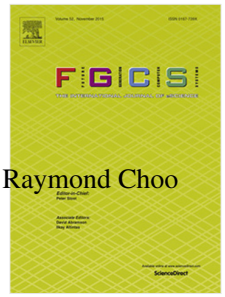
Accepted Manuscript



Smart vehicle forensics: Challenges and case study

Nhien-An Le-Khac, Daniel Jacobs, John Nijhoff, Karsten Bertens, Kim-Kwang Raymond Choo

PII: S0167-739X(17)32242-2
DOI: https://doi.org/10.1016/j.future.2018.05.081
Reference: FUTURE 4256

To appear in: *Future Generation Computer Systems*

Received date : 30 September 2017
Revised date : 18 April 2018
Accepted date : 29 May 2018

Please cite this article as: N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, K.-K.R. Choo, Smart vehicle forensics: Challenges and case study, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.05.081

Smart Vehicle Forensics: Challenges and Case Study[1]

Nhien-An Le-Khac[a], Daniel Jacobs[b], John Nijhoff[c], Karsten Bertens[c], Kim-Kwang Raymond Choo[d,e]

[a] *University College Dublin, Belfield, Dublin, Ireland*
[b] *Dutch National Police, Eenheid Rotterdam, The Netherlands*
[c] *Dutch National Police, Eenheid Oost-Brabant, The Netherlands*
[d] *Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA*
[e] *School of Information Technology & Mathematical Sciences, University of South Australia, Adelaide, SA 5095, Australia*

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) or a terrorist attack, the investigators focus on the acquisition of DNA, fingerprints and other identifying materials that are usually non digital in nature. However, modern-day cars, particularly smart or driverless cars, store a wealth of digital information, such as recent destinations, favorite locations, routes, and personal data (e.g. call logs, contact lists, SMS messages, pictures, and videos). In this paper, we describe some of the challenges associated with vehicle data forensics, which is an understudied area. Next, we present our case studies on forensic acquisition and data analysis of an entertainment system on a Volkswagen car. We also discuss potential hardware and software solutions that can be used to acquire forensic artifacts from such vehicles. Finally, we describe and analyze the mobile data traffic from an Audi car, a VW car and a BMW car.

Keywords: Vehicle system forensics; Data acquisition; Volkswagen car forensics; RNS-510 forensics

1. 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 male individual 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 who rented the car then 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 (and in this paper, 'vehicles' and 'cars' are used interchangeably) are becoming popular and commonplace. 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

[1] This is an extended version of the conference paper [35], with more than 80% new content. Certain commercial entities, equipment, or materials are identified in this paper in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the authors or the institutions they work for, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

communication data (e.g. digital content sent to and from the devices in, or part of, the vehicle, 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 broader view of vehicle system forensics. There are different forensic challenges and forensic artefacts associated with the examination of such vehicles. 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 future forensic investigation of vehicles.

Therefore, in this paper, we seek to identify the locations of different systems in a vehicle where user data could potentially be located. Such information would facilitate forensic data acquisition. We then discuss the different forensic tools required for acquisition and analysis of the vehicle's artefacts, which allows us to determine the type of evidence that could be recovered.

We 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. Finally, we describe and analyze another case study of mobile traffic of three modern-day cars (i.e. an Audi car, a VW car and a BMW car) and the relevance to a forensic investigation.

The rest of this paper is organized as follows: Section 2 presents related literature relating to digital forensics of automotive vehicle systems. Relevant forensic challenges are presented in Section 3. We discuss potential forensic tools in Section 4. Findings from the two case studies are respectively reported in Sections 5 and 6, and the conclusion is presented in Section 7.

2. 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 (IoT).

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, 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, in practice, due to the different standards 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.

When mobile data communication becomes cheaper, the top-of-the-line cars are being fitted with telemetry systems. In only a few years, both mobile data cost dropped considerably and computer penetration in cars increased. A popular connectivity device is e-call [8], [9] and from 2018, car

manufacturers are obligated to offer an automatic call after a car emergency to the 112 services in Europe[2]. There are, however, concerns that e-calls can be abused, for example to track cars without their knowledge and without a legal warrant or court order [15], [16]. Clearly, strict rules are required to avoid e-call data been misused for tracking persons.

As cars today are increasingly digitalized, there is more potential for misuse of such interconnected systems, for example by exploiting vulnerabilities in such systems which may use the same standards and protocols underpinning home networks [10].

At the Usenix 2011 conference, for example, Checkoway et al presented an overview of attack interfaces of a modern-day car [11]. A research initiated by ADAC, the German automobile club, also revealed several weaknesses in BMW's ConnectedDrive [13]. The findings resulted in BMW introducing HTTPS connections to the factory, instead of plain HTTP connections. In 2015, a group of researchers documented the data a car is collecting over its drivers and passengers [14]. While the research does not indicate whether the data is sent over the mobile connection, but such data can be read by the maintenance software of the manufacturer. This is not surprising since cars are generally not designed with cyber security in mind, as evidenced by the attacks and security flaws documented on *iamthecavalry.org* [12].

From a digital forensic perspective, Shauffer [17] briefly described the way the immobilizer system works, mainly based on the General Motors Passkey systems, and how this system was replaced by the Passlock system. He also have an overview of radio frequency identifier (RFID)-based immobilizer systems and the different tools that could be used to clone or program transponder keys. In June 2016, the "Scientific Working Group on Digital Evidence" (https://www.swgde.org) published a "Best practice guide for vehicle infotainment and telematics systems"[3] for evidence preservation and evidence handling. The guide also describes the different types of data acquisition for the storage media present in the infotainment and/or telematics systems. This includes the different evidence acquisition approaches (e.g. manual, logical, file system, physical, chip-off and micro-read).

Such and Gaultier [18] presented a method to extract information of the firmware of a Volkswagen Touareg. This system, a RNS-850, runs a QNX Operating System. They were able to extract files from the QNX File System using 2 QNX utilities. Moos et al [19] studied a BMW infotainment system, and demonstrated how one can acquire data from the hard disk and analyze the QNX filesystem using different forensic tools. They described the difficulties in acquiring and analyzing the data inside the QNX filesystem. Although they found recognizable files like *.db* and *.sqlite*, these files were not able to be examined in their native format.

Al-Kuwari and Wolthusen [36] briefly reviewed existing vehicle communication systems and proposed a live forensic approach, designed to analyze passenger behaviors. However, live data forensic examination is not always feasible in real-world smart vehicle investigation as in most cases, vehicle are seized after it has been used in some criminal activities. In addition, the authors proposed modifying the car communication system. This presents a challenge to evidence integrity, and it is unlikely that a criminal will modify the system to facilitate evidence collection that can be used against him/her (i.e. self-incriminating).

Singleton et al. [37] described an approach to recover data from the event data recorder (EDR) unit via using the crash data retrieval (CDR) system. This approach only allows the retrieval of vehicle identification number (VIN), vehicle attributes, model year, etc. The authors also discovered un-interpreted data. In

---

[2] https://ec.europa.eu/jrc/en/news/saving-lives-our-roads-ensuring-112-emergency-auto-call-technology-works, last accessed April 17th, 2018.

[3] https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Vehicle%20Infotainment%20and%20Telematics%20Systems, last accessed April 17th, 2018.

addition, this approach is dependent on the CDR software and hardware developed by General Motors; thus, it is only for specific vehicle models of Ford and Chrysler.

3. 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, such as vehicle speed, and state of engine. A vehicle forensic investigator needs to consider the following:

1. Where and what information does 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 complicate forensic investigations. 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 second 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 [20]:

1. What are the types of electronic components and devices of interest, both built-in and stand-alone devices (e.g. Radio Navigation System, such as RNS-XXX devices), and how can data be forensically acquired from these electronic components and devices?
2. What types of personal information (e.g. call histories, and social medial data) are stored in the vehicles, and how are they stored?
3. What is the supporting infrastructure, for example are there additional sources of evidence that forensic investigators can rely upon (e.g. smart traffic lights and CCTVs in a smart city/nation)? How do vehicles interact with the supporting infrastructure, what types of data (e.g. due to the interactions) 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 acquire the data. For example, can we reliably acquire the data using the vehicle's gateway via the OBDII connector [21], 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. The following considerations also need to be taken into account:

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 [20], [22], the guidelines and frameworks relating to the digital investigation of a vehicle are still evolving and there are a number of pressing challenges for vehicle system forensics, such as the following:

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

Vehicle system forensic challenges are somewhat similar to CCTV forensic challenges [23], 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.

4. Existing forensic tools

Just like any other digital investigations, forensic tools are needed to conduct an investigation. A natural question is whether existing commercial and open-source forensic tools are suitable for vehicle forensic investigations. Existing commercial and open-source forensic solution market can be broadly categorized into general forensic suites and solutions (software and hardware) for a specific purpose.

4.1 General forensic tools

Popular general forensic software include Guidance Software Encase 7.x, Accessdata Forensic ToolKit 6.x, and Xways Forensic 18.x.

We will now study their effectiveness based on their filesystem support and flexibility on none-structured data like EEPROM dumps. As previously discussed, ECUs, in-vehicle infotainment systems, and others, can be a great source of evidence. Infotainment systems have varied configurations, for example some use traditional hard drives and others use flash-based storage devices. Most infotainment systems usually run specific operating system (OS). For example, BMW uses the QNX OS in their infotainment systems. Ford, Fiat, Nissan and Kia vehicles use Windows embedded automotive, and Volkswagen vehicles

mainly use the VxWorks OS. Each OS uses their own specific file system support – see Table 1.

Operating System	File system
QNX	QNX4 QNX6
Windows Embedded	FAT FAT32 User Defined File System (UDFS)
VxWorks	High Reliability File System (HRFS) FAT-based file systems (DosFS)

Table 1. Operating System with their respective supporting file systems

The next question is then whether existing forensic software can work with these specific filesystems? We will now conduct a desk-based review of these forensic software, according to information provided on the respective documentations – see Table 2.

It appears Encase 7.x only supports general file systems used in Windows embedded OS, but not support any of the filesystems within the QNX OS or the VxWorks. With the additional analysis features, Encase appears to be able to decode data from an EEPROM dump. In previous version of Encase, the bookmark function was needed to review specific hexadecimal values. With version 7, this limitation is resolved with the decode view, which is much more user-friendly. Besides the decode view, Encase also has a Transcript view. The Transcript tab displays plaintext content pulled from its non-plaintext native format.

Accessdata Forensic Toolkit does not appear to have any filesystem support for QNX or VxWorks. Although Xways appears to be the only forensic software with additional support for Unix-like/Linux-like filesystems (e.g. XFS and UFS), it does not support specific filesystems in QNX and VxWorks.

4.2 Forensic tools for vehicles

In addition to the general forensic tools discussed in Section 4.1, we can also use other tools, both software and hardware, to extract a specific type of data. For example, software that extracts Internet-related data or software can also be used to extract encrypted data.

To perform diagnostics on a vehicle, there are a number of commercial solutions available. Most of these solutions are brand specific and can be used to acquire information such as serial numbers, part numbers and error code data. The error code data (or freeze frame data) is a collection of parameters and data that are recorded in the memory of an ECU. The freeze frame data could contain information about the engine (temperature, RPM, time since start) and vehicle speed. This information can be useful in forensic investigations of car crashes, but they are not designed as a forensic tool.

At the moment, vehicle forensics is a niche market and there are only a small number of forensic tools

specific for vehicle forensics (e.g. Berla iVe and Bosch crash data retrieval system).

File system support	Encase 7.x	Access Forensics	Xways 18.x
FAT 12/16/32	x	x	x
exFAT	x	x	x
NTFS	x	x	x
EXT2/3	x	x	x
ReiserFS	x	x	x
UFS 1/2	x		x
AIX	x		
LVM8	x		
FFS	x		
Palm	x		
HFS(+)	x	x	x
CDFS	x	x	x
ISO 9660	x		x
UDF	x		x
DVD	x		
TiVo1/2	x		
ReFS		x	
VxFS (Veritas File system)		x	
TFAT			
Next3®			x
XFS			x

Table 2. Desk-based review of forensic tool support

iVe created by Berla Corporation is a software-hardware tool, designed for evidence acquisition and decoding from infotainment and telematics systems. This tool extracts information from these systems and presents them in a report structure, similar to mobile forensic tools. iVe is able to extract vehicle information like serial numbers, part numbers and VIN, as well as user related data like navigation data, information from car kits and user related events (doors open, Wi-Fi and Bluetooth connections, points-of-interest, tracklogs and previous destinations).

In addition, the tool also extracts information from synchronized phones connected with the car, like phonebooks, calls and SMS messages. As cars are increasingly equipped with Internet connectivity (like Opel Onstar wifi hotspot, BMW ConnectedDrive or Volkswagen Car-net), vehicle infotainment systems are becoming more common and are frequently paired with mobile phones. iVe is able to extract information from installed applications and Wi-Fi connections. As the number of Internet-connected increases, so will the usefulness of such vehicles as an evidence source.

iVe is also able to extract both physical and logical data from the infotainment and telematics units, via the OBD II port, USB connections inside the vehicle, and/or special diagnostics ports on the navigation system. The extraction method and analysis is proprietary; thus, it is not completely clear how they extract the information and what filesystems iVe supports. At this moment, iVe only supports a small number of European vehicles like BMW and Volkswagen. For example in BMW QNX filesystem, the tool can be used to extract logical information over the OBD II port or the USB port connected to the infotainment

system. Although it is not possible to create a physical extraction, it is possible to import a binary file into iVe. Additional research is needed to find out whether the tool supports the analysis of the QNX filesystem or it "uses" the infotainment system as a stepping stone to access the data. The support for VxWorks filesystem also appears to be work in the same way. The tool is not able to make a complete physical extraction and is not able to decode the VxWorks filesystems. According to the manufacturer, the support will increase in the future.

Another product is the Bosch crash data retrieval system. Since 2015, an EDR is mandatory for vehicles manufactured in the U.S., while this is not the case for vehicles manufactured in Europe. However, a number of manufacturers like Volvo and Toyota have install the EDR by default. An EDR installed in a vehicle stores more information in the event of a crash than the freeze frame information in ECU. The EDR stores information before, during and just after an accident. This information contains speed, brake status, seatbelt status and airbag deployment.

The Bosch crash data retrieval system is mainly used in crash investigations. It extracts data from the EDR by using the OBD II connector or a direct connection to the EDR. This tool is not built to extract and decode filesystems, and not surprisingly the tool cannot be used to extract data from immobilizers or ECUs.

We also observed at the time of this research that there is no forensic tool available on the market to extract the information from immobilizers and other electronic control modules. In other words, forensic investigators have to use general diagnostics tools or remove memory modules for analysis.

5. Case Study 1: 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.

5.1. 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-fixes).

• 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 Faraday cage (i.e. designed to block any static electric signals [24]) large enough to contain a vehicle forensic cases. Thus, in this case study, an underground garage can be used as the Faraday cage.

5.2. 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 facilitates data acquisition. In other words, one of the approaches to retrieve 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 used VCDS from RossTech [26] 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 determine 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 second author's workplace, a team of forensic investigators is specially trained and equipped to investigate car accidents. These investigators have the skills, know-how and tools to extract the information from the different modules of popular car vendors.

After the automatic scan was undertaken, investigators can retrieve the following information: (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 (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 (i.e. Auto HVAC, Cent. Elect. and CAN Gateway – see Table 3). 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.

… VCDS – Windows Based VAG/VAS Emulator VCDS Version: 12.12.2.0 (x64) Data version: 20140212 VIN: WVWZZZ1KZCM638…[4] License Plate: Mileage: 45047 Repair Order:
Chassis Type: 1K (7N0)
Scan: 01 02 03 08 09 15 16 17 19 25 42 44 46 52 61 62 72 VIN: WVWZZZ1KZCM638… **01-Engine** – Status: OK 0000 **02-Auto Trans** – Status: OK 0000 **03-ABS Brakes** – Status: OK 0000 **04-Steering Angle** – Status: OK 0000 **08-Auto HVAC** – Status: Malfunction 0010 **09-Cent. Elect.** – Status: Malfunction 0010 **15-Airbags** – Status: OK 0000 **16-Steering wheel** – Status: OK 0000 **17-Instruments** – Status: OK 0000 **19-CAN Gateway** – Status: Malfunction 0010 **25-Immobilizer** – Status: OK 0000 **42-Door Elect, Driver** – Status: OK 0000 **44-Steering Assist** – Status: OK 0000 **46-Central Conv.** – Status: OK 0000 **52-Door Elect, Pass.** – Status: OK 0000 **61-Battery Regul.** – Status: OK 0000 **62-Door, Rear Left** – Status: OK 0000 **72-Door, Rear Right** – Status: OK 0000

Table 3. OBDII diagnostic results

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

5.3. 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. Using this approach allows

[4] The VIN number and License plate could not be fully disclosed due to the privacy information

the time and date settings to be obtained from the display. 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 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.

5.3.1. 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 [26] (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).

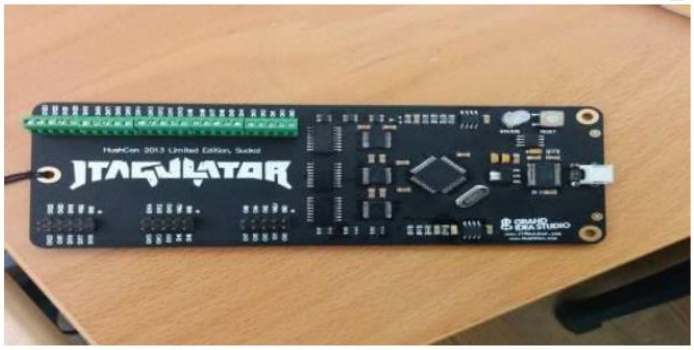


Fig. 2. Jtagulator.

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 [27].

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 recovered from future versions of the RNS.

However, this approach cannot be used if there is no JTAG connector on the device. At the time of writing, JTagulator does not support the extraction of data from RS-510. Hence, we applied the second approach: chip-off as described in Section 5.3.2.

5.3.2. Chip-off:

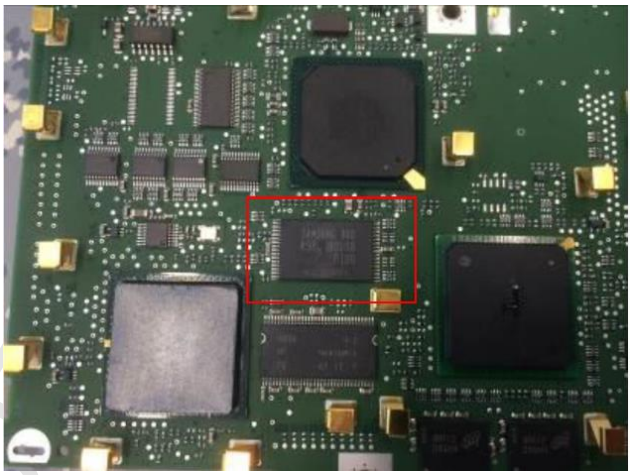


Fig. 3. RNS-510 circuit board, side A, Samsung K9F1G08U0B chip (in red rectangle).

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 acquisition from these chips.

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

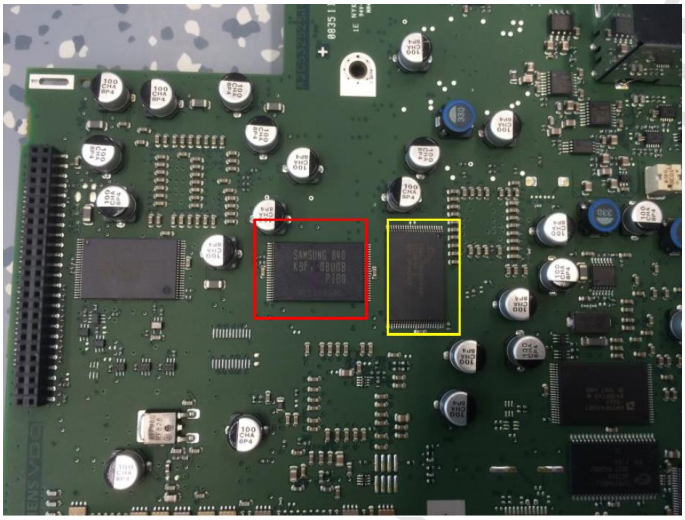


Fig. 4. RNS-510 circuit board, side B, Samsung K9F1G08U0B chip (in red rectangle) and Spansion S29AL016D90TFA01 chip (in yellow rectangle)

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.

- Spansion S29AL016D90TFA01: We were able to forensically acquire VIN / chassis number, hardware part number, hardware version number, and VW ECU serial number, as well as 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). We were not able to recover any name or phone number from the phonebook, although previous examination from the second author's colleagues at KLPD National Police of the Netherlands had successfully recovered phone numbers.

5.5. 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 (i.e. 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 connecter. The hard drive used for this experiment had an IDE connecter.

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

5.6. 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 OS with unknown filesystem. 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.

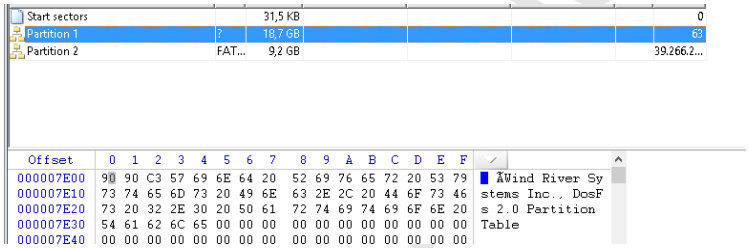


Fig. 5. Hard drive partition overview.

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)

We then 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).

At first glance, the WindRiver partition did not appear to have readable data. As this was a nearly 20GB partition, we used Photorec [28] 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).

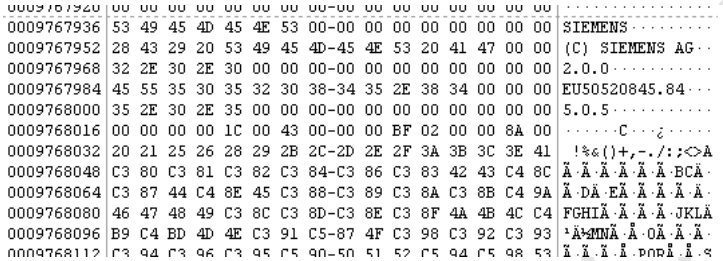


Fig. 6. Hard drive FAT partition file.

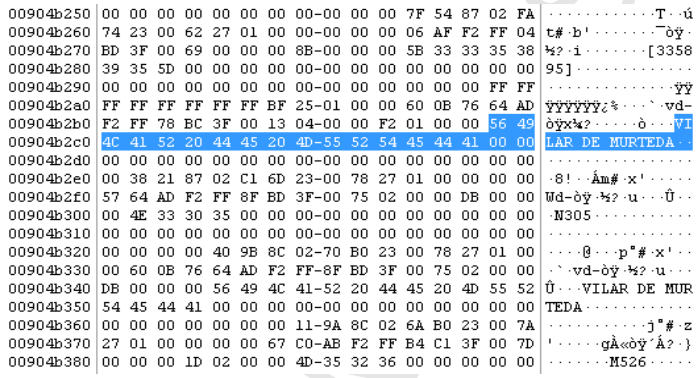


Fig. 7. Hard drive FAT partition: location.

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

6. Case Study 2: Mobile traffic data from vehicles

As mentioned above, vehicles today are more and more connected to the internet. Such connection over the Internet allows one the opportunity to intercept communication data. In our case study, we focused on

GSM/3G/4G networks. The aim of analyzing mobile traffic data is to examine the location and use of a vehicle. Normally, vehicle manufacturers would encrypt such communication data. However, metadata is generally unencrypted. We will now discuss the interception of mobile data from a car as well as potential sources of evidence. In this section, we assume that the data interception is legal (e.g. with a court order).

Depending on the jurisdiction, interception of phone calls and IP traffic may be treated differently from a legal perspective. Also, intercepting data from a car is not explicitly mentioned in most European lawful interception legislation. Since e-call will be mandatory in European cars from 2018 [38], such modules can be leveraged in data interception, lawful or unlawful. Types of data that can be intercepted include:

- PCAP data (e.g. IP data) can be trivially intercepted and viewed using tools such as Wireshark.
- Metadata that is generally unencrypted, include those described in ETSI TS 102 232-5 [n29]. For example, cell tower information is part of this metadata.
- After the period of interception, call detail records (CDR) can be requested from the service provider. Part of this data is expected to echoed those found in the metadata from the interception system. Indeed, it can be expected that the CDR will be more comprehensive. There are, however, differences between interception metadata and CDR. For example, when a crime is committed, it is possible to request CDR after the fact. However, in the case where crime was committed without the police being informed upfront, no interception data is requested. In some European countries, interception can only be requested for future data. So if at the time of the crime, no interception was in place, then such data cannot be requested. Clearly, it is not in the criminal's interest to inform / tip off law enforcement or their criminal endeavor; thus, only CDR records are available for analysis.

Location is also of great interest to investigation. For example, to physically stalk someone, the stalker has to be in close vicinity to the victim (e.g. physical observation, Wi-Fi measurements or eavesdropping are most likely within meters from a target). It may be possible to extract the exact location from the intercepted data, or triangulate the location based on the cellular tower information of the mobile network.

6.1. Findings

Now, we present our findings from the experiments on an Audi, a VW and a BMW. As the findings are similar, we will only describe the Audi's artefacts as follows:

- *CarStatus: 0\r\n* - Indicating 0 error (i.e. an error-free car).
- *Accept-Language: nl-NL\r\n*; - Indicating that the language of the car is set to Dutch, which was the case.
- *VIN: J286780\r\n* - This indicates the VIN of the car, which matches the license paper of the testing car (full VIN is not disclosed due to privacy).
- *Coordinates: 187409899/18960735/316\r\n*
  This could indicate the current location of the car.
  187409899 / 3600000 = 52,05830528 (longitude)
  18960735 / 3600000 = 5,266870833 (latitude)

The coordinates latitude 52,05830528, longitude 5,266870833 match a location in Driebergen, the Netherlands where experiments are performed.

747 10.119.57.0 2016-04-22 08:28:54.000000 keyhole.1.google.com HTTP 433
GET /flatfile?q2-0-q.687 HTTP/1.1
782 10.119.57.0 2016-04-22 08:28:55.000000 keyhole.1.google.com HTTP 436
GET /flatfile?q2-0203-q.687 HTTP/1.1
835 10.119.57.0 2016-04-22 07:23:53.000000 keyhole.1.google.com HTTP 492
GET /flatfile?q2-02030031-q.687+f1c-020-t.687+f1c-02030-t.687+f1c-0203003-
t.687&v=1 HTTP/1.1
959 10.119.57.0 2016-04-22 07:23:54.000000 keyhole.1.google.com HTTP 468
GET /flatfile?q2-020300312101-q.687+f1c-020300312-t.687&v=1 HTTP/1.1 1224
10.119.57.0 2016-04-22 07:24:47.000000 keyhole.1.google.com HTTP 556
GET /flatfile?q2-0203003121010112-q.687+q2-0203003121010113-q.687+q2-
0203003121010120-q.687+q2-0203003121010121-q.687+q2-0203003121010122-
q.687&v=1 HTTP/1.1

Figure 9. Location artefacts

Another example of location encoding is presented in Figure 9. The car navigation connects to *kh.google.com*, or *keyhole.1.google.com*, which is the Google Maps server. When Google Maps is active, the url requesting for mapping data can be identified. Arranging the numbers in ascending order reveals the following pattern:

0
020
0203
02030
0203003
02030031
020300312101
0203003121010112

First observation, all numbers are 0, 1, 2 or 3. The second observation is that each larger number appears as the start in the next number.

On the MSDN website [28], the quadtree/quadkey technology is explained. A flat projection of the earth is at the highest level (level 0) and is labelled as 0. Each level can be divided in four quarters. So level 1 consists of 4 quarters, from left to right for the top row and then from left to right for the bottom row. Each quarter again can be divided into four quarters. This is the Quadtree mechanism.

Each next level of tiles adds an extra number between 0 and 3 at the end of the above tile number. This number is a number from the quaternary numbering system, or a base 4 numbering system. This base 4 number uniquely identifies each tile in the tree, and is known as the Quad-key. If this correlation is clear and the Quad-key can be related to a tile, then the same map can be displayed as the actual map on the display of the car's navigation. This could give a street level accuracy of the location of the car.

Using http://www.maptiler.org/google-maps-coordinates-tile-bounds-projection/ (last accessed April 17, 2018), the tiles found are numbered 12020211. This matches the Bing map. Further research is suggested to find this link.

6.2. Discussion

The intercepted data from a car contain information, both data and metadata, which can provide an insight

into the lifestyle, locations and behavior of the car and the driver/owner. Potential data include typical (mobile) network data and client devices used to connect to vehicles. For example, one can potentially obtain location information from the mobile device. User behavior and patterns can also be learned by analyzing the timeline data of an interception and other open source intelligence.

Content analysis of data, particularly encrypted data, can be challenging and time consuming. Compounding the challenge is lack of documentations or the use of proprietary protocols. For example, Audi vehicles use Google Maps for navigation and this can also be determined from the HTTP requests. Map tiles seem to be downloaded in a way comparable with Bing maps, and the latter's quadtree/quadkey mechanism is publicly available. Google Maps, on the other hand, seems to use a comparable mechanism, but the information is not as well documented.

These map tiles can be centimeter accurate, but navigating could be possible with maps to a street level accuracy. Unfortunately, the translation from the http query to a Bing maps quadkey is not known at this moment. If this relation becomes clear, then navigation maps of Audi vehicle can be at a street level. In other words, a location may be retrieved to a street level accuracy. Thus, this is one potential research area.

The vehicles in our case studies could be identified uniquely by their VIN in the data; thus, it is possible to detect and identify cars in mass interception systems. The metadata from the interception system provide more detailed results than CDRs. However, due to legal constraints, in some cases only CDR records are made available to law enforcement. Hence, we should also consider gaining access to relevant activity log and GPS installed in the targeted vehicle, as well as other relevant data, to inform the investigation.

7. Conclusion

Vehicles are getting more complex and it is increasingly challenging for a forensic investigator, including those in government and law enforcement agencies, 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, an Audi, a VW and a BMW, as case studies, 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.

Future research agenda includes:

1. Extending this research to other car makes and models. Such examinations will potentially allow the digital forensic community to be better equipped in digital investigations of vehicles.
2. Another potential area of research is on integrating forensic readiness in the design of future vehicles, a term coined forensic-by-design in [29][30]. This will facilitate future forensic investigations of such vehicles.
3. Continue the research on the forensic acquisition and analysis of GPS, maps, VoIP, IM apps, and other integrated components in a vehicle, such as those described in [31][32][33][34]. Indeed, for the analyzing of mobile data from a vehicle can be automatic.
4. Research on the automated real time acquisition of target vehicle or intercept stream based on their IP or other unique information. Hence, there may be a need to design tools or interfaces that allow

live forensic investigations.

References

[1] Song J., Yang, F., Choo, K.-K. R., Zhuang, Z., Wang, L. (2017). SIPF: 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 Technologie, Götenborg, Sweden, Department of Computer Science and Engineering. Adelaide, Australia: E-Forensics.

[8] Automatic emergency call devices in all new car models from spring 2018, European Parliament press release, April 28 2015, author unknown, retrieved online from http://www.europarl.europa.eu/news/en/news-room/20150424IPR45714/ on August 11 2016

[9] Working document on data protection and privacy implications in eCall initiative, European Commison, adopted September 26 2006, author unknown, retrieved online from http://ec.europa.eu/justice/policies/privacy/docs/ wpdocs/2006/ wp125_en.pdf on August 11 2016

[10] How hackable is your car, Wired.com, August 6 2014, Andy Greenberg, retrieved online from https://www.wired.com/2014/08/car-hacking-chart/ on August 11 2016

[11] Comprehensive Experimental Analyses of Automotive Attack Surfaces , 2011, Stephen Checkowa et al, retrieved online from http://www.autosec.org/pubs/cars-usenixsec2011.pdf on August 11 2016

[12] I am the cavalry , automotive, date unknown, author unknown, retrieved online from https://www.iamthecavalry.org/domains/automotive/ on August 11 2016

[13] Beemer, Open Thyself! – Security vulnerabilities in BMW's ConnectedDrive, Heise.de, Februari 6 2015, Dieter Spaar, retrieved online from http://www.heise.de/ct/artikel/Beemer-Open- Thyself-Security-vulnerabilities-in- BMW-s-ConnectedDrive-2540957.html on August 11 2016

[14] My Car My Data, FIA, November 2015, author unknown, retrieved from http://www.fiaregion1.com/download/mycarmydata/ covering_text_for_technical_study_final.pdf on August 11 2016

[15] Briefing Note e-call, Big Brother Watch, July 2014, author unknown, retrieved online from https://www.bigbrotherwatch.org.uk/wp-content/ uploads/2014/07/Briefing-Note-eCall-PDF.pdf on August 11 2016

[16] Officer are you tracking me ?, The Sunday Times, January 26 2014, Dominic Tobin, retrieved online from http://www.thesundaytimes.co.uk/sto/ingear/ cars/article1366310.ece on August 11 2016

[17] Stauffer and Bonfanti, Forensic Investigation of Stolen-Recovered and Other Crime-Related Vehicles; Academic Press, 2006

[18] Such, Gaultier; PLAYING WITH CAR FIRMWARE; Defcon 22, 2014

[19] Moos, Davies and Lewis et al; Digital Forensics for Automobile Systems: The Challenges and a Call to Arms; International Journal of Forensic Sciences; 2016

[20] Martini, B., Choo, K.-K.R. (2012). An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), pp. 71-80.

[21] http://theksmith.com/technology/hack-vehicle-bus-cheap-easy-part-1/ [last accessed 16 May 2017]

[22] Quick, D., Martini, B., Choo, K.-K.R. (2013). Cloud storage forensics. Syngress, an Imprint of Elsevier.

[23] 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

[24] https://www.faradaycages.com/forensic-research [last accessed 16 May 2017]

[25] http://hackaday.com/2013/10/02/jtagulator-finds-debug-interfaces/ [last accessed 16 May 2017]

[26] http://www.ross-tech.com/vag-com/ [last accessed 16 May 2017]

[27] 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.

[28] Bing Tile Map System, Microsoft, date unknown, Joe Schwartz, retrieved online from https://msdn.microsoft.com/en-us/library/bb259689.aspx on August 11 2016

[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] 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.

[31] 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.

[32] 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

[33] Le-Khac N-A., Roeloffs M., Kechadi T. (2014). Forensic Analysis of the TomTom Navigation Application. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics X. DigitalForensics 2014. IFIP Advances in Information and Communication Technology, Vol 433. Springer, Berlin, Heidelberg

[34] 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.

[35] Jacobs, Daniel, Choo, K. K.-R., Tahar Kechadi, M., Le-Khac, N. (2017). Volkswagen Car Entertainment System Forensics. In Proceedings of TrustCom/BigDataSE/ICESS 2017, pp. 699-705.

[36] Saif Al-KuwariStephen D. Wolthusen (2010). On the Feasibility of Carrying Out Live Real-Time Forensics for Modern Intelligent Vehicles, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering book series (LNICST) Vol. 56, pp 207-223

[37] Singleton, N., Daily, J. and Manes, G., (2008). Automobile Event Data Recorder Forensics, in IFIP International Federation for Information Processing, Volume 285; Advances in Digital Forensics IV; Indrajit Ray, Sujeet Shenoi; (Boston: Springer), pp. 261–272.

[38] Miriam Cabo et al. (2014). Universal access to eCall system, 5th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion, Elsevier Procedia Computer Science 27 (2014) pp. 104-112

Nhien-An Le-Khac is a Lecturer at the School of Computer Science, University College Dublin , Ireland (UCD). He is currently the Director of UCD Forensic Computing and Cybercrime Investigation programme - an international programme for the law enforcement officers specializing in cybercrime investigation. He obtained his Ph.D. at the Institute National Polytechnique Grenoble, France. He has published more than 100 scientific papers in international peer-reviewed journal and conferences in related disciplines

Daniël Jacobs is a Digital Forensic Investigator at the Regional Criminal Investigations Service, Team Digital Investigations, Dutch National Police, Division Rotterdam. His research and professional interests are Automotiv (In-build infotainment systems) and Chip-off / In System Programming (ISP) / JTAG investigations on mobile phones, tablets and navigation (Tomtom, Garmin etc).

John Nijhoff is a Digital Forensic Investigator at the Regional Criminal Investigations Service, Team Digital Investigations, Dutch National Police, Division Oost-Brabant. His research and professional interests are in the IP traffic of cars.

Karsten Bertens is a Digital Forensic Investigator at the Regional Criminal Investigations Service, Team Digital Investigations, Dutch National Police, Division Oost-Brabant. Currently his interests are in Automotive and Cybercrime investigations.

Kim-Kwang Raymond Choo received the Ph.D. in Information Security from Queensland University of Technology, Australia. He holds the Cloud Technology Endowed Professorship in the Department of Information Systems and Cyber Security at the University of Texas at San Antonio. He was named one of 10 Emerging Leaders in the Innovation category of The Weekend Australian Magazine/Microsoft's Next 100 series in 2009, and the Cybersecurity Educator of the Year – APAC in 2016 (produced in cooperation with the Information Security Community on LinkedIn). In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, ESORICS 2015 Best Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian

Computer Society, an IEEE Senior Member, and an Honorary Commander of the 502nd Air Base Wing, Joint Base San Antonio-Fort Sam Houston.

Highlights

1. Automotive digital forensics
2. Smart vehicle digital forensics
3. Vehicle entertainment system forensics
4. Volkswagen car entertainment system forensics