



Master of Science (M.Sc.)

# MASTER THESIS

Recent Developments and Emerging Trends  
in Automotive Digital Forensics

Kim Strandberg

Network Forensics,  
School of Information Technology

Halmstad University, June 3, 2025

Kim Strandberg: *Recent Developments and Emerging Trends  
in Automotive Digital Forensics* © June 2025

SUPERVISOR:  
Mohamed Eldefrawy

## ABSTRACT

---

The automotive industry is increasingly facing growing cybersecurity challenges as vehicles become more connected and autonomous. Modern cars equipped with sophisticated electronic systems are becoming more susceptible to cyber threats. Enhancing detection and forensic capabilities within automotive systems is essential for mitigating these risks. This work builds upon and extends a previous systematic literature review of automotive digital forensics, covering 2006 to early 2021. However, recent advancements in the field have introduced new challenges and opportunities, particularly in light of an evolving, dynamic threat landscape and growing vehicle complexity. These developments have driven numerous advancements, particularly in artificial intelligence, machine learning, and blockchain technologies.

In response, we review the latest state-of-the-art developments from 2021 to 2025, addressing critical challenges and technical solutions to provide a comprehensive understanding of the evolving landscape and its implications for both researchers and practitioners. By categorizing and comparing these advancements with prior research, we highlight key trends and innovations, analyze security concerns, and ultimately offer valuable insights into future research directions and emerging trends.



## PUBLICATIONS

---

A conference publication based on this thesis with the title *Advances in Automotive Digital Forensics: Recent Trends and Future Directions* has been accepted for publication at the 20th International Conference on Availability, Reliability and Security (ARES 2025) conference.



## CONTENTS

---

|   |                          |    |
|---|--------------------------|----|
| 1 | INTRODUCTION             | 1  |
| 2 | RELATED WORK             | 3  |
| 3 | SCOPE AND METHODOLOGY    | 5  |
| 4 | CONTRIBUTIONS            | 7  |
| 5 | CATEGORIZATION OF PAPERS | 9  |
| 6 | DISCUSSION               | 23 |
| 7 | CONCLUSION               | 25 |
|   | BIBLIOGRAPHY             | 27 |

## LIST OF FIGURES

---

|          |   |   |
|----------|---|---|
| Figure 1 | Visualization of the methodology: Database searches and analysis. | 5 |
|----------|---|---|

## LIST OF TABLES

---

|         |  |    |
|---------|--|----|
| Table 1 | Selected papers concerning technical solutions | 10 |
| Table 2 | Selected papers concerning surveys             | 10 |



## INTRODUCTION

---

Digital forensics, a subset of forensics, includes various domains, including automotive digital forensics (ADF), focusing specifically on vehicles. Generally, digital forensics considers all devices that can store or process data and communication between such devices. Digital forensics investigations must follow a strict process, and the data used must meet cybersecurity requirements to ensure forensic soundness. The process can vary but typically includes the following phases: *identification, preservation, acquisition, verification, analysis, and reporting* [1]. Cybersecurity requirements ensuring forensic soundness can include fulfilling common security properties, such as Confidentiality (C), Integrity (I), and Availability (A), commonly known as the CIA triad. In addition, the CIA is typically extended with other properties, such as Non-Repudiation (N) and Privacy (P), where the former extends upon (I) to additionally ensure data origin, and fulfilling the latter infers that privacy-sensitive data is secured and all storage justified both considering the type of data and how long the data is kept [2]. A modern vehicle is a complex safety-critical system containing over 150 computers, known as Electronic Control Modules (ECUs), and over 100 million lines of code. These ECUs, along with their code, control various functionalities, such as safety-critical steering, braking, and engine control, as well as more straightforward tasks, such as door nodes that check the status of open or closed doors. For instance, steering or braking typically involves a sensor that detects the position of the brake pedal or steering wheel and sends this data to an ECU. The data is processed and validated by the ECU, and a signal is sent from the ECU to an actuator, that performs the actual response, such as aligning the wheel and brakes according to the signal.

Infotainment systems tend to be more complex, with the potential to run various applications. ECUs are part of the vehicle's electrical/electronic (E/E) architecture, can run different operating systems, and use various communication buses. Vehicles are becoming more connected to the outside world via Vehicle-to-Everything (V2X) communication, which includes communication with other vehicles (V2V), infrastructure (V2I), the cloud (V2C), the grid (V2G), and pedestrians (V2P). Thus, forensically relevant data is not only found in the vehicle itself but also distributed across various locations. ADF is a distinct and rapidly evolving field, separate from similar fields such as the Internet of Things (IoT), i.e., devices with Internet connectivity, such as smartphones, sensors, and actuators. Although there are similari-

ties, such as the use of IoT devices in vehicles, the main distinction is that vehicles are safety-critical cyber-physical systems (CPS) with real-time requirements. Therefore, failures can lead to serious and potentially fatal consequences for drivers, passengers, or people in the surroundings. As an example, a hypothetical scenario for forensic investigation follows:

*The airbag system unexpectedly deploys, causing the driver to lose control and crash. The driver is seriously injured and placed in a medical coma. A forensic investigation reveals that the incident was caused by a cyberattack targeting the communication between the airbag sensors and the control system, where signals were spoofed. Given the driver's political importance and the attack's complex routing through multiple servers, it's suspected that the attack originated from a foreign entity seeking to influence political outcomes.*

For this hypothetical incident, it is imperative that the data is *Available (A)*, meaning sufficient data has been detected and logged. Furthermore, the data must be accessible only by authorized individuals, ensuring *Confidentiality (C)* and *Privacy (P)* considerations are maintained. Additionally, the data must be trustworthy, guaranteeing both *Integrity (I)* and *Non-repudiation (N)*. In summary, vehicle manufacturers are required to ensure the appropriate cybersecurity properties are in place when needed, such as the aforementioned CIANP (Confidentiality, Integrity, Availability, Non-repudiation, and Privacy) [3].

There are various regulations and standards that include requirements affecting ADF, such as UN Regulation No. 155 [4] for cybersecurity and digital forensics, UN Regulation No. 156 [5] for vehicle software updates (which impact the ability to update and adapt mechanisms), UN Regulation No. 160 [6] for Event Data Recorders (EDRs), and the ISO 21434 [7] standard for vehicle cybersecurity. However, no standard specifically addresses ADF or defines key aspects such as format, tools, processes, and data management. While related standards and regulations exist, they offer limited detail, particularly with regard to ADF. As a result, vehicle manufacturers are responsible for demonstrating to authorities how regulations, such as UN Regulation No. 155 [4], are being met.

## RELATED WORK

---

In [2], K. Strandberg et al. conducted a comprehensive systematic literature review (SLR) in the field of ADF, covering the most relevant related work from 2006 to 2021. A list of relevant data sources for ADF is identified and presented in Table 3 of the referenced SLR. Additionally, articles are organized into categories based on their purpose in Table 1 (technical solutions) and Table 2 (surveys), respectively. In addition, recommendations are provided for securing various data by maintaining security properties, and stakeholders are identified for the data. The SLR discusses that the automotive industry relies primarily on traditional methods for root cause analysis of incidents, such as examining component integrity, service history logs, and fault codes. Additionally, there are very few tools specifically adapted for vehicle data extraction. Examples include Berla iVE [8] for infotainment systems and the Bosch Crash Data Retrieval System for diagnostics and fault codes [9].

A few of the main challenges identified in the SLR include the lack of cybersecurity mechanisms to ensure trustworthy forensic data and considerations for privacy. There is a significant risk of data compromise and misuse, such as data tampering. Additionally, there is a lack of standardization for ADF, including format, tools, and procedures. Currently, the ability to establish the chronological order of events across different communication buses and align with, for example, other vehicles potentially involved in an incident, is limited. The cost of securely detecting and storing forensic data is another significant challenge.

Regarding the most relevant related work from the more recent period (2021-2025), this will fall within the scope of this work and will be addressed in the following sections.



## SCOPE AND METHODOLOGY

An extensive approach to an SLR was employed, using four databases, covering the period from 2006 to early 2021 [2]. However, in contrast to [2] and as shown in Figure 1, this thesis focuses on the most recent advancements from 2021 to early 2025, comparing these developments with the findings of previous work included in the SLR.

Papers were included based on relevance to the automotive domain, publications between 2021-2025, and being published in journals or conferences, and excluded based on being unrelated to automotive digital forensics, not written in English, or already included in the previous SLR [2].

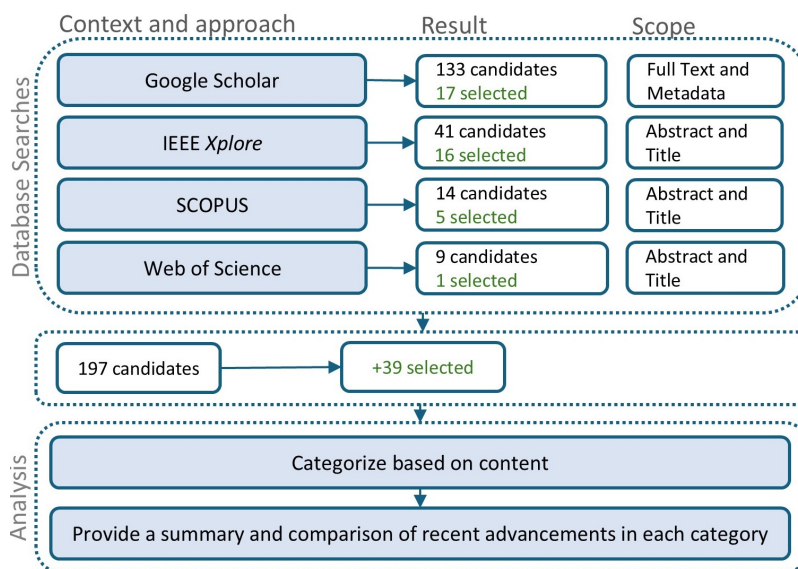


Figure 1: Visualization of the methodology: Database searches and analysis.

We used the following search terms: *digital forensics* in conjunction with *vehicle*, *car*, or *automotive*. Google Scholar<sup>1</sup> returned 133 candidates, with 17 selected. IEEE Xplore<sup>2</sup> returned 41 candidates, with 16 selected. SCOPUS<sup>3</sup> returned 14 candidates, with 5 selected. Web of Science<sup>4</sup> returned nine candidates, with one selected. This resulted in 197 candidates, of which 39 were selected. We started with Google Scholar, which was less specific and returned most papers, but many were not relevant. The other three databases returned more specific and relevant articles, but due to duplicate removal, fewer articles were

<sup>1</sup> Google Scholar search performed on 2025-01-21

<sup>2</sup> IEEE Xplore search performed on 2025-01-28

<sup>3</sup> SCOPUS search performed on 2025-01-28

<sup>4</sup> Web of Science search performed on 2025-01-28

selected in each subsequent database search. With some adjustments to better align with recent developments, the categories established in [2] are applied to classify and analyze the publications, enabling a comparison with the latest advancements.

## CONTRIBUTIONS

---

Our main contributions are as follows:

- **Comprehensive Review of ADF:** We provide a detailed review of existing ADF research, focusing on critical challenges, technical solutions, and data collection methods, serving as a valuable resource for researchers and practitioners.
- **Categorization, Comparative Analysis, and Relevance Assessment:** We categorize and compare research from 2021-2025 with an SLR from 2006-2021 [2], highlighting trend shifts and innovations reshaping the field. We also assess the technical solutions in terms of security and practical relevance.
- **Recent Trends and Future Directions:** We provide a perspective on the future direction of ADF by analyzing recent developments, offering insights into emerging trends and key research areas, and providing practical guidance for researchers and engineers.



## CATEGORIZATION OF PAPERS

---

We have divided the results into two main categories: technical solutions (Table 1) and surveys (Table 2). Articles proposing technical solutions are included in the former category, while all other articles are placed in the latter. Additionally, each paper is assigned to one or more identified focus categories. We also specify whether the papers were published in a conference or journal. Furthermore, we explicitly state whether the technical solution considers and emphasizes the CIANP properties and, if so, which ones. We begin with a summary of each category based on the period from 2006 to early 2021 [2], followed by the addition of the most recent advancements from 2021 to early 2025. We acknowledge that there is some overlap between categories for the papers, and we have chosen to summarize each paper under the category we believe is most applicable. Additionally, we use main categories when subcategories are more prone to overlap; for example, data collection and extraction are similar, with only a slight difference in emphasis.

**1. Data: different types of forensic data, data retrieval, and extraction techniques.** *1a. Data Collection.* *1b. Extraction Techniques.* This category discusses various aspects of data management and forensic techniques. Forensic data is considered from both the front- and back-end perspectives. The former focuses on data inside the vehicle, addressing challenges such as the lack of standardized interfaces for data extraction and formatting, as well as the absence of debug ports, which often require dismantling storage circuits. Additionally, it explores data extraction techniques, proposing methods using the JTAG (Joint Test Action Group) port, and mentions the issue that debug ports are commonly closed in production vehicles for security reasons. To some extent, tools related to data extraction, such as Alientech KTag [47], and PEmicro Cyclone [48], are discussed, with the compatibility issue highlighted. Blockchain for data management is also explored, emphasizing both potential benefits and challenges, including security and privacy concerns.

**Recent Trends.** In [12], J. Lee et al. perform a study specifically on how data relevant to forensics are stored and transmitted in Tesla vehicles through the concept of software-defined vehicles (SDVs) and the centralized data storage provided by Tesla's SDV architecture. The study details the technical process of identifying, acquiring, analyzing, and verifying data from EDRs, multiple sensors, over-the-air (OTA) updates, and logs, with an emphasis on cross-referencing and integrat-



ing diverse data sets to strengthen the reliability of the forensic process. However, the legal and ethical concerns, particularly regarding privacy and the confidentiality of the data, require more attention. In [38], M.A. Shayer et al. conducts a comparative study of Generative Adversarial Networks (GANs), specifically DCGAN, VSGAN, and CGAN, for vehicle identification. The authors highlight VSGAN as an architecture specifically designed for vehicle image generation, emphasizing its superior performance in generating clearer and more accurate car images compared to DCGAN and CGAN.

In [39], N.I. Chowdhury et al. analyze challenges, issues, and defenses for vehicles in three main areas: forensics, communication, and over-the-air updates. The Mitre ATTACK database is used to identify attack scenarios and mitigation. In [33] K.G. Buquerin et al. investigate the Tesla autopilot with an emphasis on its file system, addressing questions such as who, where, when, and how events occurred. They identify relevant timestamps, user accounts, media files, and system logs. The authors used Python and Magnet AXIOM [49] for their analysis, highlighting the integrity of the data while making assumptions, such as the accuracy of timestamps and the absence of tampering. In [41], C. Stathers et al. survey and perform practical experiments focusing on data extraction using mobile forensic techniques and On-Board Diagnostics (OBD) software on a 2008 Mitsubishi Colt. They examine data from sources such as the dashboard camera, the head unit, and other ECUs. The main conclusion is that even older cars contain a significant amount of data. However, the security and privacy aspects should be emphasized more in the investigation process. In [45], R. Rak et al. focus on digital vehicle identifiers across various components in over 250 vehicle models and their applicability for forensic practices in identifying vehicles. The authors highlight the challenges and the need for standardization in the methods and devices used to collect such data.

## **2. Challenges: general challenges, requirements and guidelines.**

*2a. General Challenges. 2b. Requirements, Guidelines.* Automotive systems are becoming increasingly complex, with modern vehicles functioning as *computers on wheels*. However, many of these systems lack reliable security measures, making data extraction easier for forensic investigators. Still, these vulnerabilities present significant challenges, as the absence of security mechanisms in ADF reduces trust in the evidence and exposes data to cyberattacks. Major issues include the lack of authentication for in-vehicle communication, limited storage capacity, and difficulties in maintaining data integrity and authenticity during forensic investigations. The lack of standardization forces manufacturers to develop and implement their own strategies for data storage, interfaces, and forensic processes, further complicating forensic investigations.

The vast amount of data and its distributed nature require extensive manual effort for collection and extraction. Adherence to laws for both privacy and data collection for digital forensics is a significant concern. The lack of forensic tools is also discussed. Several suggestions have been made to improve the security of forensic data. For instance, the telematics unit is proposed to be used for storage with a circular buffer and additional memory. Requirements for event reconstruction and the need for detection and secure storage, such as using hashes to detect manipulation, are also highlighted. Machine learning (ML) is proposed to identify patterns, predict crimes, and link vehicles to individuals through data sources like cell phone logs and vehicle communication. A proposal for an organizational framework for traffic police is suggested to guide further research into accidents and crimes by integrating multiple data sources, such as vehicles, cell phones, and traffic data.

**Recent Trends.** In [37], S. Hussain et al. survey the potential integration of blockchain technology for vehicle communication, focusing on secure communication, forensics applications, secure data storage, trust and reputation management, and privacy. A comparison of Ethereum and Hyperledger consensus algorithms, along with challenges, is performed, with the author favoring Ethereum in terms of performance, efficiency, and scalability. In [42] J. Repas et al. conduct a study focusing on various challenges in ADF. However, most of the conclusions have already been discussed in other papers. Nonetheless, the authors emphasize the increasing complexity in the evolution of vehicles and the need for new and better-aligned methodologies for timely evidence collection in forensic investigations. In [44], P. Sharma et al. analyze the components of Connected Autonomous Vehicles (CAVs), including sensors, communication networks, and actuators, and discuss the current cybersecurity and forensic challenges. The paper reviews various mitigation techniques, with a primary focus on security issues. It emphasizes the need for enhanced forensic solutions to detect, investigate, and understand security breaches, while also highlighting the critical role of strong cybersecurity measures in protecting forensic evidence and facilitating effective post-incident analysis.

**3. Communication: cloud, fog, edge node communication, Vehicular Ad hoc Networks, and Vehicle-2-Everything** 3a. Cloud/Fog/Edge. 3b. VANETs/V2X. The emphasis is on communication systems and cloud, fog, and edge computing, considering data transfer and storage, including VANETs for forensic data collection. For cloud computing, mechanisms for collecting and transferring data to the cloud using interfaces like Bluetooth or WiFi connected to the OBD-II port, are proposed, along with a discussion around the security risk introduced with such connections. The move toward fog/edge computing to reduce bandwidth by processing data closer to the source,

such as utilizing RSUs (roadside units), is proposed to address issues with large data volumes. Still, issues remain in terms of security and data processing capacity. A solution for Multi-access Edge Computing (MEC) is proposed to improve accident handling by collecting driving data (position, speed, and acceleration) before and after an accident and analysing this data in an edge infrastructure to determine accident liability. An Algorithm to embed location, timestamp, and other data, i.e., digital watermarking, into real-time accident photographs in VANETs, adding properties of authentication and integrity for digital evidence is introduced. Still, privacy and trust issues due to the fact that potentially sensitive information, such as videos and pictures of individuals, may be present remain significant challenges for making this feasible in a practical setting. Additionally, a vehicle witness system is proposed to use moving vehicles and RSUs as witnesses for incidents, sending forensic data anonymously to the cloud to preserve privacy. Still, videos and pictures can, as mentioned, contain sensitive information that must be taken into account. Thus, privacy concerns remain.

**Recent Trends.** In [10], Y. Lee et al. propose SA-Dedup, a Secure Approximate Deduplication scheme for forensic images in fog-assisted crowdsensing vehicular networks. The system divides the forensic region into geospatial grid cells based on vehicle positions, with the help of fog nodes. One key benefit highlighted is the reduction in storage requirements, as the system efficiently minimizes communication and storage overhead by detecting and eliminating near-duplicate images. The authors perform experimental validation to confirm the effectiveness and practicality of their approach. In [16], Q. Tao et al. propose a blockchain-based dynamic, extensible privacy protection and message authentication scheme for VANETs. The scheme uses elliptic curve-based point multiplication and batch message verification to reduce computational costs, while the Chinese Remainder Theorem (CRT) ensures secure message transfers and adaptive responses for RSUs. In [31], M.Y. Alkhanafseh et al. propose a framework for securing VANETs utilizing blockchain, Intrusion Detection Systems (IDS), and forensics mechanisms. The framework is built upon four layers: blockchain for authentication, cluster formation to avoid data collisions, IDS enhanced with AI technology for attack detection and forensics techniques to secure data collection and storage. The authors acknowledge that the framework is still in the conceptual phase. Thus, implementation and evaluation are left as future work. Although solutions such as [10, 16, 31] seem promising, several challenges remain in making these approaches viable, such as infrastructural dependencies, high storage and bandwidth demands, and significant computational requirements, factors that come with high costs and may not be prioritized in practice.

**4. Software: *applications, software, and tools.*** *4a. Applications and Software.* *4b. Forensic Tools.* This category focuses on applications and software, specifically road safety systems and forensic tools. It covers systems monitoring vehicle data to detect road disturbances and accidents, highlighting security vulnerabilities, such as communication protocol issues. Forensic tools are essential for extracting forensically relevant data from sources like EDRs, OBD, USB, and JTAG ports. While several tools are available, many lack support for automotive-specific file systems like QNX. This highlights the need for more secure, automotive-compatible tools and solutions for ADF.

**Recent Trends.** In [19], J. Jung et al. propose a process for collecting automotive forensic data using an Android phone connected to a vehicle's OBD-II port. They utilize Android apps such as Infocar and Torque Pro, Bluetooth HCI snoop logs, and the Android system's main log buffer. The extracted data includes vehicle velocity, speed, braking events, refueling, and Bluetooth connection times. The authors claim that this data can be used to reconstruct driver behavior. Notably, the approach does not address security or privacy concerns. In [24], R. Amala et al. focus on Vehicle Tracking Systems (VTS) within the transportation domain, presenting methods for extracting and analyzing forensic data. They introduce the IoT Forensics Suite (IFS), a tool developed by the authors, and demonstrate its use for VTS. Data extraction was performed over the SPI interface, but whether these methods also apply to other interfaces remains uncertain. Security also needs to be emphasized more in their approach.

In [28], M. Nicho et al. simulate a use case involving a 2015 Toyota Land Cruiser SUV to demonstrate the application of established forensic tools for data extraction and analysis prior to a hypothetical incident. While the scenario effectively highlights the practical need for forensics in the automotive domain, it may not fully reflect real-world investigations due to its hypothetical nature. The authors emphasize the importance of ensuring security throughout the process, but the primary focus is on demonstrating the use of existing forensic tools and processes, rather than addressing broader security challenges. In [46] S. Ebberts et al. investigate vehicle assistant apps from various car manufacturers from a digital forensic perspective, such as reconstructing driver patterns, e.g., routes, parking, and unlock/lock. Their findings include that appz leaves forensic traces, thus, demonstrating that data from vehicle assistant apps is useful for digital forensic investigations.

**5. Hardware: *architectural digital forensic design. Solutions, and mechanisms for sensors such as GPS, LIDAR, and cameras. Requirements for Event Data Recorders (EDRs) and Blackboxes.*** *5a. Architecture.* *5b. Sensor.* *5c. EDR and Blackbox.* This category highlights different hardware solutions applicable to ADF. For instance, a blockchain architecture is proposed for use as a black box, utilizing a consensus al-

gorithm to validate transactions. However, this approach is less practical due to the real-time requirements of vehicles and the cost of implementing a new architecture in which all ECUs would be able to sign and validate messages. In the context of forensic data sources, the CAN bus is emphasized, providing examples like error messages, and the infotainment system, which includes media content, internal logs, and GPS data. Dashboard cameras are also discussed in the context of ADF. For example, an algorithm is proposed to extract engine vibration patterns from video blur for vehicle identification, achieving around 90 percent accuracy. However, privacy concerns arise when the media content contains unrelated individuals or vehicles. Additionally, audio is proposed for vehicle identification, such as sound from the engine and air conditioner. However, challenges include sound disturbances and security and privacy concerns related to data collection and storage. Another important topic discussed is the use of data recorders, such as EDRs, and cryptographic methods, like encryption and hashing, to ensure data integrity for evidence.

**Recent Trends.** In [18] M. Rayno aims to improve the utilization of EDRs by identifying functional, privacy, and security requirements while also considering regulatory constraints. A model-based systems engineering (MBSE) approach is presented, using the Magic-Grid V2 methodology. Challenges are highlighted, such as the issue of satisfying the availability of forensic data with privacy (e.g., GDPR [50]) and protecting the manufacturer's intellectual property. In [22], M. Rayno et al. continue their work and present a system model detailing how to balance the need for forensic data, securing it, and protecting OEM's Intellectual Property (IP). They define specific EDR requirements and explain how these can address forensic investigation needs (e.g., data availability) and cybersecurity concerns (e.g., IP protection).

In [20], Z. Chen et al. propose a model for digital forensic investigations of networked terminal devices to aid in determining liability in automobile accidents. The model is validated with three T-box devices, demonstrating its feasibility. However, the paper provides limited attention to security considerations regarding the model. In [3], K. Strandberg et al. propose the Automotive BlackBox architecture to support ADF, detailing data collection, storage, and analysis guidelines. The architecture introduces a specific data format and requirements within an automotive context, aligned with both current and envisioned future regulations and standards. The authors emphasize security while also recognizing several challenges, including balancing privacy with forensic capabilities and security. In [27], B. Gadekar et al. investigate challenges surrounding event-based forensic analysis and apply established forensic methods to automotive systems. The challenges are particularly highlighted in relation to the growing number of vehicles, the volume of data generated, and the

need for real-time analysis. Although security issues are highlighted as well, addressing them is not the authors' main focus. Instead, their goal is to improve data management efficiency, scalability, and real-time analysis. The authors propose a clustering-based architecture for more efficient data management in response to these challenges.

In [36], T. Long et al. introduce a tampering detection framework that utilizes a dynamic watermarking technique. The framework was evaluated using real-world data, demonstrating its effectiveness in detecting tampered data. However, since static datasets were used, the framework's effectiveness in real-world driving scenarios remains unclear. Although the main goal is to ensure tampering detection, i.e., integrity, their solution could benefit from also addressing other security and privacy considerations. In [40], R. Kurachi et al. explore the potential of using EDRs for ADF, with an emphasis on detecting evidence tampering, such as hacking attempts. They also perform aligned experiments and propose security measures to counteract these threats, including message authentication and IDS. The authors conclude that while EDRs can be useful for forensic investigations, they need to be strengthened in terms of cybersecurity to ensure the trust in the data.

**6. Algorithms: Artificial Intelligence (AI), Machine Learning (ML), and other algorithms.** *6a. AI/ML. 6b. Other Algorithms.* This category emphasizes AI, ML, and other algorithms to improve forensic investigations and data analysis in contexts such as vehicle sensor data, driver behavior, and accident reconstruction. For instance, a protocol to detect sensor manipulation, such as spoofing and jamming, is proposed using deep neural networks. However, the analysis relies on simulated data rather than real-world sensor data, which raises questions about its practical value. A dataset is used to classify drivers based on their behavior in a hypothetical hit-and-run scenario. However, more research is required to demonstrate its value for forensic use. ML is discussed for automating driver identification, but practical implementation remains challenging since a standardized forensic data format is not yet available. The CASE standard is proposed as a solution to address this challenge. Furthermore, the lack of a public specification for data communication in Vehicle Networks (IVN) is highlighted as a challenge. READ, an algorithm to reverse-engineer CAN messages to detect deviations, is proposed to help identify abnormal driving patterns before accidents. Additionally, a method is proposed to estimate the likelihood that a suspect was near a crime scene using data such as GPS, acceleration, and braking patterns. This approach aims to recalculate routes and determine suspects' locations in hit-and-run accidents, offering the main benefit of saving time compared to manual methods.

**Recent Trends.** In [17], Y. Chen et al. introduce the CPBW (Change-Point-Detection and Bag-of-Words-Based Mechanism) for driver iden-

tification, leveraging a smartphone's triaxial accelerometer. CPBW uses change point detection (CPD) and the Bag-of-Words (BoW) method to identify drivers based on driving behavior efficiently. The system was evaluated using real-world data from two vehicle models (Hyundai and Toyota) with around 400 km of driving. While the study focuses on efficiency and accuracy, the approach does not prioritize security, which may expose the system to potential cyberattacks and reduce trust in the data collected. Environmental factors, such as varying road and weather conditions, could also challenge the potential for driver identification. In [30], R. Tyagi et al. introduce a blockchain-based system to securely store forensic data while utilizing AI and ML techniques to process large volumes of data and ensure privacy by randomizing signatures to mask witnesses' true identities. Their approach is evaluated for feasibility through simulations on an Ethereum blockchain platform, which demonstrates that security and privacy concerns are addressed and that the AI/ML-based techniques improve data processing. The authors believe their approach is applicable to future 5G/V2X networks. However, although the evaluation shows improved processing, computational costs and communication overhead in a practical setting are likely to remain challenging.

In [43] S. Rizvi et al. explores the use of AI in the field of network forensics, focusing on the application of techniques such as ML, deep learning (DL), and hybrid approaches. While the primary focus is not specifically on automotive forensics, the authors highlight the relevance of AI in addressing challenges within the automotive domain. Specifically, AI is seen as a key solution for processing and analyzing the large amounts of data generated by modern vehicles, improving the accuracy of investigations, and ensuring the identification of authentic, relevant, and correct data. In [35], S. Jabeen et al. focus on the challenge of Vehicle Make and Model Recognition (VMMR) and use both structural and pattern-based feature descriptors. Four different descriptors are employed to capture both structural and textural features of vehicles, which are then processed using two classifiers: Support Vector Machine (SVM) and K-Nearest Neighbor (KNN). The evaluation demonstrates high accuracy in recognizing the vehicle make and model, with structural-based descriptors proving to be more effective than pattern-based. The paper also highlights various challenges, such as difficulties in obtaining high-quality frontal images and the required computational complexity. Additionally, security and privacy considerations need to be emphasized more for real-world applications.

In [29], F. Iqbal et al. introduce a method for detecting and categorizing unusual events in audio recordings, including a dataset called the Unusual Occurrences in Audio Forensics Database (UOAFDB). The dataset consists of sounds from events such as car crashes, ex-

plosions, and gunshots, along with sounds from various background environments. Their method employs a deep-learning approach for sound event detection and classification, with the authors claiming to achieve a detection rate of over 80 percent. However, real-world conditions can present more complex and unpredictable noise scenarios, deep-learning models are also known to be resource-intensive, and security and privacy are not emphasized.

**7. Cryptography: blockchain technology or other cryptos.** *7a. Blockchain.*

*7b. Other Cryptography.* The main content of this category focuses on various blockchain-based solutions to improve digital forensic investigations, including strengthening IVN security. A high-level traffic investigation framework is proposed using decentralized identity distribution on a blockchain with sensor data. However, its industrial use seems impractical due to its abstract nature. Another blockchain framework is proposed to secure IVN by tracking previous transactions in ECUs. While it offers historical traceability, its use is limited as it only covers actions from OEMs, service technicians, and communications with RSUs, and not events from other actors. A blockchain-based event recording system with Proof of Event mechanisms is proposed, where an election algorithm selects a verifier from a network of participants. The goal is to provide trust in event data related to accidents. However, considering the complexity of IVN data, it is likely only applicable to a small subset of forensic data. Another approach for collecting and storing forensic data, AVGuard, is proposed to secure integrity using hash chains and Bloom filters. However, the approach lacks further consideration of privacy and securing web communication and storage.

**Recent Trends.** In [11], T. Menard et al. highlight privacy challenges in ADF data collection, where previous approaches mainly prioritized user anonymity over data unlinkability, making them less efficient at preserving privacy. The authors' approach uses group signatures and secure communication to ensure both privacy and traceability to specific events. They claim their approach outperforms existing methods in terms of privacy and security and demonstrate its efficiency regarding computation and communication overhead. However, like other similar approaches, infrastructure dependencies and scalability issues exist, which may limit the practical applicability of their solution. J. Li et al. [15] propose a secure in-vehicle digital forensic scheme with public auditing to ensure data integrity and authenticity in cloud storage. Their approach utilizes verifiable delay functions (VDFs), which enable public verification of the data, allowing for the detection of tampering. The scheme aims to ensure that driving-related data uploaded to the cloud can be publicly audited and verified for authenticity. Future work should include incorporating trusted timestamps to ensure the correct time sequence of the data, as well as designing a more comprehensive vehicle forensics tool. While the scheme

addresses data integrity and non-repudiation, it lacks emphasis on other security attributes such as confidentiality, availability, and privacy.

In [32], A.R. Vieira et al. introduces BEDR, a blockchain-based distributed EDR solution for VANETs, designed as an alternative to traditional centralized EDRs. The paper presents a practical experiment using Hyperledger Iroha to simulate the BEDR solution and evaluate its feasibility, particularly in terms of performance. However, BEDR and similar solutions face several challenges for practical use in real-world scenarios, mainly related to scalability, bandwidth, computational demands, and the associated costs. In [34], X. Li et al. propose a blockchain-based cooperative transaction scheme designed to ensure data integrity, incorporating mechanisms to prevent malicious actors, enforced through blockchain and smart contracts. The authors highlight challenges such as intermittent internet connectivity, which prevents real-time updates and transaction validation, and the difficulties in ensuring security and scalability in dynamic environments.

**8. Framework and Processes: *management of automotive digital evidence and simplification of automotive digital forensics processes.***

This category focuses on incorporating ADF practices into systems to enhance accident prediction, traffic violation detection, and forensically sound data collection. Deep learning and blockchain are used in a proposal for a framework for road accidents, utilizing data from road conditions, climate, and driving patterns to predict incidents for specific road segments, accompanied by vehicle warnings from RSUs. Another framework uses a permission-based blockchain along with a public vehicle key infrastructure (VPKI) to securely collect various types of data, such as health data (e.g., from wearable devices) and automotive diagnostics. Yet another data collection system for distributed, decentralized, and mobile entities is proposed to ensure secure storage, including an algorithm for evidence integrity verification. A use case is outlined utilizing the OBD-II port and the tool WireShark, addressing forensic readiness, acquisition, analysis, and documentation. Another proposal applies a Desktop IT forensic process model to the automotive domain, including preparations, data gathering, investigation, and documentation, covering both live and static data from ECUs, sensors, and actuators. Lastly, a proposal for route reconstruction, considering data transmitted over the CAN bus, is suggested to either clear or link individuals to incidents.

**Recent Trends.** J. Liang et al. [14] proposes a block-chain based attribute-based access control model to ensure the integrity and authenticity of forensic data, along with an incentive mechanism based on reputational value creation to classify user behaviors and encourage participation. This aims to reduce insurance disputes and assist law enforcement investigations. A Raspberry Pi represents resource-constrained light nodes, and the framework is deployed via a Hyperledger Fab-

ric blockchain platform. Experiments show that the proposed framework ensures data integrity and promotes user participation. However, challenges exist in terms of scalability, resource limitations, and ensuring fairness in the incentive-based mechanisms. In [23], Y.A. Daraghmi et al. propose a framework for the automatic analysis of dashcam videos, extracting data such as time, date, speed, and GPS coordinates. The framework enables mapping both temporal and spatial evidence to track vehicle routes. Still, as with all video data, privacy concerns arise, as unrelated information, such as individuals and license plates, may be captured.

In [25], T. Bakhshi et al. conducted a survey across law enforcement agencies and identified significant gaps in automotive forensics, such as a lack of standardized methods and reliance on invasive data extraction. In response, they introduced SAFE (Standardized Automotive Forensic Engine), an ML-based tool designed to guide forensic investigators through a step-by-step process. The authors aim to release SAFE as a public web-based application to improve forensic workflows. However, challenges remain, including differences in regulations and jurisdictions, as well as privacy concerns related to the data. Additionally, the framework does not emphasize security measures. In [26], J. Han et al. introduce a conceptual Vehicle Security Operations Center (VSOC) framework aimed at guiding future research and applications. The framework provides a structured approach for managing, detecting, orchestrating, and responding to cybersecurity threats. While the paper discusses various cybersecurity threats and existing countermeasures, the authors acknowledge the challenges of addressing security concerns due to the complex and evolving threat landscape. Additionally, they highlight practical challenges in integrating their solution, given the diversity of automotive technologies and regulatory environments.

In [21], L. Ahmeti et al. propose a forensic approach for handling incidents involving autonomous vehicles within the Gaia-X framework. They emphasize the importance of ensuring security and resilience. The authors present two key use cases: one involves manipulating the vehicle's control unit to enable unauthorized autonomous driving, and the other concerns a Distributed Denial-of-Service (DDoS) attack disrupting communication. The paper applies existing forensic guidelines, to these scenarios and suggests how the Gaia-X framework can assist in investigations. A key challenge discussed is the evolving nature of both autonomous vehicle technology (including V2X communication) and the Gaia-X infrastructure, which is decentralized and complex, making it difficult to establish standardized forensic approaches.

**9. Practical Experiments: *practical cases for forensic investigation, or proposals for data management.*** This category centers around practical experiments on ADF data and related components that can be

used in digital investigations. One study explored vulnerabilities in a Skoda Octavia vRS and proposed that components and data, such as infotainment data, GPS, ECU memory, and diagnostics, could be useful for forensic investigations. Another study focused on forensic artifacts using the iVe tool from Berla Corporation [8] for two infotainment systems (Uconnect and Toyota Extension Box), revealing differences in the available data. The former provided only location data, while the latter contained additional information, such as contact and call logs, and GPS data. Additionally, crash data from the NHTSA database were analyzed in the proprietary EDRX format using a Bosch EDR tool [9]. The analysis revealed that post-2000, vehicle speed, airbag deployment, and engine throttle were recorded, and over time, more data, including diagnostic information, were added. Privacy and security issues were highlighted, raising concerns about the admissibility of such data in court. Other studies extracted data from infotainment systems and communication traffic from various networks (e.g., GSM/3G/4G) with the aim of identifying evidence, such as call records and packet captures (PCAP). Finally, a case study on a Volkswagen Golf highlighted issues, such as how to avoid data loss.

**Recent Trends.** In [13], Y. Yoon et al. conduct a forensic investigation of an Android Jellybean-based infotainment system installed in a Kia K5 2017. The focus is on collecting system logs and navigation logs to analyze their potential for reconstructing events and activities related to accidents or crimes. The system logs contain user data such as Bluetooth connections and navigation guidance, while the navigation logs provide detailed data from the navigation app, including user routes and search destinations. Notably, the approach lacks cybersecurity considerations, such as ensuring data integrity, and the general value is limited due to the study's focus on the specific Android Jellybean-based AVN system.

The categories 10-11 below, as derived from [2], have been outdated; for instance, infrastructure is included in other categories, while we did not find any recent research around ADF and smart cities. Neither TEE nor virtualization has been emphasized in recent research. Thus, we summarize previous research and refer to the discussion section.

**10. Infrastructure/Smart Cities: *infrastructure communication and smart cities.*** Issues are highlighted in handling forensic data from autonomous vehicles (AVs), such as the lack of integrity validation and unprofessional data extraction, compared to other forensic fields. It is argued that methods used both for analysis and for acquiring data for legal purposes are insufficient. A mechanism for securely acquiring AV sensor data and uploading it to the cloud is proposed as a response. Additionally, the integration of smart cars into smart city infrastructure is emphasized. As a case in point, a hypothetical use

case is provided involving a reckless driver and its interaction with other smart entities, along with a forensic investigation process.

**11. TEE/Virtualization: *securing digital evidence using Trusted Execution Environments (TEEs) and/or virtualization.*** This category emphasizes isolated environments. Not much has been done in this area. However, one study proposes a data recording system for automotive applications, i.e., T-BOX, that operates inside a TEE with the purpose of detecting data manipulations, such as removal, replacement, replaying, and truncation of data. However, their approach remains platform-dependent and does not protect data against manipulation before storage. Additionally, confidentiality and privacy considerations are not addressed with regard to the stored data.

DISCUSSION

---

**Recent Trends.** Recent trends emphasize the challenges of data collection and extraction [12, 38]. Earlier studies used tools like Alien-tech KTag [47] and PEMicro Cyclone [48], while [33] demonstrates the successful use of Magnet AXIOM [49]. Current trends reflect a continued effort to adapt existing tools and methodologies to various vehicle systems, enhancing the accuracy and reliability of forensic data extraction. Recent challenges are linked to the increasingly dynamic threat landscape and the expanded vehicle ecosystem, where there is growing dependence on services and connections outside the vehicle (V2X), along with evolving complexities related to software and architectures [44]. There is an urgent need and a clear shift toward adopting newer technologies to address these challenges, with blockchain being notably emphasized [37]. We can also see a trend toward more advanced solutions, such as [10], [16], and [31], which focus on reducing computational and storage demands, enhancing security utilizing blockchain technologies. However, challenges such as cost, infrastructure dependencies, and computational complexity remain.

The IoT Forensics Suite [24] is introduced, practical tool usage is demonstrated [46, 28], and smartphones and apps, such as Android-based tools, are used for collecting vehicle data [19]. However, security remains a significant challenge. Various papers emphasize improving and extending EDRs while balancing privacy, security, and intellectual property protection, using models like MBSE and Magic-Grid V2 [18]. Real-time analysis and scalability are highlighted through novel approaches like clustering [27] and tampering detection via watermarking [36]. Challenges remain, such as mitigating cyberattacks and detecting tampering to ensure trust in forensic evidence [40].

Recent trends highlight the need for more advanced approaches to address challenges such as managing enormous amounts of data. In response, advancements in AI/ML have emerged, along with solutions that integrate blockchain with AI/ML. For instance, the CPBW mechanism is introduced for driver identification using smartphones, and AI/ML integration with blockchain is explored for secure forensic data storage with real-world data [17]. Another blockchain-based solution also utilizes AI/ML techniques as a promising approach [30]. Other efforts focus on data integrity [14], dashcam video analysis for evidence mapping [23], and the SAFE tool for forensic investigations [25]. Additionally, responding to cybersecurity threats is emphasized in [26]. However, despite these advancements, challenges remain in

making blockchain a practical solution. There is also a tendency to address challenges with privacy, traceability, and security for practical applications [11, 15, 32, 34]. For instance, recent approaches focus on privacy through group signatures and secure communication [11], and enhanced integrity using verifiable delay functions [34].

**Future Directions.** The field of ADF is likely to move toward standardization, regulation, and more structured processes and frameworks for data handling (e.g., collection, extraction, and storage), ensuring that common tools and techniques can be applied universally across vehicle systems and manufacturers. As shown in Tables 1 and 2, there is a strong focus on these categories, along with practical experiments that demonstrate their value (categories 1, 2, 8, and 9). While blockchain continues to be explored as a potential solution for enhancing ADF and security, its cost, performance constraints, and infrastructure dependencies make it challenging for broad practical application. Despite its promise, blockchain suffers from various inherent limitations, such as scalability, and is unlikely to serve as a complete solution for ADF with the current limitations in mind. However, blockchain may serve as a supplementary technology integrated with other approaches to enhance ADF. The integration of AI and ML is emerging as a critical response to address and extract value from the massive volume of data generated by modern vehicle systems due to increasing communication and the use of services (both in-vehicle and V2X data). These technologies will be invaluable in automating data analysis, identifying anomalies, and facilitating scalability for ADF.

However, as shown in Tables 1 and 2, there is an important gap in recent research regarding virtualization and TEE. These are cutting-edge technologies that could enhance ADF by securing sensitive data (such as cryptographic keys) through execution in isolation, thus enhancing tamper resistance and preventing data leakage. Additionally, the concept of smart cities has not been widely explored in the context of ADF. Future research is likely to consider how vehicles, through their V2X communication, interact with other smart systems, and the related forensic data that can be inferred from these interactions.

In summary, we forecast the field of ADF to evolve toward standardization and clearer regulations. The integration of AI/ML technologies will become imperative to address the increased volume of data, while blockchain will remain secondary but potentially useful for specific tasks. TEE and virtualization represent potential areas for further research to enhance ADF security. Lastly, as vehicles become more integrated into other smart systems, such as smart city ecosystems, future research will likely explore how this increasingly interconnected environment can benefit ADF with relevant data.

## CONCLUSION

---

We have provided an updated and comprehensive SLR of the field of ADF, categorizing and comparing recent developments with prior research, while highlighting state-of-the-art trends, such as emerging solutions in artificial intelligence, machine learning, and blockchain. By analyzing these solutions from both a security and practical perspective, we offer valuable insights and implications for future research. This SLR not only emphasizes the latest advancements but also presents a forward-looking perspective on the future of ADF. As the automotive industry continues to evolve, we believe our work will be of value to both researchers and practitioners navigating this dynamic and critical field.



## BIBLIOGRAPHY

---

- [1] B. Nelsons, A. Philips, and C. Steuart. *Guide to computer forensics and investigations*. Cengage, 2018.
- [2] Kim Strandberg, Nasser Nowdehi, and Tomas Olovsson. A systematic literature review on automotive digital forensics: Challenges, technical solutions and data collection. *IEEE Transactions on Intelligent Vehicles*, 8(2):1350–1367, 2023.
- [3] Kim Strandberg, Ulf Arnljung, and Tomas Olovsson. The Automotive BlackBox: Towards a Standardization of Automotive Digital Forensics. In *2023 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6, NACernberg, Germany, December 2023. IEEE.
- [4] United Nations Economic Commission for Europe (UNECE). UN Regulation No. 155. <https://unece.org/sites/default/files/2021-03/R155e.pdf>, 2022. Accessed: 2025-01-22.
- [5] United Nations Economic Commission for Europe (UNECE). UN Regulation No. 156, 2022.
- [6] United Nations Economic Commission for Europe (UNECE). UN Regulation No. 160. <https://unece.org/transport/documents/2023/01/standards/un-regulation-no160-revision-1-event-data-recorder-edr-01>, 2023. Accessed: 2025-01-23.
- [7] The International Organization for Standardization. Road vehicles – Cybersecurity engineering. <https://www.iso.org/standard/70918.html>, 2022. Accessed: 2025-01-22.
- [8] Berla Corporation. Ive - vehicle system forensics, 2025. Accessed: 2025-02-21.
- [9] Bosch. Crash data retrieval (cdr) tool, 2025. Accessed: 2025-02-21.
- [10] Yating Li, Liang Xue, Le Wang, Jingwei Liu, and Xiaodong Lin. Secure Approximate Deduplication for Forensic Images in Crowdsensing Vehicular Networks. *IEEE Transactions on Vehicular Technology*, pages 1–14, 2025.
- [11] Trent Menard and Mahmoud Abouyoussef. Towards Privacy-Preserving Vehicle Digital Forensics: A Blockchain Approach. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6, San Antonio, TX, USA, April 2024. IEEE.

- [12] Jung-Hwan Lee, Seong Ho Lim, Bumsu Hyeon, Oc-Yeub Jeon, Jong Jin Park, and Nam In Park. Tesla Log Data Analysis Approach from a Digital Forensics Perspective. *World Electric Vehicle Journal*, 15(12):590, December 2024.
- [13] Yejin Yoon, Jeehun Jung, Seong-je Cho, Jongmoo Choi, Minkyu Park, and Sangchul Han. Forensic Investigation of An Android Jellybean-based Car Audio Video Navigation System. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, pages 1–8, Vienna Austria, July 2024. ACM.
- [14] Jingying Liang, Jing Chen, Rui Zhu, Chen Miao, Kaixian Lu, and Liyang Jiao. Reputation Value-Based Converged Dual-Channel Digital Forensics for Blockchain-Enabled Smart Vehicles. *IEEE Transactions on Intelligent Vehicles*, pages 1–15, 2024.
- [15] Jiangtao Li, Zhaoheng Song, Zihou Zhang, Yufeng Li, and Chenhong Cao. In-Vehicle Digital Forensics for Connected and Automated Vehicles With Public Auditing. *IEEE Internet of Things Journal*, 11(4):6368–6383, February 2024.
- [16] Qi Tao, Hongwei Ding, Tian Jiang, and Xiaohui Cui. B-DSPA: A Blockchain-Based Dynamically Scalable Privacy-Preserving Authentication Scheme in Vehicular Ad Hoc Networks. *IEEE Internet of Things Journal*, 11(1):1385–1397, January 2024.
- [17] Yu-Ming Chen, Phone Lin, En-Hau Yeh, Shun-Ren Yang, and Rongxing Lu. CPBW: A Change-Point-Detection and Bag-of-Words-Based Mechanism Utilizing Smartphone Triaxial Accelerometer Data for Driver Identification. *IEEE Internet of Things Journal*, 11(18):29766–29780, September 2024.
- [18] Mars Rayno and Jeremy Daily. Integrating Model-Based Systems Engineering for Enhanced Digital Forensics in Crash Investigations. In *2024 IEEE International Systems Conference (SysCon)*, pages 1–8, Montreal, QC, Canada, April 2024. IEEE.
- [19] Jiheon Jung, Sangchul Han, Minkyu Park, and Seong-je Cho. Automotive digital forensics through data and log analysis of vehicle diagnosis Android apps. *Forensic Science International: Digital Investigation*, 49:301752, June 2024.
- [20] Zigang Chen, Qinyu Mu, Wenjun Luo, Xingchun Yang, Danlong Li, Xin Shao, Yuhong Liu, and Haihua Zhu. Digital Forensics for Automotive Intelligent Networked Terminal Devices. *IEEE Transactions on Vehicular Technology*, 73(4):5128–5138, April 2024.
- [21] Liron Ahmeti, Klara Dolos, Conrad Meyer, Andreas Attenberger, and Rudolf Hackenberg. A Forensic Approach to Handle Autonomous Transportation Incidents within Gaia-X. *CLOUD COMPUTING*, 2024.

- [22] Mars Rayno and Jeremy Daily. Balancing Digital Forensic Investigation with Cybersecurity for Heavy Vehicle Traffic Crashes. *INCOSE International Symposium*, 33(1):638–648, July 2023.
- [23] Yousef-Awwad Daraghmi and Ibrahim Shawahna. Digital Forensic Analysis of Vehicular Video Sensors: Dashcams as a Case. *Sensors*, 23(17):7548, August 2023.
- [24] R. Amala, K. Renin Roy, G. S. Aravind, S. Dija, and Krithi Manohar. Digital Forensics Analysis of a Vehicle Tracking System. *SN Computer Science*, 4(6):835, October 2023.
- [25] Taimur Bakhshi, Bogdan Ghita, and Ievgeniia Kuzminykh. SAFE: a Standardized Automotive Forensic Engine for Law Enforcement Agencies. In *2023 15th International Conference on Innovations in Information Technology (IIT)*, pages 196–201, Al Ain, United Arab Emirates, November 2023. IEEE.
- [26] Jinpeng Han, Zhiyang Ju, Xiaoguang Chen, Manzhi Yang, Hui Zhang, and Rouxing Huai. Secure Operations of Connected and Autonomous Vehicles. *IEEE Transactions on Intelligent Vehicles*, 8(11):4484–4497, November 2023.
- [27] Bhagyashree Gadekar, R. V. Dharaskar, and V. M. Thakare. An Event Based Digital Forensic Scheme for Vehicular Networks. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(5):383–394, May 2023.
- [28] Mathew Nicho, Maha Alblooki, Saeed AlMutawi, Christopher D. McDermott, and Olufemi Ilesanmi. A Crime Scene Reconstruction for Digital Forensic Analysis: An SUV Case Study. *International Journal of Digital Crime and Forensics*, 15(1):1–20, July 2023.
- [29] Farkhund Iqbal, Ahmad Abbasi, Abdul Rehman Javed, Gautam Srivastava, Zunera Jalil, and Thippa Reddy Gadekallu. Identification and Categorization of Unusual Internet of Vehicles Events in Noisy Audio. In *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, Florence, Italy, June 2023. IEEE.
- [30] Ranu Tyagi, Sachin Sharma, and Seshadri Mohan. Blockchain Enabled Intelligent Digital Forensics System for Autonomous Connected Vehicles. In *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, pages 1–6, Chennai, India, March 2022. IEEE.
- [31] Mohammad Y. AlKhanafseh and Ola M. Surakhi. VANET Intrusion Investigation Based Forensics Technology: A New Framework. In *2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA)*, pages 1–7, Karak, Jordan, November 2022. IEEE.

- [32] Andre R. Vieira, Claudio M. Farias, Wilson S. Melo, and Ewer-ton L. Madruga. BEDR: Blockchain Event Data Recorder. In *2022 IEEE 25th International Conference on Intelligent Transportation Sys-tems (ITSC)*, pages 2716–2721, Macau, China, October 2022. IEEE.
- [33] Kevin Gomez Buquerin and Hans-Joachim Hof. Digital Forens-ics Investigation of the Tesla Autopilot File System. *SECUR-WARE 2022 : The Sixteenth International Conference on Emerging Security Information, Systems and Technologies*, 2022.
- [34] Xinghao Li, Chenchen Tan, Minghao Liu, Tom H. Luan, Longxi-ang Gao, and Youyang Qu. A Blockchain-Based Cooperative Per-ception in Internet of Vehicles. In *2021 IEEE 94th Vehicular Tech-nology Conference (VTC2021-Fall)*, pages 1–6, Norman, OK, USA, September 2021. IEEE.
- [35] Sara Jabeen, Aqsa Jabeen, Syed M. Adnan, and Wakeel Ahmad Rao. Vehicle Make and Model Recognition Using Structural and Pattern Based Feature Descriptors. In *2021 International Conference on Communication Technologies (ComTech)*, pages 73–78, Rawalpindi, Pakistan, September 2021. IEEE.
- [36] Tao Long, Antai Xie, Xiaoqiang Ren, and Xiaofan Wang. Tamper-ing Detection of LiDAR Data for Autonomous Vehicles. In *2021 40th Chinese Control Conference (CCC)*, pages 4732–4737, Shanghai, China, July 2021. IEEE.
- [37] Sadia Hussain, Shahzaib Tahir, Asif Masood, and Ihsan Elahi. Enhanced Trust & Risk Based Access Control, in Autonomous Vehicles, by Using Ethereum vs Hyperledger Platforms Consen-sus Algorithms. In *2024 IEEE 16th International Conference on Ad-vanced Infocomm Technology (ICAIT)*, pages 261–267, Enshi, China, August 2024. IEEE.
- [38] Mirza Ahmad Shayer, Sushana Islam Mim, Nafisha Anjum, Md. Abu Sajid Chowdhury, Noshin Nanjiba Islam Preoshi, and Moin Mostakim. The Car Image Generation Quality of DCGAN and VSGAN: A Comparative Study. In *2024 7th International Con-ference on Informatics and Computational Sciences (ICICoS)*, pages 143–148, Semarang, Indonesia, July 2024. IEEE.
- [39] N. M. Istiak Chowdhury and Ragib Hasan. Security Analysis of Connected Autonomous Vehicles (CAVs): Challenges, Issues, Defenses, and Open Problems. In *2024 IEEE World Forum on Pub-lic Safety Technology (WFPST)*, pages 81–86, Herndon, VA, USA, May 2024. IEEE.
- [40] Ryo Kurachi, Takanari Katayama, Takamitsu Sasaki, Masaki Saito, and Yoshimasa Ajioka. Evaluation of Automotive Event

- Data Recorder towards Digital Forensics. In *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, pages 1–7, Helsinki, Finland, June 2022. IEEE.
- [41] Corey Stathers, Musa Muhammad, Adebamigbe Fasanmade, Ali Al-Bayatti, Jarrad Morden, and Mhd Saeed Sharif. Digital Data Extraction for Vehicles Forensic Investigation. In *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pages 553–558, Sakheer, Bahrain, November 2022. IEEE.
- [42] Jozsef Repas, Lajos Berek, and Miklos Schmidt. Autonomous Vehicles Forensics-The next step of the Digital Vehicles Forensics. In *2022 IEEE 1st International Conference on Cognitive Mobility (CogMob)*, pages 000067–000072, Budapest, Hungary, October 2022. IEEE.
- [43] Syed Rizvi, Mark Scanlon, Jimmy Mcgibney, and John Sheppard. Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions. *IEEE Access*, 10:110362–110384, 2022.
- [44] Prinkle Sharma and James Gillanders. Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art. *IEEE Access*, 10:108979–108996, 2022.
- [45] Roman Rak, Dagmar Kopencova, and Miroslav Felcan. Digital vehicle identity – digital vin in forensic and technical practice. *Forensic Science International: Digital Investigation*, 39:301307, December 2021.
- [46] Simon Ebbers, Fabian Ising, Christoph Saatjohann, and Sebastian Schinzel. Grand Theft App: Digital Forensics of Vehicle Assistant Apps. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pages 1–6, Vienna Austria, August 2021. ACM.
- [47] Alientech. K-tag ecu programming tool, 2025. Accessed: 2025-02-21.
- [48] PEmicro. Arm programming solutions, 2025. Accessed: 2025-02-21.
- [49] Magnet Forensics. Magnet axiom | digital forensic software, 2025. Accessed: 2025-02-24.
- [50] Proton Technologies AG. Complete guide to GDPR compliance. <https://gdpr.eu/>, 2020. Accessed: 2025-02-18.