Blackber	RIM BlackBerry Device	Bluetooth
	Davyytona			80C5E6F4FC71	Bluetooth Address	MAC-> Microsof		Bluetooth
	Galaxy A5 (2016)			D8C4E9E557D8	Bluetooth Address	samsung, MAC-> SamsungE	SM-A510F	Bluetooth
	Galaxy J5			BC54510D53A9	Bluetooth Address	samsung, MAC-> SamsungE	SM-J530F	Bluetooth
	Honor 8 Black			5001D93D5B76	Bluetooth Address	HUAWEI, MAC-> HuaweiTe	FRD-L09	Bluetooth
	iPhone od Katarina			8C8EF2100F67	Bluetooth Address	"Apple Inc.", MAC-> Apple	iPhone8,1	Bluetooth
	iPhone od tpapac			285AEB878F5D	Bluetooth Address	"Apple Inc.", MAC-> Apple	iPhone7,2	Bluetooth
	iPhone od tpapac			Device_ID_8				Bluetooth Au
	iPhone od tpapac			Device_ID_1003				Bluetooth
	iPhone od tpapac			Device_ID_1007				Bluetooth
	Mobile_Device_1_BT			Mobile_Device_1_BT				
	SM-G950F			ce051715e125903403	Serial Number	SAMSUNG	SAMSUNG_Android	USB

Figure 5. iVe analysis (connected devices via Bluetooth)

VI. CONCLUSION

In today's modern world the digitalization of everyday things is growing more and more. This effect did not bypass the car industry. Modern cars are getting more digitalized, with every new model a new feature or upgrade of the previous infotainment or security system is added to make the everyday traveling and commuting safer and easier for users or drivers. Because of this, the cars are having more and more code that keeps all the added functionality running, which ultimately gives room for errors, and security oversight that hackers can use in malicious ways. Therefore, the branch of digital forensics of vehicles has developed in these pasts few years. But the main reason is not only to recover the hacker attacks on cars - car forensic is mainly used to solve crimes by connecting the criminals or the suspects to crimes committed while using a car. Extracting data from embedded car systems is done because it contains security logs of the vehicle moments before an accident happened. There is also the data from the infotainment systems that is more interesting for car forensic in cases different than traffic disputes. That is because it contains all kind of data and logs from the vehicle and devices that the vehicle was connected to. Ultimately, the car is one of the best sources of information or digital evidence today. And can be very useful if the forensic investigator knows the where to look for evidence and is familiar with the methods for data acquisition from a vehicle.

REFERENCES

[1] P. L. Prospero Sanchez, D. P. Franco, A. Feliz Dants, Car hacking and forensics, eForensics magazine, volume 05, July 2016, Pages 24-43

[2] Hack proof your smart car: 12 ways to protect your vehicle (2015, December 7), Retrieved from gearbrain: https://www.gearbrain.com/hack-proof-your-smart-car-12-ways-to-protect-your-vehicle-1622025156.html

[3] K-line-ISO 9141 (2019), Retrieved from softing: https://automotive.softing.com/en/standards/bus-systems/k-line-iso-9141.html

[4] SAE J1850 (2019), Retrieved from softing: https://automotive.softing.com/en/standards/bus-systems/sae-j1850.html

[5] J. Lacroix, Vehicular Infotainment Forensics: Collecting Data and Putting It into Perspective (2016). Retrieved from: https://ir.library.dc-uoit.ca/bitstream/10155/821/1/Lacroix_Jesse.pdf

[6] M.M. Houck, Forensic engineering, 2017, Pages 104-107. Retrieved from Google books: https://books.google.hr/books?id=EIPDDgAAQBAJ&pg=PA104&lpg=PA104&dq=umbilical-to-ECU&source=bl&ots=clN6V8sy7_&sig=ACfU3U3HzP9g4GekjoXDl1N6uBEngRNzgw&hl=hr&sa=X&ved=2ahUKEwj8zMvL1ZDgAhWJx4UKHUjAA2kQ6AEwAHoECAQQAQ#v=onepage&q=umbilical-to-ECU&f=false

[7] Digital Forensics - Automotive Infotainment and Telematics Systems (2017, May 1). Retrieved from SansDFIR: https://digital-forensics.sans.org/blog/2017/05/01/digital-forensics-automotive-infotainment-and-telematics-systems-2/

[8] Fortuna, Digital forensics on automotive infotainment systems, (2017, May 5). Retrieved from So Long, and Thanks for All the Fish: https://www.andreafortuna.org/cybersecurity/digital-forensics-on-automotive-infotainment-systems/

[9] W. Rosenbluth, Collecting EDR Data for Crash Investigations, (2010, June). Retrieved from ForensicsMag: https://www.forensicmag.com/article/2010/06/collecting-edr-data-crash-investigations

[10] Crash Data Retrieval (CDR) Tool (2013, January 14). Retrieved from Vehicle services pros: https://www.vehicleservicepros.com/in-the-bay/diagnostic-repair-info/diagnostic-test-equipment/product/10852860/bosch-diagnostics-crash-data-retrieval-cdr-tool

[11] Arxan Technologies Sets New Standard for Rapid Mobile and Web App Protection (2018, October 04). Retrieved from Bloomberg: https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=2887779

[12] CAN - ISO 11898 (2019), Retrieved from softing: https://automotive.softing.com/en/standards/bus-systems/can-iso-11898.html