


A Crime Scene Reconstruction for Digital Forensic Analysis: An SUV Case Study

Mathew Nicho, Rabdan Academy, UAE*

 <https://orcid.org/0000-0001-7129-3988>

Maha Alblooki, Zayed University, UAE

Saeed AlMutiwei, Zayed University, UAE

Christopher D. McDermott, Robert Gordon University, UK

Olufemi Ilesanmi, Robert Gordon University, UK

ABSTRACT

The abundance of digital data within modern vehicles makes digital vehicle forensics (DVF) a promising subfield of digital forensics (DF), with significant potential for investigations. In this research, the authors apply DVF methodology to a SUV, simulating a real case by extracting and analyzing the data in the period leading up to an incident to evaluate the effectiveness of DVF in solving crime. The authors employ DVF approach to extract data to reveal evidential information for judicial evaluation and verdict. This data helped determine whether the incident represented an accident or an act of crime. This simulated case and the assumptions supported by the DVF evidence provides a compelling example of how law enforcement agencies can leverage DVF to collect and present evidence to relevant authorities. This form of forensics can assist government in planning for and regulating the deployment of DVF data, the judiciary in assessing the nature and admissibility of evidence, and vehicle manufacturers in complying with the regulations relating to the harvesting and retrieval of data.

KEYWORDS

Crime Investigation, Digital Forensics, Digital Vehicle Forensics, Vehicle Control History

INTRODUCTION

Investigations of cybercrime rely increasingly on digital forensics (DF) for the gathering and presentation of evidence (Bankole et al., 2022; Garfinkel, 2010; Sunde and Dror, 2019). However, the use of evidence obtained through DF has proved to be challenging in terms of establishing that

DOI: 10.4018/IJDCF.327358

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

it is sufficiently authentic, accurate, complete, and convincing to a jury to be legally admissible (Yeboah-Ofori and Brown, 2020). Furthermore, there is a pressing need to assess the quality of the large number of commercial tools available (Talib et al., 2020). Computer and DF techniques have become popular in recent years, with the US market predicted to grow by 17% from 2016 to 2026 (GwyneddMercy University, 2021) and having grown from USD \$4.62B in 2017 to \$9.68B in 2022, an annual compound rate of almost 16% (Reedy, 2020). According to another estimate, the DF market is expected to grow at a rate of 10.97% from 2021 to 2026 in step with increased use of devices linked to the Internet of Things (IoT) and increases in government regulations and cyber-attacks (Mordor, 2022). In this respect, the expanding scope of cyber threats and attacks has expanded the need for DF (Paul Joseph and Norman, 2019). Indeed, DF has become a critical aspect of almost every criminal investigation owing to the large amount of electronic evidence that most crimes create (Arshad et al., 2018).

The targets of DF include smartphones, unmanned aerial vehicles (UAVs) or drones, automobiles, and other devices connected to the IoT. Traditionally, DF has been limited to mobile phones and computers, but, with advances in digitalization, smart cars have come on the market with fully integrated systems that hold a wealth of forensically valuable data. For instance, Tesla's Model D is digital down to its basic components, such as the electromechanical hydraulic braking system, which differs fundamentally from the mechanical brakes usually found in cars. This major transition in the automobile industry, then, is increasing the relevance of digital vehicle forensics (DVF).

In a conventional incident scenario, when a vehicle is involved in a crime or associated with a crime scene, the investigators focus on the acquisition of non-digital evidence, such as DNA, fingerprints, and other identifying materials, and do not necessarily avail themselves of the valuable retrievable data stored in modern products (Le-Khac et al., 2020). These data can pertain to routes and vehicle events, in the form of access event logs associated with such activities as opening doors and shifting gears as well as odometer and speed records and ignition cycles, and to locations, in the form of navigation information such as track logs, active routes, and previous destinations—all from devices that are connected through USB ports, Bluetooth or wireless networks, and media and communication data (Berla, 2022). A typical vehicle relies on 75 or more computer systems with 150 million or more lines of code and generates some 25 gigabytes of data hourly, and access to it can be essential for investigations to prove successful (Rak and Kopencová, 2020). DVF, also referred to as automotive forensics or car forensics, involves the rapid acquisition and analysis of digital data (or digital evidence) from motor vehicles (Bates, 2019) and the in-depth assessment of the components of vehicles to answer questions about scenarios such as accidents (Thommasone, 2021). With cars become increasingly reliant on sensors to perform everyday driving operations

The present study addresses the effectiveness of DVF as a means to recover critical evidence during criminal investigations through the use of a simulated case to arrive at the truth. With the rapid adoption of digital technologies in multiple industries, most crimes today have a digital component, and governments and police forces are usually required by law to preserve digital evidence indefinitely (Granja and Rafael, 2017). We chose a Toyota Land Cruiser SUV to observe as a case study for exploring where vehicles' data sources are located and the acquisition and analysis of the data with VF tools.

The rest of the paper is organized as follows. In section 2, we discuss the use of VF data, the challenges involved, and the observations and findings of previous researchers from multiple perspectives. We present the methodology in section 3, explaining our considerations and the forensic actions and processes that we simulated for the case scenario, the tools that we employed, and the specific sources of the data that we extracted from the vehicle. In section 4, we present the results of our experimental set-up, and in section 5 we discuss our conclusions and avenues for future research.

LITERATURE REVIEW

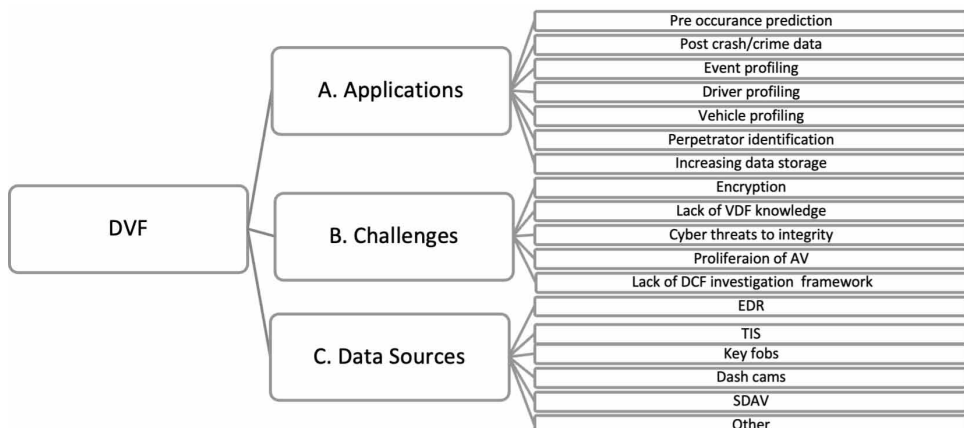
While the use of the data acquired using DVF is a promising research area for academics and practitioners, there has as yet been relatively little research since the technology is fairly recent (Bankole et al., 2022). We base this conclusion on a Google Scholar search of the titles of articles published from the beginning of 2018 through June 2022. The phrase “digital forensics” yielded 865 results but just 9 results for “vehicle forensics,” 7 for “automotive forensics,” 4 for “vehicle digital forensics,” 2 for “digital vehicle forensics,” and 1 for “car forensics.”

Application of DVF Data

DVF has proved useful for both post- and pre-event analyses. Li et al. (2021), for instance, applied a cryptographic blockchain framework that can facilitate the deterrence of terrorist activities such as the driving of a vehicle into a crowd by focusing on suspicious driving behavior by the drivers of rentals without compromising data integrity and privacy. Further demonstrating the value of vehicle data for forensic examinations, Vandiver and Anderson (2018) used the Berla iVe tool to access the event data recorder (EDR) and obtain data from Ford SG2 and SG3 modules relating to driving behavior, roads, and speeds and found their approach to be highly reliable in obtaining information after a crash or crime. Vinzenz and Eggendorfer (2019) assessed the value of the data that can be retrieved from a vehicle’s EDR regarding airbag deployment during car crash incidents using a sample of 11,000 accidents and found that these data provided insights into the particulars.

Lacroix (2016) evaluated the feasibility of DVF using a Ford vehicle, observing the types of data that can be obtained and what they can reveal about drivers’ behavior and actions. Dološ et al. (2020) used the EDR system to develop an exploratory methodology to identify the perpetrators in a hit-and-run scenario in which three drivers are involved and, based on the driving behavior of each, to assign blame. Similarly, Jacobs et al. (2017), applied forensic practices to analyze a Volkswagen Golf using the Windows-based VAG-COM diagnostic system (VCDS) and reported that they were able to extract critical data from 18 modules. Le-Khac et al. (2020) successfully extracted plain text and encrypted data (including the chassis number, hardware part number, serial number, text, locations, and audio files) from a 2012 Volkswagen Golf’s entertainment system, engine control unit (ECU), anti-lock braking system (ABS), and body control module (BCM) using a VCDS. Xing et al. (2018) ran experiments on Toyota’s autonomous emergency braking (AES) system with controlled variables, driving the car toward another vehicle and extracting the data using Bosch’s crash data retrieval (CDR) tool, and found only minor differences between the actual data and CDR recorded data.

Figure 1. Data sources and challenges encountered in the application of DVF



Challenges to the Retrieval and Use of DVF Data

Incorporating vehicle forensics into the evidence used by law enforcement is challenging. In the first place, the manufacturers of in-vehicle infotainment (IVI) systems, such as Android, Automotive Grade Linux, and Windows Embedded Automotive, focus on addressing consumers' privacy concerns by incorporating encryption mechanisms that complicate data acquisition in forensics cases (Jackson Jr., 2020).

Second, law enforcement is the primary use of vehicle forensics, and investigators tend to search for evidence to reconstruct the events that lead to accidents, whether it points to behavioral miscalculation, road rage, or a problem with the vehicle. However, according to one study, few police officers understand the process of identifying, collecting, and analyzing data extracted from a vehicle or the importance of these data for the analysis of fatal accidents (Holt and Dolliver, 2021).

Third, smart vehicle systems that rely on artificial intelligence are also susceptible to cyber-attacks, so, from a cyber-crime perspective, hackers may be able to control autonomous vehicles as if they were botnets. Thus, by exploiting a vulnerability in the controller area network protocol that is the mainly used standard in a vehicle network, a message injection attack can be launched to manipulate the ECU. From the perspective of forensics, this vulnerability threatens the integrity of potential evidence (Jeong, 2020).

Fourth, more than 21 million autonomous vehicles with advanced technological systems are expected to be on the roads by 2035 (Mearian, 2016) thanks to the efforts of car manufacturers such as Tesla and Mercedes and other companies such as Uber and Google. The novelty of the technology, rapid expansion of this part of the automotive sector, and abundance of data stored in IVI systems leave IoT-connected vehicles open to exploitation and cyberattacks that can compromise, for instance, the braking and engine systems.

Lastly, while IoT-based forensic approaches differ from conventional DF in terms of the sources of the data for analysis, there is a need to design forensically sound digital investigation guidelines and frameworks for IoT devices (Stoyanova et al., 2020). Moreover, forensic examiners need to be familiar with at least 20 electronic automobile modules as well as the challenges involved in requesting access to drivers' information from car manufacturers (Jacobs et al., 2017). Buquerin et al. (2021) proposed a framework characterized by versatility, reproducibility, and comprehensiveness to address the difficulties encountered when seeking to obtain forensics incidents in the process of DVF. To address the lack of a common framework for DVF and its complexity, Mansor et al. (2016) suggested a user-friendly mobile application called DiaLOG that facilitates data retrieval in a readily accessible format by preserving the integrity of the acquired data.

The accuracy of forensic sciences has always been a cause for concern and debate (Arshad, Jantan, & Abiodun, 2018). In DVF investigations, the multitude and diversity of recording and storage technologies employed by different vehicle brands pose a significant challenge in terms of standardization. Consequently, conducting diagnostics, examining the content of black boxes, monitoring various processes, or extracting data from Electronic Control Units (ECUs) across all brand names is not a straightforward task (Kopencova & Rak, 2020). Given that digital evidence is intricate, dispersed, volatile, and susceptible to accidental or improper modification during collection and preparation, the chain of custody becomes crucial in ensuring that the collected evidence can be deemed reliable and truthful by the court.

Due to rapid advances in technology, there is a dramatic increase in digital evidence being presented before judicial authorities (Meyers & Rogers, 2005). In legal proceedings, two major factors namely the quality, and authenticity of any evidence are critical to avoid unjustified decisions (Arshad et al., 2018). The process or procedure used in conducting the forensics investigation of a crime has a direct influence to the outcome of the investigation (Yusoff, Ismail, & Hassan, 2011). One of the challenge is to ascertain how the principles of forensic investigation can be applied so that evidence is not altered during the course of an investigation (Baig et al., 2017). When judges evaluate the scientific validity of the data collection method or reasoning in question in digital forensics, they

encounter several considerations. These include assessing the reliability of the presented evidence and considering factors such as peer review and acceptance within the scientific community (Meyers & Rogers, 2005). Hence, following correct procedures and guidelines ensures admissibility in the relevant court of law. In this regard, the digital or physical evidence presented in the forensic report should have conclusions that are reproducible by independent third parties. Additionally, any documents discovered, opinions formed, and references made should be clearly attributed to their respective sources (Garrie, 2014).

Sources of Data for DVF

The built-in electronic modules on vehicles include the ECU, transmission control unit, ABS, and BCM (Le-Khac et al., 2020). Thus, many systems and modules have types of data that can be integrated to provide evidence for DVF. For instance, the data storage capacity of Garmin vehicle navigation maps increased over time, from around 8 MB in 1998 to 256 MB in 2005 (Buquerin et al., 2021), and the navigation systems of Tesla and Audi vehicles doubled their data storage from 5 GB in 2018 to 10 GB in 2020 (Jacobs et al., 2017). Other sources of digital evidence in motor vehicles include the EDR, telematics/infotainment systems (TISs), key fobs, after-market technologies, front and rear cameras with data storage capability, self-driving and autonomous vehicle (SDAV) systems, data transmitted from vehicles and stored by manufacturers or other third parties, and data that apps store on drivers' smartphones (ABForensics, 2022).

METHODOLOGY

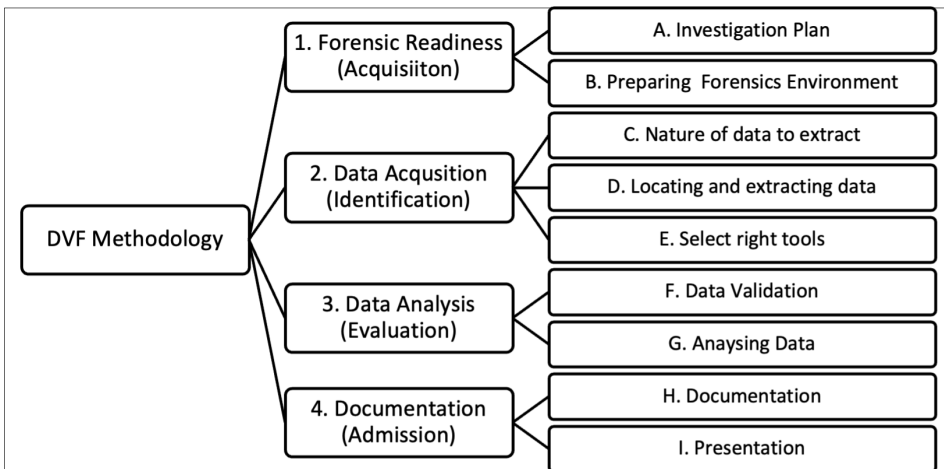
Case Scenario

To explore these issues, we created a hypothetical criminal case involving VDF in which a woman's body is recovered from an accident site on a mountain road: her SUV swerves unexpectedly while traveling uphill, crashes through a road barrier, and rolls down a slope. The medical professionals and police find the driver already dead, and the post-mortem examination of the body reveals that she died before the accident. The investigators seek evidence that can help determine whether the woman was murdered and placed in the driver's seat and the car then deliberately driven off the road to make her death appear to be a case of suicide. In such scenarios, the reliability of autopsy results and scientific forensics can be enhanced through the use of digital automotive forensics. This is particularly important in open crime scenes where assumptions may be inconclusive and time consuming.

To simulate the incident, we used a 2015 Toyota Land Cruiser SUV with 164,574 kilometers. Starting from a residential area in Dubai, we drove on the highway to the outskirts of the city and staged the crash on a sandy hill off the road after traversing some small dunes. With the SUV tilted 30 to 45 degree from its center of gravity, we abruptly stopped it, using the rollover sensor to simulate the case scenario. We also tampered with the key fobs and door to see whether evidence that these components were compromised could be extracted afterward.

In a formal DF inquiry, the investigators follow a uniform approach and a plan prepared in advance to assist courts of law in assessing the reliability of the digital evidence that they generate (Montasari, 2016). They need to access the logs of vehicles and manage the data that they contain using the appropriate tools to allow for verification and validation. Accordingly, the computer forensics investigation process consists of four phases: acquisition (the gathering of evidence), identification (the discovery of digital components and conversion of the data into a usable form), evaluation (determining the relevance of the data), and admission (presentation of the data in a court of law) (Yusoff et al., 2011). Correspondingly, the forensic process for vehicles (Figure 2) consists of four phases: forensic readiness, data acquisition, data analysis, and documentation (Buquerin et al., 2021).

Figure 2. CFIP investigation plan



Outlining an Investigation Plan

The complexity and sophistication of vehicle systems can create numerous challenges for investigators. The formulation of a sound forensic plan for analyzing a vehicle requires taking into consideration several factors at the outset of an investigation, in particular:

1. The kind of data stored in each system.
2. The type of tools that can be used to access the data while maintaining their integrity.
3. Whether live data acquisition can be performed through a port or the system needs to be dismantled to extract the data.
4. Whether loss of power in a vehicle during the extraction of data affects their availability.
5. The tools that can be deployed to analyze and interpret the data accurately.

Though most automotive system modules communicate with each other, they are distinct when it comes to data acquisition, for each stores unique data specific to the system. The airbag module, for example, receives data from the ABS, which monitors the vehicle's speed and engine status. It can be difficult to access, let alone investigate, the data from such modules since a forensic examiner must understand how multiple modules function within a given vehicle with respect to their type, configurations, and structure.

Preparing the Forensics Environment

Once the correct procedure has been used to recover a vehicle, the investigators need to assess the state of the battery, electrical circuits, and transmission of electricity to ensure that the data are available and can be extracted seamlessly. In this process, the proper forensics environment ensures data preservation. Thereafter, the vehicle must be transported or towed to an underground basement location where it will receive no signals, with the ignition remaining off to avoid potential GPS connectivity and data override. A signal jammer can be used as an extra preventive measure (Lacroix et al., 2016). Following these procedural steps helps to ensure the integrity of VDF data.

Nature of the Data to Extract

The sources of digital evidence include event data recorders (EDRs, the so-called black boxes), telematics/infotainment (T/I) systems, ECUs, eCALL units, key fobs, front and rear cameras, vehicle

control history (VCH) data, and aftermarket technologies (Kopencova and Rak, 2020). While EDRs store data from specific vehicle crash events, the VCH in Toyota vehicles records and stores certain vehicle data based on select driver inputs (Lewis et al., 2019). T/I systems store GPS locations, routes, and speed, timestamps indicating whether the engine is on or off, and data from connected cellphones, contact lists, music albums, messages, and call logs, all of which are synched to T/I systems through Bluetooth, USB cables, or Apple CarPlay. VCH, on the other hand, is a data source for car engineers and technicians seeking to understand a car's performance and access its diagnostics. The metrics and type of data in a VCH can also aid in understanding how a car accident occurs, with records of over 50 parameters being preserved once a trigger event occurs, such as activation of the AES or pre-collision system. Depending on the trigger event, the parameters recorded may include the direction of the steering wheel, brake pedal status, and forward collision sensor status. Similarly, the EDR stores parameters helpful for tracing a car collision before, during, and after the event, such as engine performance data, ABS deployment, airbag information, and seatbelt status. The requirements for the installation of a VHS depend on the region, but Toyota includes one by default in all of its vehicles (Mansor et al., 2016).

Locating and Extracting Data

All of the data categories just discussed are extracted from ECUs, which are also known as electronic control modules. Each of these small devices manages a particular function. Current cars often include 100 or more ECUs for basic functions such as the engine and power steering, heating, ventilation, and air conditioning, security operations such as door locks and keyless wireless entry, and accessories such as power windows and seats. ECUs also handle basic active safety measures, such as airbags and emergency braking (Lacroix et al., 2016).

An ECU acquires data from various parts of a vehicle depending on its function. When a passenger presses the door lock/unlock button on a car door or on a wireless key, for example, a door lock module or ECU receives the input. Likewise, crash sensors and other vehicle sensors that identify when a seat is occupied provide input to an airbag ECU, and every fastening of the seatbelt is logged with a timestamp (Jackson Jr, 2020). In addition, forward-facing radar that detects when the vehicle is approaching an object rapidly provides information to an automated emergency braking ECU.

Selecting the Right Tools

Because of the variety and diversity of vehicles, VF can be complicated. Every model of every brand utilizes distinct parts, systems, and software that, in turn, necessitate the use of tools specific to a given vehicle. A few open-source VF tools are currently available as well as commercial tools, each with distinct properties and file system compatibilities. Examples include Guidance Software Encase 7.x, AccessData Forensic Toolkit 6.x, Berla iVe, and Bosch Crash Data Retrieval (Lacroix et al., 2016). For T/I retrieval, a forensic examiner must first determine whether the system stores the data on a hard disk or flash-based storage memory and then identify the operating system (OS). For example, Nissan and Ford use Windows Embedded Automotive, which is supported by Encase 7.x, whereas BMW and Toyota use QNX (Dobromirov et al., 2017). Global Techstream (GTS) is a next-generation diagnostics tool developed by Toyota for its vehicles. Commercial tools are easier to acquire, brand-specific, and retrieve distinctive types of data, such as serial and part numbers and error code data relevant to diagnostics. Berla iVe, for example, is only commercially available for VF and is said to support data acquisition from the infotainment and telematics systems of more than 4,600 vehicle models and the presentation of it in a report structure (Whelan et al., 2018). The Bosch crash data retrieval system is often used to analyze accidents, especially in the context of insurance disputes.

Analyzing Logs

A vehicle system holds a vast amount of raw data, but, of course, only the data and files of interest are analyzed in an investigation, which usually involves determining which parties played roles in the incident and the behavior of the driver or drivers.

Validating Tools and Data

DF practitioners need to be able to identify disparate sources of evidence, test methods of extracting data in a repeatable manner, and undertake research to determine the validity of extracted data (Quick and Choo, 2018). Validation and testing ensure that the tools used in a DF process are reliable and produce valid results. The emphasis is on validation of the reliability and performance of tools rather than validation of results, with data validation and parsing ensuring that the correct types of data are recovered, all relevant types of data are taken into account, no errors occur, whether false positive or false negatives (Sunde and Horsman, 2021).

Documenting Procedures

Documentation is necessary throughout the technical and diagnostic forensic processes, being performed before, during, and after and including a record of the participating forensic examiners. The preliminary report should state a timeline of the incident, the times at which the examination starts and ends, the environmental conditions (such as the weather), and the nature of the examination site (such as whether it is outdoors or indoors), for these factors may affect the acquired data (Dobromirov et al., 2017). The integrity of data cannot be assumed simply because they are available and accessible, for a major concern during VF is whether they have been tampered with (Mansor et al., 2016). In any case, forensic examiners can follow the currently available vehicle identifiers and data preservation methods to establish a certain level of validity. First, the vehicle identification number (VIN) or chassis number must be noted as a unique identifier number, and the vehicle's odometer reading should be recorded before and after examination to ensure that the vehicle has not been driven so as to cause the overwriting of the data. Again, the type of OS, the tools used, and the methods for acquiring the data should be recorded. Moreover, hashing should be part of the verification process once the logs have been acquired since the analysis needs to be reproducible, with backups created and write blockers used to prevent accidental data modification. Lastly, the results and findings of the relevant modules and in-vehicle components and their contents should be listed and numbered.

Presentation

In the presentation phase, all of the steps throughout the investigation are explained in detail so that they are ready to be presented before the court. This phase thus involves preparing and presenting all of the evidence about a case using non-technical language as far as possible since juries cannot be expected to include individuals with the requisite expertise (Gülatas and Baktir, 2018).

RESULTS AND EXTRACTED ARTIFACTS

(Please note that, since the objective of this paper was to demonstrate the role of vehicle digital forensics using a simulated case rather than to document and present evidence to the appropriate authorities, the last two steps [documentation and presentation] were omitted from the discussion).

Investigation Plan

The 2015 Toyota Land Cruiser for our case study used the QNX OS, for which the appropriate tool was required. We selected GTS version 12.10.019, a commercial diagnostics software that provides comprehensive access to many types of data in Toyota, Lexus, and Scion vehicles. To obtain a detailed analysis of the incident, we connected the vehicle's system to a laptop through a Mini Vehicle

Communication Interface (VCI) J2534 OBDII diagnostic cable model. On-board diagnostics (OBD) systems were introduced in 1988 in California for viewing the data from car modules and in 1991 became mandatory for new vehicles (TransportPolicy, 2018). However, the standardization of OBD gateways was problematic because car vendors incorporated them in various ways with respect to the interface, cable type, placement, and even the fault codes. This problem was solved in the 1990s with the second generation, OBDII, which is now used widely for vehicle diagnostics, software updates, and data acquisition (TransportPolicy, 2018). Figures 3 and 4 show the connection in the Toyota SUV used for the simulation.

Preparing the Forensics Environment

GTS provides a graphical user interface on which a visual representation of a vehicle is displayed, labeling each of the parts diagnosed. When initialized, then, GTS opens a screen that displays the vehicle's structure clearly, with icons representing the various modules (Figure 5). From this screen, the user can extract the data from the modules or ECUs (Saufi et al., 2019).

Figure 3. Location of the Toyota OBDII port



Figure 4. The Mini-VCI J2534 cable

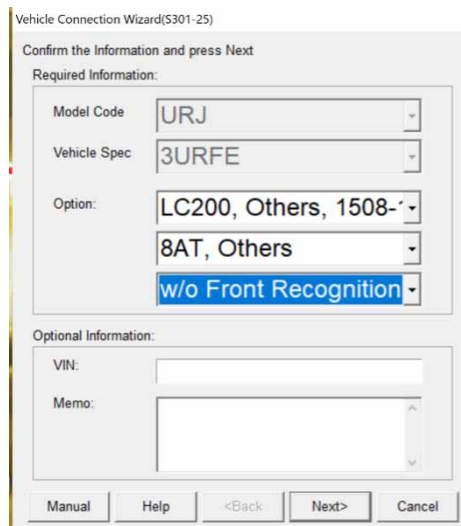


However, the startup interface of GTS varies depending on the region selected during the setup of the tool. After we connected the Toyota's OBDII port (Figure 3) to the forensics machine through the mini-VCI J2534 cable (Figure 4), we selected the *Connect to Vehicle* tab in the software, through which we were able to identify and confirm the required information about the vehicle, such as its code and spec number, before initiating the data acquisition and analysis (Figure 6).

Figure 5. The Global TechStream (GTS) startup page



Figure 6. GTS setup confirming the specifications for the connected vehicle



Nature of the Data to Extract

In this scenario, since the primary focus of the evidence collection was on the driver’s behavior patterns, we extracted the VCH and EDR data from GTS. Toyota’s VCH system can store four to five events before it begins overwriting the data when a new event occurs (Xing, 2018), and this capacity was more than adequate for our investigation. The scope of the information collected, then, was the VCH and EDR data, but we inspected all of the potentially relevant data provided by the tool. It displays 14 modules containing data that can provide useful evidence (Figure 7) so, among the modules available on GTS, a few of the logs had the potential to prove useful for the case scenario. We considered, in particular, the following logs:

- Auto Entry Warning Operation History displays warning alerts in relation to vehicle entry, including opening the car door while the ignition is off or attempting to lock the car using the handle sensor when the key is detected inside the car.
- Trunk/Back Door shows the time and date at which the back door and trunk have been opened and how (i.e., physically or remotely).
- Run Distance of Previous Trip shows the number of kilometers traveled in the vehicle’s most recent journey.
- Smart Code Registration lists the number of keys registered for the vehicle and the attempts to register a new key and enables registration of new keys.

Locating and Extracting the Data

We collected potentially valuable artifacts from the ECUs of the Toyota used in the simulation, selecting them from among the vast amount of available data on more than 40 modules (Figure 10). As expected, the selected data consisted of the four modules discussed above, Entry & Start, Main Body, Engine, and Smart Key (Figure 8).

Figure 7. Modules containing data (GTS)

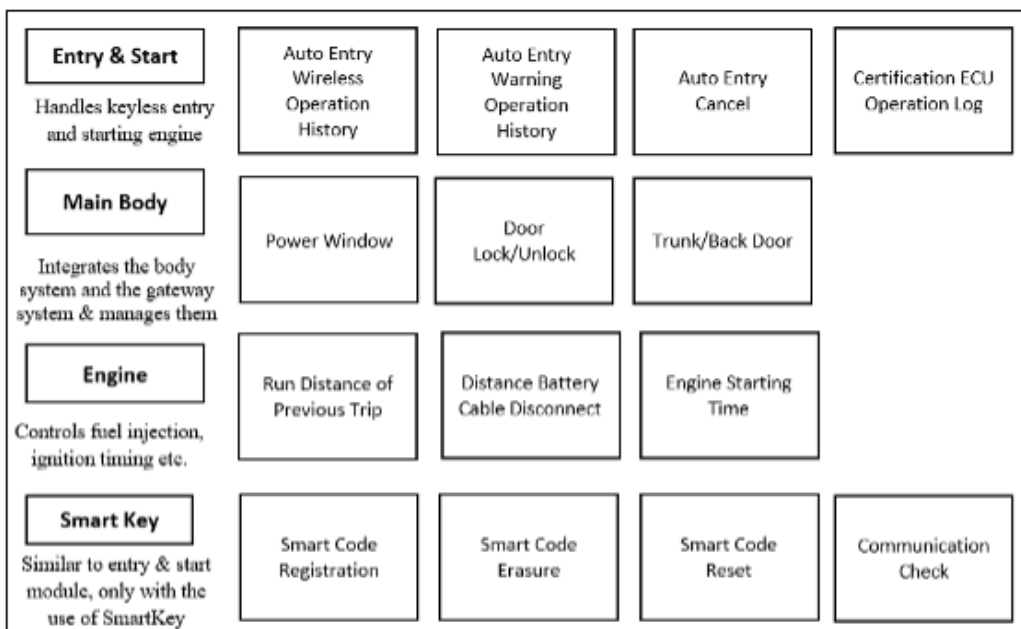
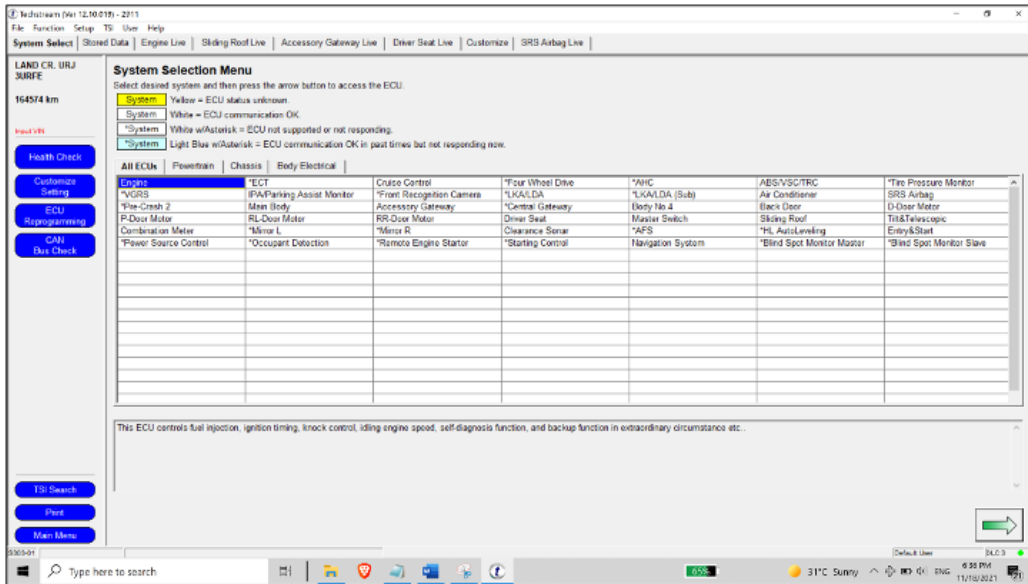


Figure 8. Selected modules from which data were extracted



Selecting the Appropriate Tools

DF relies on software applications and other computer forensics tools (Ghazinour et al., 2017). From among the many tools available on the market, we chose GTS because it is a next-generation diagnostics tool developed by and for Toyota Motor Corporation and is free to download.

Data Validation

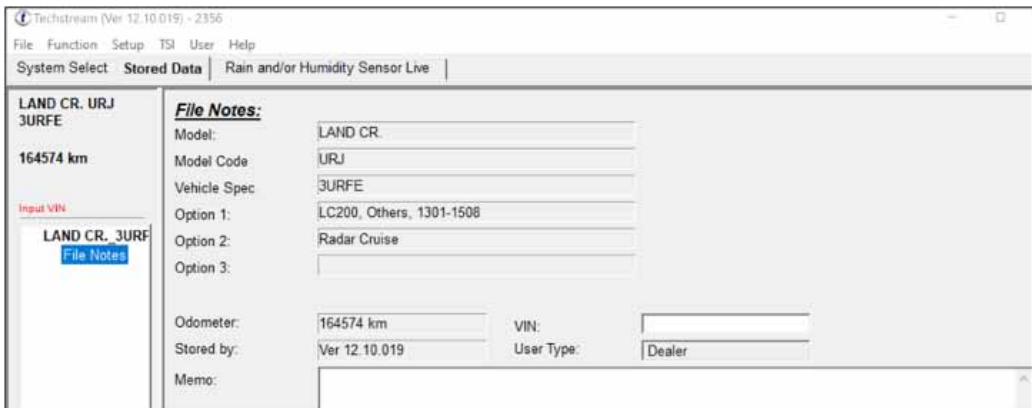
Prior to gathering the data, we performed tool validation by conducting trial runs and taking note of the VIN, engine code, model, and odometer reading. Since a unique VIN is assigned to every vehicle, this number is the most reliable means to identify vehicles from which evidence can be retrieved. Clear identification is necessary to avoid intentional and unintentional manipulation of evidence and preserve the integrity of documentation and reports. A fixed, unchanged odometer reading demonstrates sound forensic procedure and the integrity and reproducibility of the evidence for presentation in court. The following are the results from our scenario (Figure 9):

- VIN number: JTMHY05J2F4028493
- Vehicle spec: 3URFE (engine specifications V8 5.7 liters)
- Car model: LAND CR
- Model code: URJ (manufactured for the Middle East)
- Odometer reading: 164,574 km

Analysis of the Data

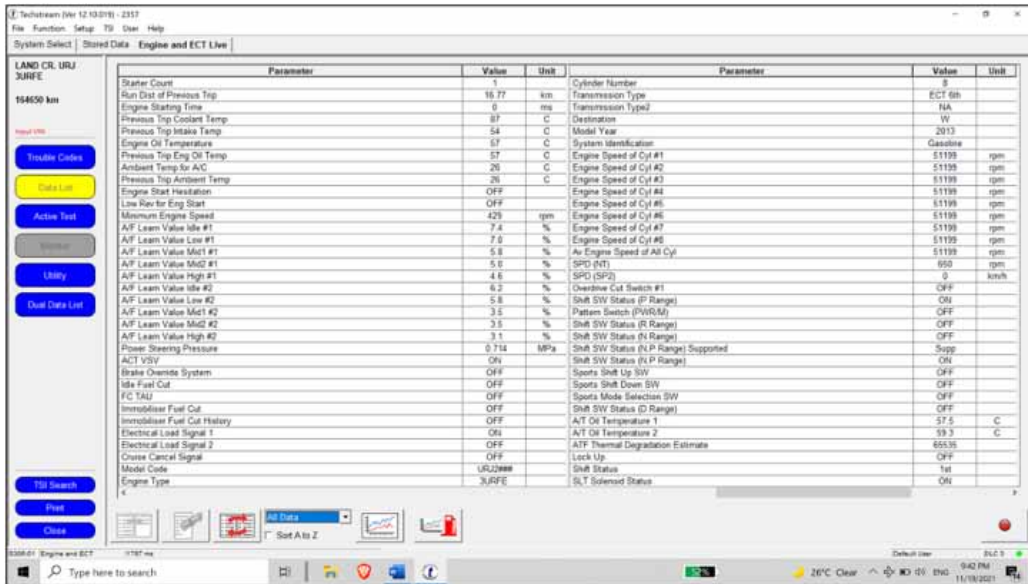
GTS automatically analyzed the results of the vehicle's components through comparison with the stored default parameters. The software also offers an extensive Toyota database that can assist users in the analysis of vehicles and is utilized during investigations. The GTS modules provide data relating to specific geographical regions, so we extracted the following results of the modules with respect to multiple geographical regions to establish a global perspective for the investigation:

Figure 9. Data that can serve to specify and validate a vehicle



- **Entry and Start:** Following a pattern, the driver usually unlocks the vehicle through the handle sensor rather than the key. However, on the date of the simulated crime, the SUV was unlocked using the key. This change in the driver's behavior suggests that another individual drove the car on the day in question. Moreover, a "new key registration error" indicating a failed attempt to add a new key one month prior to the crash, a suspicious action suggestive of an effort to control the car discreetly (as discussed, we simulated this suspicious activity prior to staging the crime scene and to determine whether DF could detect it).
- **Main Body:** The trunk had been opened at the assumed time of the crime, indicating that the driver may have brought cargo on the trip. In addition, a warning alert of a failed attempt to lock the car remotely with the door handle while the key was inside the vehicle was triggered, again suggesting that a party other than the driver tried to lock it (again, we simulated this suspicious activity prior to staging the crime scene and to determine whether DF could detect it).
- **Engine:** The run distance of the vehicle's last trip, which was on the date of the crash, was 16.77 km (Figure 10). This kind of data makes it possible to conduct a geographical analysis of the driver's origin, whereabouts, and stops on the day of the crash. Thus, the search of a radius of 16.77 kilometers around the crime scene helped to determine the activities of the driver and other parties that may have been involved, including the proximity of the latter to the vehicle during the last trip.
- **Smart Key:** The available configured keys for the car were listed as the main key and the spare key. Since an extra key was available, it could have fallen into the hands of someone other than the driver. Figures 11 to 14 show the wealth of information available regarding suspicious activity. Figure 11 details attempts to open the door, which triggered the following four warnings:
 - The Non-IG OFF Warning (Door open) indicates that a door was opened while the ignition was off, an act that could be routine or suspicious depending on the correlations among events.
 - The Non-IG OFF Warning (Alighting) indicates that the vehicle was remotely unlocked using the key, another act that could be routine or suspicious depending on the correlations among events as well as the timing of the crash.
 - The Carry Out Key from Other Than D-Seat Warning indicates that a key was not detected near the driver's seat, a potentially critical piece of evidence since the key is normally near the driver's seat when the driver is in the car.
 - The Key Left in Vehicle Lock Operating Warning indicates a failed attempt to lock the vehicle while the key is still inside using the door handle sensor. This is another critical piece of evidence that a third party tried to lock the door from the outside while a key was inside, which drivers do not normally do, normally only trying to open the door when another key

Figure 10. The distance of the previous trip by the vehicle displayed as 16.77 km



is inside. Combining this and related evidence can help to reconstruct the events leading to the crash.

Figure 12 shows the evidence relating to the opening of the back door. In this case, the output shows multiple instances of the trunk being opened with the key, potentially indicating whether the driver or someone else attempted to open the trunk.

Figures 13 and 14 provide crucial evidence regarding the registration of the vehicle’s keys. In this case, a failed attempt to register a duplicate key may indicate malicious intent. Such suspicions can be corroborated with related evidence to reconstruct the events leading to a crash.

The results thus extracted from multiple sources can then be documented in the appropriate format as potential pieces of evidence, with an explanation of each of the modules and their functions presented in simple, jargon-free language so that those who read the report, whether the prosecutor or lawyers for the case or the judge, can interpret the findings easily. Further, high-quality reports present the evidence in ways that are clear and concise, including diagrams and photographs when possible to show the scene of the incident, and are written in the appropriate professional style (Abbas, 2015).

CONCLUSION AND DIRECTIONS FOR FUTURE RESEARCH

Digital vehicle forensics (DVF) is a relatively new and innovative domain that is growing rapidly owing to the enormous amounts of rich data currently being collected and stored in vehicle modules. These data can be very useful to law enforcement agencies and the courts. Accordingly, DVF has become a critical aspect of cyber forensics for investigators seeking to solve cases as well as predict clues to a crime. We demonstrated the potential of DVF through a simulation of a crime, crime scene, and investigation involving a Toyota Land Cruiser SUV. The collection of the data relating to the incident provided factual evidence of the events leading up to the simulated crash.

There has been scant research on DVF to date, so the insights and suggestions for government agencies regarding the formulation of appropriate policies and guidelines for the use of DVF data in the present paper are especially valuable. Thus, law enforcement agencies can use the simulated

Figure 11. Door entry warning operation log

Operation History			
Time Stamp when the data was stored			
Elapsed Time after CPU Reset	Time & Date	Key Cycle	CPU Reset Count
52d 10h 27m	11/18/2021 9:01 AM	238	0

Operation History			
Auto Entry Warning Operation ▾			
Elapsed Time after CPU Reset	Time & Date	Key Cycle	CPU Reset Count
52d 07h 36m	11/18/2021 6:10 AM	235	0
52d 07h 33m	11/18/2021 6:07 AM	234	0
51d 17h 57m	11/17/2021 4:31 PM	233	0
50d 14h 45m	11/16/2021 1:19 PM	231	0
50d 14h 45m	11/16/2021 1:19 PM	231	0
50d 13h 36m	11/16/2021 12:10 PM	230	0
50d 11h 39m	11/16/2021 10:13 AM	229	0
50d 09h 03m	11/16/2021 7:37 AM	228	0
50d 08h 24m	11/16/2021 6:58 AM	228	0
49d 22h 54m	11/15/2021 9:28 PM	227	0
49d 22h 51m	11/15/2021 9:25 PM	227	0
49d 22h 39m	11/15/2021 9:13 PM	226	0
49d 11h 42m	11/15/2021 10:16 AM	226	0
49d 11h 42m	11/15/2021 10:16 AM	226	0
49d 11h 42m	11/15/2021 10:16 AM	225	0
49d 11h 36m	11/15/2021 10:10 AM	225	0
48d 22h 36m	11/14/2021 9:10 PM	225	0
48d 22h 15m	11/14/2021 8:49 PM	224	0
48d 21h 21m	11/14/2021 7:55 PM	223	0

Figure 12. Vehicle trunk actions log

Operation History				
Trunk/Back Door ▾				
Elapsed Time after CPU Reset	Time & Date	Key Cycle	CPU Reset Count	Parameter Name
38d 08h 03m	11/3/2021 5:10 PM	193	3	Back Door Open by Back Door SW Input
38d 01h 00m	11/3/2021 10:07 AM	191	3	Back Door Open by Back Door SW Input (Auto Entry)
37d 20h 42m	11/3/2021 5:49 AM	189	3	Back Door Open by Back Door SW Input
37d 20h 39m	11/3/2021 5:46 AM	188	3	Back Door Open by Back Door SW Input
37d 20h 03m	11/3/2021 5:10 AM	185	3	Back Door Open by Back Door SW input (Auto Entry)

case described here as guidance in similar cases, and members of the judiciary can take the findings presented here into consideration when deciding on the admissibility of evidence from the data sources accessed during DVF, including for the corroboration and substantiation of facts based on multiple pieces of evidence.

Of course, the research described here is not without limitations. Thus, since the simulated crime did not actually take place, the data that we obtained using the DF tool may not be entirely consistent with the data obtained during an actual DF investigation. Further, more robust results could be obtained using another tool and comparing the data extracted with the tool that we used. Moreover, simulations involving multiple scenarios, rather than the single scenario described here, could provide additional data to validate the results.

Since VDF is an emerging domain, there is a need to assess empirically and standardize the tools used in investigations, streamline the data-retrieval process, and establish consistent data interfaces and presentation formats. Accordingly, topics in need of research in this field include a vetting process and model for VDF tools, a standardized interface for the retrieval of DF data, and a framework for

Figure 13. The current number of registered car keys

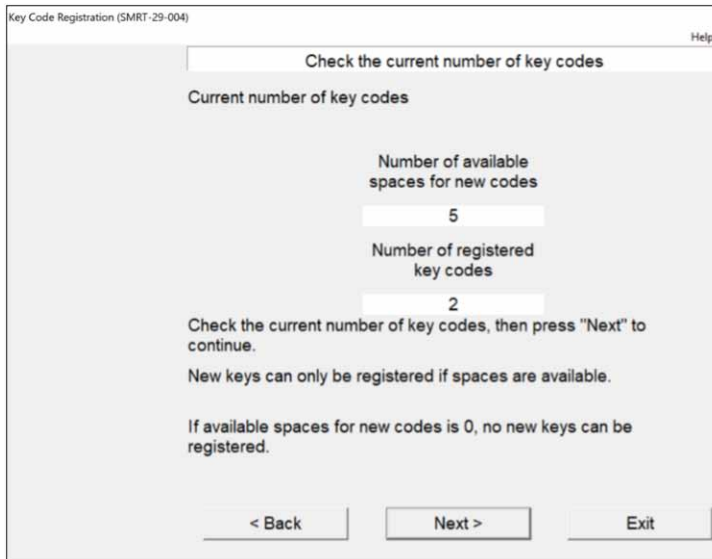


Figure 14. The operation history log showing a failed attempt to register a key

Operation History				
Time Stamp when the data was stored				
Elapsed Time after CPU Reset	Time & Date	Key Cycle	CPU Reset Count	
52d 10h 27m	11/18/2021 9:01 AM	238	0	
Operation History				
Certification ECU operation log ▾				
Elapsed Time after CPU Reset	Time & Date	Key Cycle	CPU Reset Count	
50d 13h 45m	11/16/2021 12:19 PM	230	0	Immobiliser Verification Error
50d 13h 45m	11/16/2021 12:19 PM	230	0	Immobiliser Verification Error
21d 08h 03m	10/18/2021 6:37 AM	247	0	Immobiliser Verification Error
5d 04h 24m	10/2/2021 2:58 AM	212	0	New Key Registration Error
5d 04h 18m	10/2/2021 2:52 AM	207	0	Immobiliser Verification Error
5d 04h 18m	10/2/2021 2:52 AM	207	0	Failed Registration Mode
5d 04h 18m	10/2/2021 2:52 AM	207	0	Failed Registration Mode

the presentation of DVF data in a format appropriate for use in the legal system. Since DVF is an emerging science, it has yet to be used extensively in the courts, and challenges remain in terms of the variety of vehicle systems and lack of standard guidelines and frameworks. This branch of forensics can be expected to continue developing rapidly to keep pace with technological innovations in the vehicle industry.

The rapid adoption of digital systems in vehicles by automobile manufacturers, such as EDR, ECU, VCDS, and CDR, provides drivers with a seamless and comfortable driving experience. Furthermore, these technologies present ample opportunities to serve as reliable evidence in the judiciary, aiding

in the pronouncement of accurate verdicts. However, this requires standardized procedures for the collection and presentation of digital evidence before judicial proceedings:

1. A standardized format for the collection, chain of custody, and presentation of digital evidence before judicial authority.
2. Judges to be trained in multiple perspectives of digital forensics to effectively review the evidence and render judgments. Without such training, it may pose a challenge to accurately assess the evidence and make informed decisions (Kessler, 2010).
3. A global compliance regulatory standard for automobile data recording technologies that cuts across all automobile manufacturers. This standard would assist the three critical stakeholders in digital forensics: vehicle manufacturers, law enforcement agencies, and the judiciary. It would ensure fair judgment and facilitate effective evidence analysis and interpretation.

REFERENCES

- Abbas, T. M. J. (2015). Studying the documentation process in digital forensic investigation framework/models. *J Al-Nahrain University.*, 18(4), 153–162. doi:10.22401/JNUS.18.4.21
- ABForensics. (2022). *Digital vehicle forensics*. ABForensics. <https://abforensics.com/digital-vehicle-forensics/>
- Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, 14, 346–376.
- Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 22, 3–13. doi:10.1016/j.diin.2017.06.015
- Bankole, F., Taiwo, A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Sci Int: Digit Investig.*, 40, 301–348. doi:10.1016/j.fsidi.2022.301348
- Bates, E. A. (2019). *Digital vehicle forensics*. ABForensics. <https://abforensics.com/wp-content/uploads/2019/02/INTERP-OL-4N6-PULSE-IssueIV-BATES.pdf>. (accessed November 19, 2019).
- Berla. (2022). *Discover Vehicle Forensics*. Berla. <https://berla.co/discover/>
- Buquerin, K. K. G., Corbett, C., & Hof, H.-J. (2021). A generalized approach to automotive forensics. *Forensic Sci Int: Digit Investig.*, 36, 301111.
- Dobromirov, V., Dotsenko, S., Verstov, V., & Volkov, S. (2017). Methods of examining vehicle electronic systems in the course of automotive forensic expert examinations. *Transportation Research Procedia*, 20, 143–150. doi:10.1016/j.trpro.2017.01.037
- Določ, K., Meyer, C., Attenberger, A., & Steinberger, J. (2020). Driver identification using in-vehicle digital data in the forensic context of a hit and run accident. *Forensic Sci Int: Digit Investig.*, 35, 301090.
- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64–S73. doi:10.1016/j.diin.2010.05.009
- Garrie, D. B. (2014). Digital forensic evidence in the courtroom: Understanding content and quality. *Nw. J. Tech. & Intell. Prop.*, 12, i.
- Ghazinour, K., Vakharia, D. M., Kannaji, K. C., & Satyakumar, R. (2017). A study on digital forensic tools. Paper presented at the 2017 IEEE International Conference on Power, Controls, Signals and Instrumentation Engineering (ICPCSI). IEEE. doi:10.1109/ICPCSI.2017.8392304
- Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. *Int J Electron Secur Digit Forensics.*, 9(1), 1–18. doi:10.1504/IJESDF.2017.081749
- Gülataş, İ., & Baktir, S. (2018). Unmanned aerial vehicle digital forensic investigation framework. *J Nav Sci Eng.*, 14, 32–53.
- Gwynedd Mercy University. (2021). *Computer forensics career guide: bridging criminal justice and CIS*. Gwynedd Mercy University. <https://www.gmercyu.edu/academics/learn/computer-forensics-career-guide>, .
- Holt, T., & Dolliver, D. S. (2021). Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes. *Forensic Sci Int: Digit Investig.*, 37, 301167. doi:10.1016/j.fsidi.2021.301167
- Jackson, K. A., Jr. (2020). *Infotainment and telematic systems challenges affecting vehicle forensic law enforcement capabilities*. [Doctoral dissertation, Utica College].
- Jacobs, D., Choo, K.-K. R., Kechadi, M.-T., & Le-Khac, N.-A. (2017). Volkswagen car entertainment system forensics. Paper presented at the 2017 IEEE Trustcom/BigDataSE/ICCESS, . Jeong D. Artificial intelligence security threat, crime, and forensics: taxonomy and open issues. IEEE. doi:10.1109/Trustcom/BigDataSE/ICCESS.2017.302
- Kopencova, D., & Rak, R. (2020). Issues of vehicle digital forensics. Paper presented at the 2020 XII International Science-Technical Conference on Automotive Safety. IEEE. doi:10.1109/AUTOMOTIVESAFETY47494.2020.9293516

- Lacroix, J., El-Khatib, K., & Akalu, R. (2016). Vehicular digital forensics: what does my vehicle know about me? Paper presented at the *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*, ACM. doi:10.1145/2989275.2989282
- Le-Khac, N.-A., Jacobs, D., Nijhoff, J., Bertens, K., & Choo, K.-K. R. (2020). Smart vehicle forensics: Challenges and case study. *Future Generation Computer Systems*, 109, 500–510. doi:10.1016/j.future.2018.05.081
- Lewis, L., Hare, B., Clyde, H., & Landis, R. (2019). *Vehicle control history: data from driver input and pre-collision systems activation events on Toyota vehicles*. SAE Technical Paper.
- Li, M., Weng, J., Liu, J.-N., Lin, X., & Obimbo, C. (2021). Toward vehicular digital forensics from decentralized trust: An accountable, privacy-preserving, and secure realization. *IEEE Internet of Things Journal*, 9(9), 7009–7024. doi:10.1109/IIOT.2021.3116957
- Mansor, H., Markantonakis, K., Akram, R. N., Mayes, K., & Gurulian, I. (2016). Log your car: the non-invasive vehicle forensics. Paper presented at the *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE. doi:10.1109/TrustCom.2016.0164
- Mearian, L. (2016). By 2035, 21M self-driving vehicles will be on the road. *Computerworld*. <https://www.computerworld.com/article/3080590/by-2035-21m-self-driving-vehicles-will-be-on-our-roads.html>.
- Meyers, M., & Rogers, M. (2005). Digital forensics: meeting the challenges of scientific evidence. *Advances in Digital Forensics: IFIP International Conference on Digital Forensics*. National Center for Forensic Science. Springer.
- Montasari, R. (2016). A comprehensive digital forensic investigation process model. *Int J Electron Secur Digit Forensics.*, 8(4), 285–302. doi:10.1504/IJESDF.2016.079430
- Mordor, I. (2022). *Digital forensics market size, trends*. Mordor Intelligence. <https://www.mordorintelligence.com/industry-reports/digital-forensics-market>
- Paul Joseph, D., & Norman, J. An analysis of digital forensics in cyber security. Paper presented at the First International Conference on Artificial Intelligence and Cognitive Computing, 2019. doi:10.1007/978-981-13-1580-0_67
- Quick, D., & Choo, K.-K. R. (2018). IoT device forensics and data reduction. *IEEE Access: Practical Innovations, Open Solutions*, 6, 47566–47574. doi:10.1109/ACCESS.2018.2867466
- Rak R, Kopencová D. (2020). Actual issues of modern digital vehicle forensic. *Internet of Things and Cloud Computing*, 8.
- Reedy, P. (2020). Interpol review of digital evidence 2016–2019. *Forensic Science International. Synergy*, 2, 489–520. doi:10.1016/j.fsisyn.2020.01.015 PMID:33385144
- Saufi, N. N. C., Razak, N. S. M., & Mansor, H. (2019). FoRent: vehicle forensics for car rental system. Paper presented at the *Third International Conference on Cryptography, Security, and Privacy*. ACM. doi:10.1145/3309074.3309101
- Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys and Tutorials*, 22(2), 1191–1221. doi:10.1109/COMST.2019.2962586
- Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation*, 29, 101–108. doi:10.1016/j.diin.2019.03.011
- Sunde, N., & Horsman, G. (2021). Part 2: The phase-oriented advice and review structure (PARS) for digital forensic investigations. *Forensic Sci Int: Digit Investig.*, 36, 301074. doi:10.1016/j.fsid.2020.301074
- Talib, M. A., Alnanih, R., & Khelifi, A. (2020). Application of quality in use model to assess the user experience of open source digital forensics tools. *Int J Electron Secur Digit Forensics.*, 12(1), 43–76. doi:10.1504/IJESDF.2020.103870
- Thommasone, S. (2021). *What is automotive forensics?* AZO Life Sciences. <https://www.azolifesciences.com/article/What-is-Automotive-Forensics.aspx>

Vandiver, W., & Anderson, R. (2018). Analysis of Berla iVe acquisitions of vehicle speed data from ford sync systems. *SAE International Journal of Transportation Safety*, 6(3), 257–274. doi:10.4271/2018-01-1442

Vinzenz, N., & Eggendorfer, T.(2019). Forensic investigations in vehicle data stores. Paper presented at the Proceedings of the Third Central European Cybersecurity Conference, 2019. doi:10.1145/3360664.3360665

Whelan, C. J., Sammons, J., McManus, B., & Fenger, T. W. (2020). Retrieval of infotainment systems artifacts from vehicles using iVe. *J Appl Digit Evidence.*, 1, 30–45.

Xing, P., Yang, M., Tsuge, B., & Flynn, T. (2018). *The accuracy of Toyota vehicle control history data during autonomous emergency braking*. SAE Technical Paper.

Xing, P., Yang, M., Tsuge, B., Flynn, T., Lawrence, J., & Siegmund, G. P. (2018). *The accuracy of Toyota vehicle control history data during autonomous emergency braking*. SAE Technical Paper. , 201810.4271/2018-01-1441

Yeboah-Ofori, A., & Brown, A. D. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *J Forensic. Leg Investigative Sci.*, 6(1), 1–8. doi:10.24966/FLIS-733X/100045

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science and Information Technologies*, 3(3), 17–31. doi:10.5121/ijcsit.2011.3302

Mathew Nicho is an Associate Professor at the Research and Innovation Centre at Rabdan Academy, UAE. College of Technological Innovation at Zayed University, Dubai, United Arab Emirates teaching and researching in the cyber security domain. Prior to this he was an Associate Professor at Zayed University Dubai, lecturer in cybersecurity and IT governance at the School of Computing and Digital Media at Robert Gordon University, Scotland. He obtained his Masters and PhD from the Auckland University of Technology, Auckland, New Zealand. His teaching and research are in the socio technical aspects of cyber-attacks, advanced persistent threats, as well as intrusion detection using machine learning and IT security governance. His research outputs have appeared in journals and conferences namely Communications of the Association of Information Systems, Information and Computer Security, International Journal of Information Security and Privacy, and conferences namely Hawaii International Conference on System Sciences, International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, and ICISSP.

Maha Alblooki did her MSc in Cyber Security at Zayed University and is working in the College of Technology Innovation at Zayed University. She is an avid researcher.

Saed AIMutiwei did his MSc in Cyber Security at Zayed University and is currently working in the industry in a security role.

Christopher D. McDermott (Ph.D., Robert Gordon University) is a Lecturer in Human-centred security. His research focuses on human factors of security, privacy and trust, with a particular focus on Security by Design (SBD), using personas and threat modelling to design and optimise systems that promote secure behaviour and situational awareness of threats.

Olufemi is a multi-faceted academic with diverse background in International Law, Public Theology and Ethics of Communication. He has a PhD in Law from the University of Aberdeen. Before earning an LLM in International Law from the University of Westminster, London, he had studied for an MTh in Theology and Ethics of Communication at the New College, University of Edinburgh. Femi is interested in exploring 'universalist/relativist debates in Criminology, International Relations & Law' with a focus on international human rights and competing worldviews. He has a particular interest in regional security studies, counterterrorism, and computer misuse.