Research Repository UCD

Title	Volkswagen Car Entertainment System Forensics
Authors(s)	Jacobs, Daniel, Choo, Kim-Kwang Raymond, Le-Khac, Nhien-An, Kechadi, Tahar
Publication date	2017-08-04
Publication information	Jacobs, Daniel, Kim-Kwang Raymond Choo, Nhien-An Le-Khac, and Tahar Kechadi. "Volkswagen Car Entertainment System Forensics." IEEE, 2017.
Conference details	The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Sydney, The 11th IEEE International Conference on Big Data Science and Engineering and The 14th IEEE International Conference on Embedded Software and Systems, Sydney, Australia, 1-4 August 2017
Publisher	IEEE
Item record/more information	http://hdl.handle.net/10197/9119
Publisher's statement	© 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works
Publisher's version (DOI)	10.1109/Trustcom/BigDataSE/ICESS.2017.302

Downloaded 2023-04-07T10:52:29Z

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd_oa)

© Some rights reserved. For more information

Volkswagen Car Entertainment System Forensics

Daniel Jacobs
Police Rotterdam
The Netherlands

daanj74@gmail.com

Kim-Kwang Raymond Choo
Department of Information Systems
and Cyber Security, University of
Texas at San Antonio, San Antonio,
TX 78258, USA
raymond.choo@fulbrightmail.org

Nhien-An Le-Khac, M-T. Kechadi
School of Computer Science,
University College Dublin, Ireland
{an.lekhac, tahar.kechadi}@ucd.ie

Abstract—Vehicles are fast becoming another important source of digital evidence in a criminal investigation. Traditionally, when a vehicle is involved in a crime scene (e.g. drink driving), the investigators focus on the acquisition of DNA, fingerprints and other identifying materials, usually non digital in nature. However, modern day cars, particularly smart or driverless cars, store a wealth of digital information, such as recent destinations, favourite locations, routes, personal data such as call logs, contact lists, SMS messages, pictures, and videos. In this paper, we describe some challenges associated with vehicle data forensics, an understudied area. Next, we present our case study on forensic acquisition and data analysis of an entertainment system on a Volkswagen car.

Keywords— *Vehicle system forensics; Data acquisition; Volkswagen car forensics, RNS-510 forensics*

I. INTRODUCTION

Vehicles (also referred to as automotive) such as cars are not common sources of digital evidence traditionally. For example, in 2012, a law enforcement agency in a European country was investigating a case where a man was shot and killed. The investigators found out that one of the suspects had a rented Volkswagen Golf, and a day after the murder the car was returned to the rental company without its license plate. The individual reported that the plate was stolen in the night while he was asleep. However, the car does not have a track-and-trace system installed; hence, no digital evidence could be recovered.

With the increased digitalization of our society, smart vehicles and driverless vehicles are becoming popular. Such vehicles have digital devices (e.g. digital multimedia systems, GPS systems, and Internet connectivity) integrated or built-in. For example, a driver is able to download his/her favorite music or view the status updates from his/her friends on Facebook, etc, via the built-in Wi-Fi in the car [1]. In other words, modern-day vehicles store a range of (digital) information, driving-related data (e.g. recent destinations, favorite locations, routes), personal data (e.g. call logs, contact lists, SMS messages, pictures, and videos), and other communication data (e.g. digital content sent to and from the vehicle devices to other “Things” or nodes in a smart vehicle or city network).

Predictably, modern-day vehicles will be an important source of evidence in a digital forensic investigation, and vehicle system forensics is an emerging research area. Existing approaches typically focus on the acquisition and analysis of data from parts of selected car models (see [2], [3]), rather than taking a broad view of vehicle system forensics, such as forensic challenges and vehicle forensic artefacts. As previously discussed, there is a wealth of data of forensic interest in modern-day vehicles, and one particular contribution to knowledge would be a process or framework that can be used to guide the digital forensic investigation of vehicles.

Therefore, in this paper, we describe challenges related to vehicle system forensics. We also discuss locations of different systems in a vehicle, where user data could potentially be located. Such information would facilitate forensic acquisition. We then use a Volkswagen Golf as a case study, which is a popular car in the European market. Based on our findings, we identify the types of forensic artefacts that could be recovered from its entertainment system.

The rest of this paper is organized as follows: Section II presents related literature on digital forensics of automotive systems. We describe vehicle system forensic challenges in Section III. Our case study findings is reported in Section IV, and the conclusion is presented in Section V.

II. RELATED LITERATURE

Vehicle system forensics is an emerging area of research, possibly due to the recency of smart and driverless vehicles as well as the supporting infrastructures such as smart cities, smart nations and Internet of Things.

For example, researchers from the University of Tulsa [4] researched on the security (vulnerability identification) and forensic aspects of automotive security. They explained the fundamentals of Controller Area Network bus (CAN-bus) and how to do perform reverse engineering on the signals. A device named TIB was designed to facilitate simulation of a vehicle so that a user can attach an Engine Control Unit (ECU). TIB also has an instrument cluster and a simulated anti-lock braking system. It is not clear, however, if their device allows connection to a digital multimedia system. In addition, their device may not be compatible with ECUs due to the different standard used in U.S. and Europe.

In [5], the authors simulated a couple of attacks to the ECU in a car on the FlexRay [6] bus network. As the vehicle network is designed to achieve reliability rather than security (FlexRay protocol is a communication protocol with a cyclic redundancy check for case of transmission errors), it is not surprising that using a strong adversary in the Nilsson-Larson [7] attacker model, the in-vehicle network is demonstrated to be insecure. Specifically, the authors demonstrated that by injecting a request on the bus, they were able to switch on the emergency lights remotely.

III. VEHICLE FORENSIC CHALLENGES

In this section, we present challenges associated with vehicle system forensics. As previously discussed, modern-day vehicles can be viewed as a typical computing system with different electronic modules connected and controlled by different computing devices in the vehicle. The information is being sent over buses, which is an internal communication network that connects components inside the vehicle. This allows the components and the vehicles to interact with each other. We also remark that there are buses commonly used by different vendors like CAN-bus and there are bus protocols designed for only a couple of vendors like Vehicle Area Network (VAN; developed by the Peugeot, Citroën and Renault (PSA) group).

The typical built-in electronic modules on vehicles include the following:

- Engine Control Unit (ECU)
- Transmission Control Unit (TCU A9.30)
- Anti-lock Braking System (ABS)
- Body Control Modules (BCM A9.2)

Each module stores different data, and communicates with other modules. Normally, in digital forensics (e.g. personal computers or laptops), the investigators generally look at the physical memory and the hard drive. However, in the context of vehicle system forensics, a vehicle has many different stand-alone computing devices, working together in a network. All these stand-alone computing devices have some storage and data exchange capabilities. For example, the airbag module obtains information from the ABS system, such as vehicle speed, and state of engine. Unlike a 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 compound the above challenges. For example, to investigate a modern-day vehicle, the investigators may also have to understand the workings of 20 or more electronic modules, their configurations, and their interactions.

Based on our experience, including the first author's experience in forensically examining vehicles with the National Police Digital Forensic Investigation Unit, forensic investigators should focus on the following questions, categorized using the cloud forensics framework of Martini and Choo [8]:

1. What are the types of electronic components and devices are of interest, both built-in and stand-alone devices (e.g. Radio Navigation System, such as RNS-XXX devices), and how they can be recovered forensically?
2. What types of personal information (e.g. call histories, and social medial data) are stored in vehicles, how they are stored?
3. What are the supporting infrastructure, in the sense that whether there are additional sources of evidence (e.g. smart traffic lights and CCTVs in a smart city/nation)? How vehicles interact with the supporting infrastructure, what types of data are stored, where are these data stored, and how can these data be recovered?

Once the potential sources of evidence have been identified, we will need to determine how to forensically recover the data. For example, can we reliably recover the data using the vehicle's gateway via the OBDII connector [9], or do we have to remove the module from the vehicle? In the latter scenario, forensic investigators are likely to have to work with individuals with the right expertise (e.g. vehicle technicians) to remove the module, without damaging the module and/or corrupting the data. Questions such as:

1. What are the implications of a power loss for the data stored on the device?
2. Are the data stored on RAM memory, flash, EPROM (erasable programmable read only memory), other volatile data (since removing the battery connectors off such a module can have dire consequences for the volatile data), removable storage devices (e.g. USB), etc.?

Similar to cloud forensics a few years ago [8], [10], there is lack of guidelines and frameworks relating to the digital investigation of a vehicle. Thus, pressing challenges for vehicle system forensics also include:

1. Can we design a forensically sound approach to conduct digital investigation of a vehicle?
2. Do we have tools that can be used to forensically recover evidence from the vehicle and the various modules (or components)?
3. Do we have tools that can be used to forensically recover evidence from the supporting infrastructure and the various components (e.g. nodes or "Things" in the smart city/nation architecture)?

Vehicle system forensic challenges in some ways are similar to CCTV forensic challenges [11] in the sense that obtaining proprietary information from the manufacturers of

the different vehicle parts can be impossible (e.g. due to intellectual property concerns) since a vehicle is generally assembled using parts from many suppliers, and located in different countries. There is also the consideration for reputational and legal risks for sharing of information. For example, by sharing information about the internal workings of the modules, researchers may discover that the modules can be exploited to track individual drivers or discover previously unknown vulnerabilities that can be used to compromise the safety of the vehicles. These could have serious financial, legal and reputational implications on the manufacturers.

IV. CASE STUDY: FORENSIC ANALYSIS OF AN ENTERTAINMENT SYSTEM ON VOLKSWAGEN GOLF

In this section, we present our case study setup and findings. Specifically, we examined a Volkswagen Golf version 6, 2012 station wagon. This car has several modules in which digital information can be found on the ECU (also known as Engine Control Module – ECM), TCU, ABS and BCM.

A. Approaching the car

To avoid any data loss or data modification, the investigator should bear the following in mind:

- Wherever possible, the car should be parked / garaged 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-fixes¹).
- If necessary, consider using a signal jammer to avoid interference by other signals, like the GPS signal for example. The use of a signal jammer is regulated by law in some countries; hence, it is important that the forensic investigators follows the relevant legislation to ensure admissibility of evidence.
- Do not start the car, wherever possible, as some cars overwrite or change data with every turn of the ignition key. If the car has to be started, then any (potential) data modifications need to be documented and explained.
- Ensure that the navigation unit does not start up to avoid changes to information, such as timestamp and GPS-fixes.
- Locate any device (e.g. Android and iOS device, including the investigating team's devices) or vehicles nearby with its Bluetooth feature switched on, and record their Bluetooth MAC-addresses.

Unlike typical mobile device forensic investigations, it is unlikely that most law enforcement agencies will have a

¹ When a GPS device is turned on, it will take some time for the device to locate the satellite(s), which is known as the Time To First Fix (TTFF). Once the device locates sufficient satellites to set its location, we have what is known as a GPS-fix (which may be saved on the device, depending on the device configuration).

Faraday cage (i.e. designed to block any static electric signals [12]) large enough to contain a vehicle forensic cases. Thus, in this case study, an underground garage is used as the Faraday cage.

B. Car diagnostics by OBDII gateway / port

In 1988, On-Board Diagnostics (OBD) was introduced in the U.S., which refers to the car management system and the interface for reading information from different modules in the car. Cars equipped with OBD had to have a Malfunction Indicator Light (MIL) onboard. Fault codes or Diagnostic Trouble Codes (DTCs) were stored for further analysis. There was no standard for OBD parts. The OBD interface, for example, could vary between vendors. Even the location of the OBD interface could be different, and each car vendor had its own cable with its own interface. This is the reason why there are several different cables for OBD. Even the OBD codes were not standardized, and most car vendors had their own fault codes.

With the introduction of the second generation OBD, OBDII, in the 1990's, a standard was established. The OBDII hardware interface comprises a female 16 pins (2x8) J1962 connector, and in most cases this connector is situated on the driver side from the passenger seat next to the center console. Each pin in this J1962 connector has a different function. The pins 1, 3, 8, 9, 11, 12 and 13 are vendor specific and the pins 2, 4, 5, 6, 7, 10, 14, 15 and 16 always have the same (standard) function.

Originally, the OBDII gateway was designed to facilitate diagnosis (e.g. when a car had a failure), software update, etc, it also facilitate data acquisition. In other words, one of the approaches to retrieving data stored in the different modules on the car, such as the ECU is to use OBDII gateway located in the car since modern-day car generally has a data link connector.

It may be required on some occasions (e.g. when a car is damaged) to remove one or more modules from the car for forensic examination. It is advisable that the removal be attempted by a professional technician, in order to minimize the risks of damage to the module or corrupting the data.

The data acquired from the modules can be investigated with official dealer diagnostic tools, if available. In the event that such tools are not available to the investigating agency (e.g. manufacturers not willing to share their information or tool), then an appropriate third-party hard/software is required. The type of hard/software needed will depend on the kind of investigation one is performing and the nature and importance of the data.

For example, in our case study, we can use VCDS from RossTech [9] to obtain data from the different modules. VCDS is a Windows-based vehicle diagnostics software, and the version of the VCDS software package we used is 12.12.2. VCDS allows the user to know the devices present in the vehicle. It is important to note that incorrect use of VCDS may result in the corruption of the data in the modules; thus, it is strongly advised for the forensic investigators to be trained in VCDS (or other tools) prior to conducting the investigations. In

the context of the first author's workplace, a team of forensic investigators is specially trained and equipped for investigating car accidents. These investigators have the skills, know-how and hard/software to extract the information from the different modules of popular car vendors.

In this paper, we do not describe all diagnostics results in details due to page length limitations. Rather, we only present some important results.

After the automatic scan was undertaken, information such as the following can be location: (i) data and time used by the examination computer; (ii) version of VCDS; (iii) VIN/Chassis number of the car; (iv) License plate (input by user); (v) Mileage; (vi) Chassis type; (vii) modules scanned by the software; (viii) VIN number (again); and (ix) Repair order. By comparing the information the software found with the information found in the car, we can confirm whether the vehicle information was correctly displayed.

In our experiment, VCDS found 18 modules and three other modules were reported to be malfunctioned. When the program completes the module checking, it will display more information on each module. The reason for the malfunction is logged in the "frozen" frame data. In an investigation, it could be useful to determine the errors and their causes (e.g. intentional damage?).

When a RNS-XXX system is present in the car and it is installed correctly, VCDS will show the information of this unit.

C. Extracting data from a RNS-510 multimedia device

Figure 1 presents a single Radio Navigation System, RNS, type 510 [13], which has the following functions and features:

- Radio
- CD/DVD player
- Navigation
- Bluetooth phone module
- Built-in hard drive with 30 or 40 Gigabyte (GB) capacity
- Touch screen

A straightforward examination approach is to leave the unit in the car and manually go through the different menus. This allows the investigator to take a picture of every screen. When this way is used, the time and date settings are obtained from the display. There is a limitation with such an approach, namely: 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 location. Therefore, crucial data will be lost.

Another examination method is to remove the unit from the car. There is still the risk of overwriting the last GPS-fix. In our case study, we removed the RNS system from the car for further examination.

Fig. 1. RNS-510 front view.

Apart from the hard drive, data from the RNS-510 can be extracted using either JTAG or chip-off.

1) JTAG:

After the device has been removed from the car, there are two options to recover the data from the memory. The first option is to locate the JTAG connector. The JTAG connector is used for testing, debugging or any other kind of development. Circuit boards generally have a JTAG connector, and in the event that no connector is available, a connector can be attached.

To search for the JTAG connector, we used Jtagulator [14] (see Figure 2). Basically, JTAG has 5 pins, namely: Test Data In (TDI), Test Data Out (TDO), Test Clock (TCK), and Test Mode Select (TMS), and Test Reset (TRST) (optional).

Fig. 2. Jtagulator.

Once the JTAG is located, it is possible to read the data from the memory. At the time of this research, this has not been performed on a RNS-510, although this approach had been performed successfully on a RNS-310 and a RNS315 by B. van Dijk from the KLPD National Police of the Netherlands. We also remarked that JTAG has also been used in mobile device forensics, such as those reported in [15].

After the data is retrieved using JTAG, it can be read using a hex editor such as Winhex. Note that data recovered from a RNS-510 may differ from the data recover from future versions of the RNS.

2) Chip-off:

Another method is to use a chip-off or solder off. The RNS-510 has 4 memory chips, namely: two Samsung K9F1G08U0B (Figure 3), one Spansion S29AL016D90TFA01, and one AMD AM29F400BT.

Next, we will describe the forensic data from these chips.

Fig. 3. RNS-510 circuit board, side A, Samsung K9F1G08U0B chip (in red rectangle).

D. Examining data of memory chips from a RNS-510 multimedia device

Fig. 4. RNS-510 circuit board, side B, Samsung K9F1G08U0B chip (in red rectangle) and Spansion S29AL016D90TFA01 chip (in yellow rectangle)

The Samsung K9F1G08U0B is a 132MB Flash memory. The Spansion S29AL016D90TFA01 is a 2 Megabyte CMOS 3.0 Volt-only Boot Sector Flash Memory (Figure 4). The AMD AM29F400BT is a 512 Kbit CMOS 5.0 Volt-only Boot Sector Flash Memory.

We recovered the following data from these memory chips, as discussed below.

Spansion S29AL016D90TFA01: VIN / Chassis number, Hardware part number, Hardware version number, VW ECU Serial number. There are some unknown strings such as 1T0035680BX, and SW_Variant_ID3.

AMD AM29F400BT: We could not locate any software and hardware to read the data from the AMD chip.

Samsung K9F1G08U0B: We located the last GPS-fix coordinates (e.g. DP_PM_LAT = 313224715, DP_PM_LON = 33328812), and last searched addresses with coordinates. To find the last addresses stored within the data of the binary file, we searched for the following key: vdo.rns.app.nav.std.ctrls.lastdest.LastDestinationsListItem. There were also GPS coordinates corresponding to these addresses. Our examination suggested that there were no other GPS-fixes on the memory chip except for the last GPS-fix (i.e. the location where the device was turned off the last time or when the device lost the power).

Names: No name from the phonebook was located.

Phone number: No phone number from the phonebook was located, although previous examination from the first author's colleagues at KLPD National Police of the Netherlands had successfully recovered phone numbers.

E. Examining the built-in hard drive from a RNS-510 multimedia device

The latest RNS-510 model has a 45GB hard drive, at the time of this research. The RNS-510 built before 2011 had a smaller hard drive (30 GB). The hard drive is integrated within a complex system and we need to disassemble the entire system to get access to the hard drive. To extract the data from the built-in hard drive, there are two ways.

The easiest approach is to leave it in the system and connect a write-blocked device with a 2.5 inch IDE/SATA connector. The hard drive used for this experiment had an IDE connector.

Another approach is to remove the hard drive from the system, for example when there is a crashed drive.

F. Examining the built-in hard drive from a RNS-510 multimedia device

In our case study, we used FTK Imager version 3.1.4.6 to analyze the data on the hard drive and we found that it had two partitions, namely: a FAT32 and a Windows operating system with unknown file system. According to the header and signature, we determine it is a Wind River Systems DosFs 2.0 partition (Figure 5).

On the FAT32 partition, there was no information of interest from file offsets 0 to 6877051. From file offsets 6877052 to 9694207, there were only zeros. From file offsets 9694208 to 9694507, we located a piece of readable text. However, we were not able to interpret this data.

Start sectors	31,5 KB	0
Partition 1	18,7 GB	63
Partition 2	FAT... 9,2 GB	39.266.2...

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000007E00	90	90	C3	57	69	6E	64	20	52	69	76	65	72	20	53	79	AVind River Sy
000007E10	73	74	65	6D	73	20	49	6E	63	2E	2C	20	44	6F	73	46	steas Inc., DosF
000007E20	73	20	32	2E	30	20	50	61	72	74	69	74	69	6F	6E	20	s 2.0 Partition
000007E30	54	61	62	6C	65	00	00	00	00	00	00	00	00	00	00	00	Table
000007E40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Fig. 5. Hard drive partition overview.

At file offset 9767936, there was some information that appeared to be navigation map information, and specifically a Siemens AG 2.0.0 Europe map version 5.0.5 (Figure 6)

Based on this information, there is a possibility to find the navigation software on this partition. In fact, we searched for information such as places and countries, and found a piece of text that may contain the location information. In order to verify this, a quick search with Google Maps confirmed this to be a true location.

An examination of the remaining of the disk provided us with more locations from countries in Europe, which appears to be navigation cart data used by the navigation system. (Figure 7)

0009767920	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0009767936	53	49	45	4D	45	4E	53	00	00	00	00	00	00	00	00	00	00
0009767952	28	43	29	20	53	49	45	4D	45	4E	53	20	41	47	00	00	00
0009767968	32	2E	30	2E	30	00	00	00	00	00	00	00	00	00	00	00	00
0009767984	45	55	35	30	35	32	30	38	34	35	2E	38	34	00	00	00	00
0009768000	35	2E	30	2E	35	00	00	00	00	00	00	00	00	00	00	00	00
0009768016	00	00	00	00	1C	00	43	00	00	00	BF	02	00	00	8A	00	00
0009768032	20	21	25	26	28	29	2B	2C	2D	2E	2F	3A	3B	3C	3E	41	00
0009768048	C3	80	C3	81	C3	82	C3	84	C3	86	C3	83	42	43	C4	8C	00
0009768064	C3	87	44	C4	8E	45	C3	88	C3	89	C3	8A	C3	8B	C4	9A	00
0009768080	46	47	48	49	C3	8C	C3	8D	C3	8E	C3	8F	4A	4B	4C	C4	00
0009768096	B9	C4	BD	4D	4E	C3	91	C5	87	4F	C3	98	C3	92	C3	93	00
0009768112	C3	94	C3	96	C3	95	C5	90	50	51	52	C5	94	C5	98	53	00

Fig. 6. Hard drive FAT partition file.

00904b250	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00904b260	74	23	00	62	27	01	00	00	00	00	00	06	AF	F2	FF	04	00
00904b270	BD	3F	00	69	00	00	00	00	00	00	00	5B	33	33	35	38	00
00904b280	39	35	5D	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00904b290	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00904b2a0	FF	FF	FF	FF	FF	FF	BF	25	01	00	00	60	0B	76	64	AD	00
00904b2b0	F2	FF	78	BC	3F	00	13	04	00	00	F2	01	00	00	56	49	00
00904b2c0	4C	41	52	20	44	45	20	4D	55	52	54	45	44	41	00	00	00
00904b2d0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00904b2e0	00	38	21	87	02	C1	6D	23	00	78	27	01	00	00	00	00	00
00904b2f0	57	64	AD	F2	FF	8F	BD	3F	00	75	02	00	00	DB	00	00	00
00904b300	00	4E	33	30	35	00	00	00	00	00	00	00	00	00	00	00	00
00904b310	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00904b320	00	00	00	00	00	40	9B	8C	02	70	B0	23	00	78	27	01	00
00904b330	00	60	0B	76	64	AD	F2	FF	8F	BD	3F	00	75	02	00	00	00
00904b340	DE	00	00	00	56	49	4C	41	52	20	44	45	20	4D	55	52	00
00904b350	54	45	44	41	00	00	00	00	00	00	00	00	00	00	00	00	00
00904b360	00	00	00	00	00	00	00	11	9A	8C	02	6A	B0	23	00	7A	00
00904b370	27	01	00	00	00	00	67	C0	AB	F2	FF	B4	C1	3F	00	7D	00
00904b380	00	00	00	1D	02	00	00	4D	35	32	36	00	00	00	00	00	00

Fig. 7. Hard drive FAT partition file.

At first glance, the WindRiver partition did not appear to have readable data. As this was a nearly 20GB partition, we used Photorec [15] for file carving and recovered 7,431 files. Of the recovered files, 7,414 were mp3 files located in the allocated space of the partition with the title of the song, artist and album, etc. The size of these mp3 files is 13.5 GB.

Other recovered files were text files that appeared to be some kind of playlist because of the digit numbers in front of the name of the song and the artist. We found no other user related data on the hard-drive (Figure 8).

inc. - go wild - freak out (atb and tom novy anthem edit).mp3
209-dev - in the dark (mixin marc and tony svejda radio edit).mp3
210-dj sammy feat. jean-baptiste and nyah - animal (male mix).mp3
211-atb with dash berlin - apollo road.mp3
212-avicii - fade into darkness (instrumental radio mix).mp3
213-dash berlin feat. jonathan mendelsohn - better half of me.mp3
214-dennis sheperd and jonathan mendelsohn - bring me back (g and g remix edit).mp3
215-airbeat one project - airbeat army (arena edit).mp3
216-point blank - walking on air.mp3
217-kindervater feat. julia goldstern - dont stop.mp3
218-kate ryan - lovelife (mike candys radio mix).mp3
219-erick morillo and eddie thoneick feat. shawnee taylor - stronger.mp3
220-the disco boys feat. toto - hold the line.mp3
221-mats mattara feat. rockman - opera.mp3

Fig. 8. Possible mp3 playlist found on Wind River partition.

V. CONCLUSION

Vehicles are getting more complex and it is challenging for a law enforcement agency to obtain information about the design of the vehicle digital components, and their interactions which would facilitate forensic investigations.

In this paper, we described some of the challenges associated with the digital investigation of vehicle systems, such as the need for a forensically sound approach to investigate vehicles, and the need to design tools to facilitate acquisition and analysis of data from such vehicles. The challenges highlighted in this paper, hopefully, will inform future research agenda on this topic.

Using a Volkswagen car and its entertainment system as a case study, we demonstrated that data of forensic interest could be recovered from the various electronic modules, and places such as memory chips of the RNS device.

We are also extending our research into other car makes and models, such as Peugeot, Kia, and Audi. Such examinations will potentially allow the digital forensic community to be better equipped in digital investigations of vehicles.

Another potential area of research is on integrating forensic readiness in the design of future vehicles, a term coined forensic-by-design in [16][17]. This will facilitate future forensic investigations of such vehicles.

We are moreover looking at the forensic acquisition and analysis of GPS, maps, VoIP, IM apps integrated in vehicle entertainment systems by using recent techniques in [18][19][20][21].

ACKNOWLEDGEMENTS

The authors thank the five anonymous reviewers for their constructive feedback.

REFERENCES

- [1] Song J., Yang, F., Choo, K.-K. R., Zhuang, Z., Wang, L. (2017). SIFP: A Secure Installment Payment Framework for Drive-Thru Internet. *ACM Transactions on Embedded Computing Systems*, 16(2): Article No. 52.
- [2] Jessem L., El-Khatib, K., Akalu, R. (2016). Vehicular Digital Forensics: What Does My Vehicle Know About Me?. In *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*, pp. 59-66, ACM.
- [3] Daily, J.S., Singleton, N., Downing, B., Manes, G.W. (2008). Light Vehicle Event Data Recorder Forensics. In: Sobh T. (eds) *Advances in Computer and Information Sciences and Engineering*, pp. 172-177, Springer.
- [4] Daily, J., Johnson, J., & Kongs, A. (2014). Vehicle Electronic Security and "Hacking" Your Car. <http://tucrrc.utulsa.edu/Publications/SAE%20Texas%20Meeting%20On%20Car%20Hacking%2016%20Jan%202014.pdf> [last accessed 16 May 2017]
- [5] Nilsson, D. K., Larsson, U. E., Picasso, F., & Jonsson, E. (2009). *A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay*. Berlin Heidelberg: Springer-Verlag.
- [6] FlexRay Automotive Communication Bus Overview. Retrieved on May 2015 from <http://www.ni.com/white-paper/3352/en/>
- [7] Nilsson, D. K., & Larson, U. E. (2008). *Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks*. Chalmers University of Technology, Göteborg, Sweden, Department of Computer Science and Engineering. Adelaide, Australia: E-Forensics.
- [8] Martini, B., Choo, K.-K.R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9(2), pp. 71-80.
- [9] <http://theksmith.com/technology/hack-vehicle-bus-cheap-easy-part-1/> [last accessed 16 May 2017]
- [10] Quick, D., Martini, B., Choo, K.-K.R. (2013). *Cloud storage forensics*. Syngress, an Imprint of Elsevier.
- [11] Ariffin, A., Choo, K.-K. R., Yunos, Z. (2017). CCTV Forensic Readiness: A Case Study on Digital CCTV Systems. In Choo, K.-K. R. and Dehghantanha, A., editors, *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 147–162, Syngress, an Imprint of Elsevier
- [12] <https://www.faradaycages.com/forensic-research> [last accessed 16 May 2017]
- [13] <http://hackaday.com/2013/10/02/jtagulator-finds-debug-interfaces/> [last accessed 16 May 2017]
- [14] <http://www.ross-tech.com/vag-com/> [last accessed 16 May 2017]
- [15] Chanajitt, R., Viriyasitavat, W., Choo, K.-K. R. (2017). Forensic analysis and security assessment of Android m-banking apps. *Australian Journal of Forensic Sciences*, In press, <http://dx.doi.org/10.1080/00450618.2016.1182589>.
- [16] 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.
- [17] Grispos, G., Glisson, W. B., Choo, K.-K. R. (2017). Medical Cyber-Physical Systems Development: A Forensics-Driven Approach. In *Proceedings of IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE 2017)*, Philadelphia, Pennsylvania, USA, 17–19 July.
- [18] Sgaras C., Kechadi M-T., Le-Khac N-A. (2015). Forensics Acquisition and Analysis of Instant Messaging and VoIP Applications. In: Garain U., Shafait F. (eds) *Computational Forensics. Lecture Notes in Computer Science*, Vol. 8915. Springer, Cham.
- [19] Faheem M., Kechadi, M-T., Le-Khac N-A. (2015). The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends, *International Journal of Digital Crime and Forensics (IJDCF)*, Vol 7(2), pp.1-19
- [20] Le-Khac N-A., Roeloffs M., Kechadi T. (2014). Forensic Analysis of the TomTom Navigation Application. In: Peterson G., Sheno S. (eds) *Advances in Digital Forensics X. DigitalForensics 2014. IFIP Advances in Information and Communication Technology*, Vol 433. Springer, Berlin, Heidelberg
- [21] Tillekens A., Le-Khac N-A., Pham Thi TT. (2016). A Bespoke Forensics GIS Tool. In *Proceedings of 2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 15-17 Dec.