IT-Forensic Automotive Investigations on the Example of Route Reconstruction on Automotive System and Communication Data

Tobias Hoppe, Sven Kuhlmann, Stefan Kiltz, and Jana Dittmann

Otto-von-Guericke University, Magdeburg, Germany
{tobias.hoppe,sven.tuchscheerer,stefan.kiltz,
jana.dittmann}@iti.cs.uni-magdeburg.de

Abstract. As more and more complex IT systems, modern automobiles increasingly bare safety and security risks – and have a growing relevance as sources of potentially valuable traces or evidence. But existing procedures and tools, which have proven so far in the field of IT forensics, mostly focus on desktop IT systems. However, strategies and tools for IT forensic investigations on embedded systems such as automotive IT networks increasingly come into the research focus.

Alongside a process model from an IT-forensics guideline by the German BSI, this article examines how incident investigations could be performed with a focus on automotive IT systems, e.g. to close weaknesses/vulnerabilities and increase the dependability/trustworthiness of future systems. On the example of route reconstruction in a hit-and-run scenario, appropriate strategies and tools for selected process steps are proposed. These are exemplarily illustrated by practical tests on real vehicle IT (especially CAN field bus and navigation systems) and applicable ways to route reconstruction are shown.

Keywords: Automotive security and safety interplay, automotive IT forensics, forensic process models, investigation and treatment of safety/security incidents.

1 Motivation: Automotive Incident Investigation and Applications

Compared to the broad operation of vehicles, IT forensic investigations of vehicular IT are still very uncommon. Occasionally, similar techniques are used e.g. in the context of accident reconstruction, in which – due to the growing potential of embedded automotive IT – electronic evidence sources are increasingly included. One publicly known example was the fatal accident of the Austrian politician Jörg Haider [1], where specialists of the vehicle manufacturer were involved in the subsequent investigation – mainly to reconstruct the vehicle speed right before the crash. However, routine IT forensic investigations of vehicle IT and processes compliant to the IT forensic principles constitute a still largely uncharted territory. Also in the scientific community only sporadic contributions as [2] address this young research field, to which this work should add further contributions. The spectrum of application scenarios for IT-based automotive incident investigations is broad and can exceed common accident research by far:

F. Ortmeier and P. Daniel (Eds.): SAFECOMP 2012, LNCS 7612, pp. 125–136, 2012.

- Collection of (in- or exculpatory) evidence in general litigation cases
  Already in cases where a vehicle plays no, or an only marginally relevant role in a process (e.g. burglary, assault, robbery) it might provide important digital evidence.

  In- or exculpatory evidence may already be derived from the fact, that a vehicle has been used or was turned off at the time in question – especially if provably only one person has access to it. The ability to link a vehicle with concrete identities of its drivers may be further increased in future, especially in the presence of biometric authentication systems for cars [3] (first fingerprint sensors, voice and face recognition systems are already available on the market).

  By the collection of additional, complementary information a given hypothesis can further be substantiated or disproved. For example, such data may include speed, position, seat occupation or the usage of telephone and infotainment systems.

- Investigation of incidents on the vehicle as a target of electronic manipulation
  Also recognition and processing of electronic tampering with the vehicle itself, especially with the IT embedded in it, is of increasing relevance. A broad range of electronic manipulation can already be observed in practice. In 2011, the study [4] showed that the vehicle owners (or drivers) themselves are the driving force behind most current cases of electronic tampering with vehicle and infrastructure systems. Usually these persons strive to optimise features/functionality of the vehicle. Because they usually do not know about the complex dependencies and interactions in the overall system, they consequently hazard unintended consequences of their manipulations in many cases (which can range from simple malfunctions up to severe hazards).

  Additionally, further attack scenarios can be expected in the future, potentially causing severe damage. The study [4] also shows that, in face of the increasingly introduced wireless interfaces, also attack scenarios might gain future importance, which are initiated by external attackers following intended, malicious motivations. Consequently, investigations on vehicular IT should also consider external attackers and their preferred strategies (e.g. non-physical system access via injection of malicious software) as potential initiators of investigated incidents – as it is already common for IT forensics in the desktop domain.

Scenario „hit-and-run suspect“: As an application example for an IT forensic investigation in the automotive domain the following scenario is referenced in this article (mainly for the practical illustrations of the forensic procedures in section 3): *After an accident with bodily injury the responsible driver of a green medium-class vehicle committed hit-and-run. Since no eyewitness remembers the licence plate number, the law enforcement agency performs a broad investigation of corresponding vehicles in the local district. While only one car fulfils the reported criteria, its owner asserts his innocence – but cannot provide an alibi for the time in question. He admits that he was driving the car at that time, but since he was passing through a different district he was sure not to be the person responsible for the investigated incident. His vehicle is equipped with a modern, integrated navigation system, attached to the internal vehicular CAN bus network, and a CAN bus data logger. On request by the investigating law enforcement agency he gives his consent for a detailed analysis with the aim of a route reconstruction.*

This article is structured as follows: Section 2 introduces an IT forensic process model (being used in the later parts) and selected approaches from prior research, which could be integrated in future cars as strategic preparation measures and this way serve as additional data sources. Section 3 starts with a conceptual overview over the application of the different phases of the introduced process model during investigations on automotive IT systems. Afterwards, the automotive application of selected IT-forensic process steps is illustrated by presenting results from practical test setups. For the hit-and-run scenario introduced above, this section shows, which findings can be gained from automotive IT systems (in this case especially from integrated navigation systems and CAN field buses) for route reconstruction purposes. Section 4 closes with a summary and an outlook.

2 Basics

This section provides relevant basics from the IT forensics domain as well as an overview on the spectrum of research on automotive IT security.

2.1 Process Model for IT Forensics

In IT forensics the usage of IT forensic models is an appropriate way to support methodical procedures and completeness of all acquired and subsequently analysed data. In many cases such models follow a distinction of different phases – which means that correlating activities are grouped in a common phase. In the IT forensics domain a lot of different models currently exist. Exemplary references are the „Forensic Process“ model [5] defining four phases as well as the „Investigative Process Model “ [6], dividing the process into 12 phases. Picking up the phase approach (i.e. the grouping of contextual associated techniques and procedures), this article is based on the process model of the „BSI Leitfaden IT-Forensik“ [7], which is an IT forensics guideline issued by the German Federal Office for Information Security (“Bundesamt für Sicherheit in der Informationstechnik” / BSI). This model is further described in [8]. The rationale for that choice is the inclusion of a phase of ***Strategic Preparation (SP)***, which covers measures to be taken *ahead* of a suspected specific incident in a forensic fashion, including the inclusion in the comprehensive documentation and the chain of custody (see section 3.1). Measures from the ***Strategic Preparation (SP)*** include the logging discussed in section 2.2. Furthermore, this model defines additional classes of forensic methods and data types, which have already been reflected in the context of automotive IT systems in [9] and which could become relevant in future work. In this article, especially the model’s division into six phases is referenced (see Fig. 1), which is further described in section 3.1.

An important basic requirement for IT forensic investigations is the consequent protection of data integrity and authenticity as well as a complete documentation by maintaining a *chain of custody* for digital evidence. Especially at the acquisition of person related data additionally data confidentiality is an important aspect to protect the privacy of the affected persons. Usually, these security aspects are respected by the inclusion of cryptographic mechanisms like the application of cryptographic hash algorithms, digital signatures and encryption.

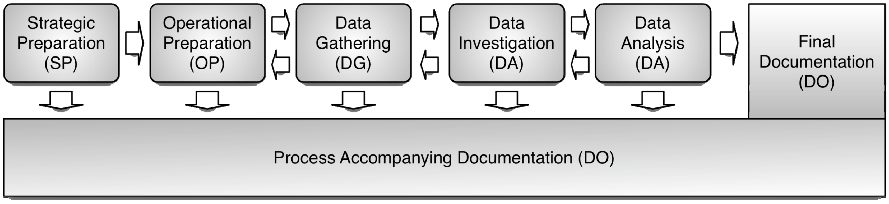

Strategic Preparation (SP)
Operational Preparation (OP)
Data Gathering (DG)
Data Investigation (DA)
Data Analysis (DA)
Final Documentation (DO)
Process Accompanying Documentation (DO)

Fig. 1. IT forensic process model modified from [7, 9]

2.2 The Spectrum of Automotive IT Security and Data Sources for IT Forensics

Motivated by the existing threats to automotive IT, which have been discussed at the beginning of this article, research activities about the application of IT security concepts to automotive IT systems and their individual characteristics are increasingly focused onto by the academic and industrial community. Especially facing the restricted maintenance and update capabilities of vehicular embedded systems, a suitable overall concept will be characterised by the fact, that – in addition to preventive measures (update verification, device authentication or tampering protection on device level) – it will also feature measures and processes of detection (recognition of indications for active attacks) and reaction (recovery to safe system states, initiation and support of incident investigations).

As in the desktop IT domain, an IT forensic investigation can profit from measures already installed before an incident (strategic preparation). Two exemplary approaches, which could serve as additional data sources for IT forensics, are:

- Permanent logging: Logs of selected information from the vehicle usage can be useful for multifaceted applications (e.g. automatic driver's logbooks or flexible insurance models). If they are recorded in a forensically sound manner, e.g. by a *forensic vehicle data recorder* [10], such log files can securely be provided to the respective users. The application cases of such a system can include the logging of information, which might be useful for the investigation of future incidents (e.g. accidents or manipulations).
- Event-triggered logging: Another type of data source could be an *automotive Intrusion-Detection-System (IDS)* [11], which monitors the operating state of automotive IT systems for potential IT security violations. Indications for respective incidents can be detected either signature- or anomaly-based, followed by an appropriate reaction [12]. While the spectrum of potential reactions can range up to active operations as a controlled stopping of the vehicle, such major interventions should only be taken in justified emergency cases based on a sufficient reliability of detection [13]. In case of less critical or only vaguely detected incidents, the IDS can also decide for the initiation or an intensification of data logging for a certain amount of time. Since also an IDS should ensure the confidentiality, integrity and authenticity of logged information, it would also be an option to connect it with a forensic vehicle data recorder (see above and [10]).

3 Concept and Illustration of Automotive Incident Investigations on the Example of a Route Reconstruction

Following the process model introduced in section 2.1, the investigation of automotive incidents (e.g. in the chosen hit-and-run scenario) should also reflect the introduced phases. This section presents a compact, conceptual overview on exemplary steps.

3.1 Overview on the Application of the Process Steps in the Automotive Context

The ***Strategic Preparation (SP)***, which is conducted *ahead* of a suspected specific incident, includes (next to the acquisition of technical specifications, wiring schemes etc.) also the provision of components supporting a subsequent forensic investigation such as forensic vehicle data or IDS components into the IT system, i.e. the car. Their installation (together with the necessary rights management and the initialisation of the cryptography key management) could be executed by the vehicle owners themselves (e.g. car fleet managers) in the medium term. However, in the long term, this installation could also be executed by car manufacturers when the acceptance rate of such components grows and the benefits are realised by the potential buyers. With the start of investigative proceedings after a suspected incident the ***Operational Preparation (OP)*** is initiated, involving the fundamental decision making about the course of action, such as the kind, extent and the manner of the gathering of volatile and non-volatile data or the set of appropriate tools. Potential incident relevant data containing traces is collected during the ***Data Gathering (DG)***, e.g. using diagnostic protocols (diagnostic trouble codes, DTC) or direct access to individual electronic control units (ECU), e.g. data that is contained in non-volatile portions such as flash memory. This data gathering needs to be executed with authenticity and integrity assuring mechanisms in place (both organisational or technical means, e.g. cryptographic algorithms). The subsequent ***Data Investigation (DI)*** involves the usage of mostly (semi-) automatic tools (e.g. to reconstruct deleted data content, extraction of timestamps etc.). In the Data Analysis (DA) those single results are put into context, involving their correlation according to time in the incident (e.g. timelining) and/or causal relationship (e.g. why-because-analysis). Each individual step of forensic proceedings starting from the Strategic Preparation (SP) is comprehensively recorded (e.g. input parameters, input data, used tool and settings, output data, environmental data) in the *process accompanying* ***Documentation (DO)***. This data and the derived information from all steps are distilled into the closing report during the *final* ***Documentation (DO)***. Some of the phases can be revisited during the forensic investigation, e.g. when results point to promising data sources not yet acquired.

3.2 Practical Illustration of Selected Process Steps

This section provides some insights to exemplary procedures, which could be performed during the execution of the single process steps. On the example of the route reconstruction application scenario introduced above, this is exemplarily illustrated for the phases Strategic Preparation (SP), Data gathering (DG) and Data Analysis (DA) using practical investigations and tests performed on real vehicular IT systems.

The navigation systems used in these tests are integrated devices for vehicles of an international manufacturer from Germany.

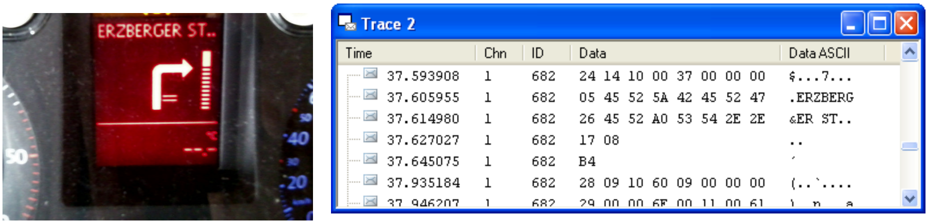
Strategic Preparation (SP)

The installation of strategic provisions as a (potentially conditional) logging function for selected information could be useful for the manufacturer himself (e.g. to support quality control and management or the processing of warranty claims) as well as for the vehicle owners (e.g. for usage in fleet management).

For scenarios as the one selected for this article, it would be useful to include geographic information into the set of proactively logged data comprising of CAN bus messages. To gather such information, components to place as strategic preparation can implement this in two different ways:

- Geographic information is already accessible in the car (e.g. if GPS coordinates are placed on the internal bus system by an existing electronic control unit)
- The respective information can (or shall) not be acquired from external devices and has to be determined by the logging device (e.g. installation of a GPS receiver in such a component)

At the same time, this choice is a compromise between costs and the reliability of the logged data.



```
Time         Chn  ID   Data                       Data ASCII
37.593908    1    682  24 14 10 00 37 00 00 00    $...7...
37.605955    1    682  05 45 52 5A 42 45 52 47    .ERZBERG
37.614980    1    682  26 45 52 A0 53 54 2E 2E    &ER ST..
37.627027    1    682  17 08                      ..
37.645075    1    682  B4                         ´
37.935184    1    682  28 09 10 60 09 00 00 00    (..`....
37.946207    1    682  29 00 00 6F 00 11 00 61    )  n   a
```

Fig. 2. Route information (street names) on the instrument cluster (left) and CAN bus (right)

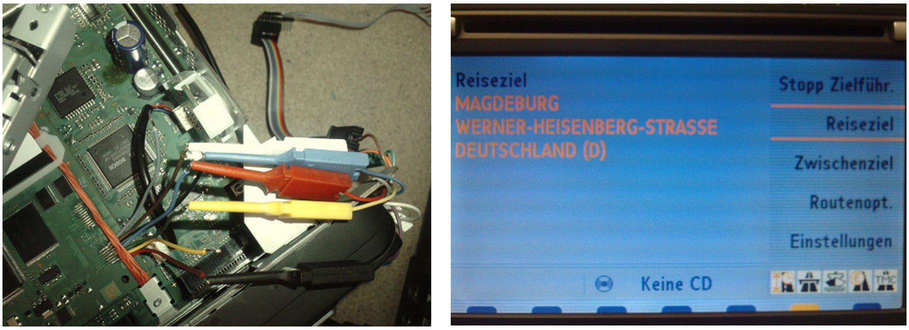
On the example of a real, integrated navigation system and its electronic integration into vehicles of a major international vehicle manufacturer from Germany, this could be implemented as follows. During operation, the navigation system displays the current route information (direction, street names etc.) also on the instrument cluster (see left part of Fig. 2). This is both for comfort and safety reasons, because this way it is visible directly in front of the driver, not distracting him from maintaining a frontal view towards the traffic. To accomplish this, respective information is transmitted over the internal vehicle CAN bus in clear text (see log excerpt in the right part of Fig. 2). A logging component placed in the context of strategic preparation (e.g. a forensic vehicle data recorder or an automotive IDS) could securely log this information (i.e. preserving confidentiality, integrity and authenticity of the log files) and enable access to it in case of future incident investigations. In the chosen hit-and-run-scenario, this data could provide significant indices for the presence or absence of the driver at the accident scene.

Data Gathering (DG)

Additionally to the data, which is collected before an incident (by measures installed as strategic preparation), further information can be acquired from other data sources after an incident – corresponding to the classical IT forensics approach.

Looking at the selected target of route reconstruction, potential evidence can be searched for on the navigation system, for example. The common approach from desktop IT forensics to perform a complete low-level block-wise image (dump) of non-volatile mass storage devices is more difficult to perform on embedded devices (due to their heterogeneous architecture, components and restricted interfaces). However, it can be tried to access such systems using debug interfaces of a controller type identified beforehand (left part of Fig. 3). Subsequently (or, at a pinch, as simplified alternative) information can be acquired using graphical user interfaces (Fig. 3, right part), while information deleted by the user can usually not be reconstructed this way. In such a scenario organisational measures (e.g. four-eyes-principle) have to ensure the authenticity and integrity of the acquired information.

The acquired data should also critically be reflected regarding their evidentiary value – since in many cases displayed information can have been manipulated by the users (e.g. the system time).



Reiseziel
MAGDEBURG
WERNER-HEISENBERG-STRASSE
DEUTSCHLAND (D)

Fig. 3. Data Gathering via debug interfaces (left side) and/or GUIs (right side)

Data Analysis (DA)

Regarding the Data Analysis (DA) phase, this section covers the analysis of (completely or selective recorded) bus communication, which can be acquired by measures of strategic preparation (e.g. a forensic vehicle data recorder or logging functions of an automotive IDS component).

Looking at the route reconstruction scenario, street names or GPS coordinates could be available in the log files (as illustrated above for the strategic preparation), which would make it a trivial case. However, even assuming that no such explicit information is available in the log files (maybe because the navigation system has not been used at the time in question) further possibilities remain for a subsequent route reconstruction. The following two subsections introduce a manual and a semi-automated approach.

Manual reconstruction based on communication logs

During a test ride in the German city of Magdeburg the CAN bus communication from the infotainment subnetwork was logged and, subsequently, evaluated.

One rudimentary approach for manual route reconstruction only requires the identification and evaluation of the speed signal. Since the semantic structure of the bus communication is usually kept secret by the manufacturers, the IT forensic personnel either has to perform their own analyses or can revert to results of respective analyses performed and published by internet communities [14]. During the manual analysis of the log file recorded in the performed test ride, an integer signal could be identified as a potential candidate for the speed signal – a continuous value between 0 and 8206. Including the known fact of an urban trip, a round scale factor of 150 can be assumed, which would correspond to a maximum speed of 54.7 km/h (In Germany, the standard urban speed limit is 50 km/h). The reconstructed velocity plot is illustrated in the upper part of Fig. 4.

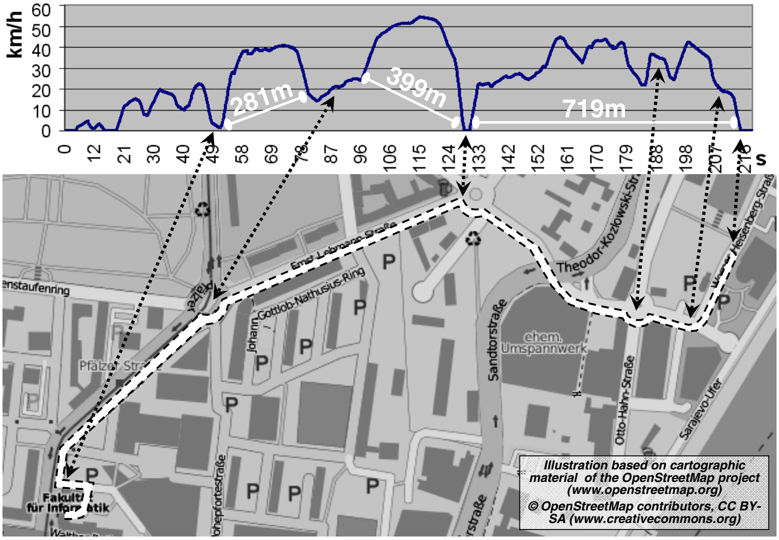


Illustration based on cartographic material of the OpenStreetMap project (www.openstreetmap.org)
© OpenStreetMap contributors, CC BY-SA (www.creativecommons.org)

Fig. 4. Manual route reconstruction based on the speed curve

If a potential position of the vehicle (especially starting or destination location) is known or can be assumed, iterative plausibility checks enable a manual route reconstruction based on the speed curve (and the covered distance, which can be determined via its integral). Fig. 4 illustrates the result of the manual route reconstruction. This practical evaluation on the logs from the test trip was done based on a known starting position.

Semi-automated route reconstruction supported by existing navigation devices

Comparable strategies for tracking vehicle positions are already implemented in some integrated navigation systems. The system data evaluated by respective algorithms usually include the vehicle's speed and, partly, steering angles or gyrometer values. With reference to the local map material, these strategies are used to correct the vehicle's position under different conditions (e.g. in tunnels or at technical GPS reception problems) as well as for the reduction of power consumption (by reducing the frequency of GPS calculations). Using this "temporary solution", some systems are even able to keep up a flawless operation for several hundreds of kilometres. This functionality already present in several devices can also be utilised by IT forensic personnel for route reconstruction purposes. To accomplish this, three main steps are required:

1. The device has to be started offline, i.e. without GPS reception and bus connection to a real car. In the lab this is usually easy to achieve by identifying and connecting the pins for power supply and ignition signal. It could also be done without dismounting it from a car by temporarily disconnecting only the vehicle bus and the GPS antenna.
2. The device has to be configured for the suspected starting position. Some devices have a dedicated system menu dialogue for this purpose, as shown in Fig. 5 (by specifying a nearby intersection, its distance and the current orientation).
3. To perform the actual route reconstruction, the device has to be provided with suitable signals (as listed above) to simulate a trip done without working GPS reception.

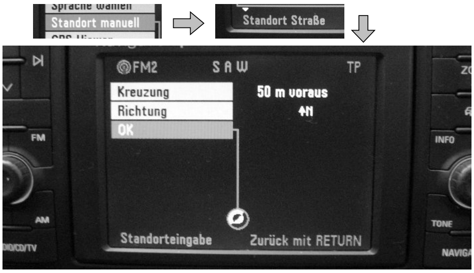


Fig. 5. Semi-automated route reconstruction – step 2 (configuring the suspected starting position)

In our test, step 3 could not be completed for the device from Fig. 5 – because this older device did not pick the speed information from the CAN bus but expects it as an analogue signal. While a D/A conversion would also be feasible with suitable hardware, digital feeding of the speed signal could successfully be implemented in a setup with a newer device shown in Fig. 6. This device uses the speed information present on the CAN bus and can be provided with respective signals (e.g. directly taken from the acquired bus communication) via a suitable bus interface. In general, a navigation system suitable for such an analysis does not necessarily have to be compatible to the bus protocol of the source vehicle. If this is not the case, it can be attempted to convert the required input values to the expected data format, temporal resolution etc.

Some snapshots from the route reconstruction (step 3) are shown in Fig. 6. As an issue of the second device we encountered that it does not evaluate the steering angle present on the infotainment CAN bus but determines the current angle with an integrated gyrometer sensor. The provision of orientation information from the outside is a bit trickier in this case. Without opening the device (e.g. to intercept the sensor connection) this could be performed by an automated rotation of the device according to the available log information (in this case: steering angle / velocity). In our setup we simply simulated this by manually turning the device.

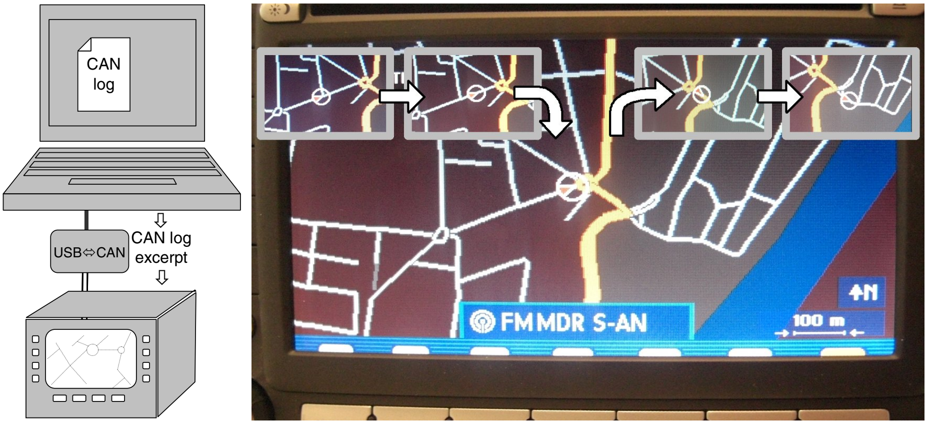


Fig. 6. Semi-automated route reconstruction – step 3: test setup and test in progress

When evaluating of the results of such a semi-automated route reconstruction, different plausibility checks should be performed to assess the likelihood, that the determined route matches the original one. Some exemplary examples for suitable criteria are:

- Is the route a realistic? This is probable, if it belongs either to the fastest or to the shortest connections between starting and destination address. It is less probable, if it contains closed circles.
- Are the speed/location mappings realistic? During the reconstruction, the “virtual” vehicle should slow down on sharp curves and stop on other points with a certain probability (e.g. STOP signs, traffic lights). In single cases it may also slow down or stop on straight road segments (e.g. due to wait for passengers or other cars) but a significantly increased amount of such events would make the assumption of the route (or, respectively, the chosen starting point) more improbable.

4 Summary and Outlook

Alongside a process model for IT forensics, this article illustrated, how IT forensic incident investigations could also be applied to automotive IT systems in a suitable and more structured way – also for investigation purposes beyond route reconstruction. Due to the increasing complexity, feature scope and connectivity, this could be increasingly essential for future automotive systems to increase their security and to reduce safety threats, which can occur as intended or unintended implications of electronic manipulations or IT-based attacks.

In the selected hit-and-run-scenario, the resulting findings would probably be suitable to support an exculpation of the determined vehicle owner. Beside such general application scenarios, automotive IT forensics bears a lot of potential for further, more vehicle-specific cases. Especially IT-based attacks targeted on the car itself might become relevant investigation scenarios in future. Electronic tampering of embedded devices or injection of forged messages into in-vehicle networks already are a daily occurrence. Recent studies revealed that still the owners/drivers themselves are the most frequent protagonists of such incidents trying to “optimise” their car. But also the relevance of third parties as initiating source of IT-based attacks on automotive systems might increase in future. Since safety and security threats can arise as (direct or indirect) implications in both cases, IT forensic investigations can help in such cases to identify and fix the exploited vulnerabilities (e.g. by providing software updates for current systems or including design fixes for future ones). This makes IT forensics an essential part in the life cycle chain to improve the dependability and trustworthiness of automotive IT systems.

Currently, the concept has still some practical boundaries, since the achievement of respective findings from current vehicles is typically a difficult task due several multifaceted restrictions. The amount of vehicular information accessible via – still mostly proprietary / manufacturer-dependent – diagnostic protocols is usually very limited. On the other hand, extraction and analyses of complete memory dumps (e.g. from flash memory) out of heterogeneous embedded devices of different manufacturers currently demand superior efforts. The alternate, comparably comfortable option of accessing potentially incident-relevant information via existing graphical user interfaces (as the GUI of the navigation system) is only possible for a small fraction of automotive systems and only has a restricted reliability (e.g. due to editing/deletion features for the users).

Future automotive incident investigations could substantially be supported by the broad introduction of logging mechanisms as vehicle data recorders, which is being demanded by many accident researchers for several years. While these have also been identified in this article as a basically suitable measure of strategic preparation, the design of such systems should place a central focus on their IT security requirements. For the IT-forensic chain of custody it is necessary to ensure integrity and authenticity of every log entry, to be able to prove its correctness at later times. Facing the increasing amount of person related (or relatable) information collected and processed by current vehicles, especially the confidentiality of log data is an essential, additional security aspect to protect the driver’s privacy.

Acknowledgements. The authors of this article would like to thank Thomas Rehse for his support and valuable input created in the context of his master thesis [15] at the Otto-von-Guericke-University of Magdeburg, Germany.

References

1. SPIEGEL Online International: Autopsy Shows Haider Was Intoxicated, Web Article from (October 15, 2008), `http://www.spiegel.de/international/europe/0,1518,584382,00.html` (last access: March 2, 2012)
2. Nilsson, D.K., Larson, U.E.: Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks. In: Networking and Telecommunications: Concepts, Methodologies, Tools and Applications, pp. 647–660. IGI Global (2010) ISBN 978-1-60566-986-1

3. Biermann, M., Hoppe, T., Dittmann, J., Vielhauer, C.: Vehicle Systems: Comfort & Security Enhancement of Face/Speech Fusion with Compensational Biometrics. In: MM&Sec 2008 - Proceedings of the Multimedia and Security Workshop 2008, Oxford, UK, September 22-23, pp. 185–194. ACM (2008) ISBN 978-1-60558-058-6
4. Dittmann, J., Hoppe, T., Kiltz, S., Tuchscheerer, T.: Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen: Gefährdungspotentiale für die Straßenverkehrssicherheit; Wirtschaftsverlag N. W. Verlag für neue Wissenschaft (2011) ISBN 978-3869181158
5. Grance, T., Kent, K., Kim, B.: Computer incident handling guide, special publication 800-61. National Institute for Standards and Technology, NIST Special Publication 800-61 (2004)
6. Casey, E.: Digital Evidence and Computer Crime. Academic Press (2004) ISBN 0-12-1631044
7. Federal Office for Information Security: Leitfaden IT-Forensik, Version 1.0.1 (March 2011), http://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/ThemenCS/IT-Forensik/it-forensik.html
8. Kiltz, S., Hoppe, T., Dittmann, J., Vielhauer, C.: Video surveillance: A new forensic model for the forensically sound retrieval of picture content off a memory dump. In: Proceedings of Informatik 2009-Digitale Multimedia-Forensik, pp. 1619–1633 (2009)
9. Kiltz, S., Hildebrandt, M., Dittmann, J.: Forensische Datenarten und -analysen in automotiven Systemen. In: Horster, P., Schartner, P. (Hrsg.) D·A·CH Security 2009, Syssec, Bochum, May 19-20 (2009) ISBN: 978-3-00027-488-6
10. Hoppe, H., Holthusen, S., Tuchscheerer, S., Kiltz, S., Dittmann, J.: Sichere Datenhaltung im Automobil am Beispiel eines Konzepts zur forensisch sicheren Datenspeicherung. In: Sicherheit 2010. LNI P, vol. 170, pp. 153–164 (2010) ISBN 978-3-88579-264-2
11. Hoppe, T., Kiltz, S., Dittmann, J.: Applying Intrusion Detection to Automotive IT – Early Insights and Remaining Challenges. Journal of Information Assurance and Security (JIAS) 4(6), 226–235 (2009) ISSN: 1554-1010
12. Hoppe, T., Exler, F., Dittmann, J.: IDS-Signaturen für automotive CAN-Netzwerke. In: Schartner, P., Taeger, J. (Hrsg.) D·A·CH Security 2011, Syssec, pp. 55–66 (2011) ISBN: 978-3-00-034960-7
13. Müter, M., Hoppe, T., Dittmann, J.: Decision Model for Automotive Intrusion Detection Systems. In: Automotive - Safety & Security 2010, pp. 103–116. Shaker Verlag, Aachen (2010) ISBN 978-3-8322-9172-3
14. Working state of a community-created CAN-ID matrix; forum discussion in the www.CANhack.de internet community,
http://www.CANhack.de/viewtopic.php?t=1017,
(last access: February 29, 2012)
15. Rehse, T.: Semantische Analyse von Navigationsgeräten und Abgleich von Daten aus dem Fahrzeugbussystem mit dem Ziel der Rekonstruktion von Fahrtrouten für den IT-forensischen Nachweis. Master thesis, Otto-von-Guericke-University of Magdeburg (2011)