USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

WIP: A Black Box System for Automotive Digital Forensics

Muhammad Yusuf Bambang Setiadji, Eirini Anthi, and
Theodoros Spyridopoulos, *Cardiff University;* Gareth Davies, *Thales UK*

https://www.usenix.org/conference/vehiclesec25/presentation/setiadji

This paper is included in the Proceedings of the
3rd USENIX Symposium on Vehicle Security and Privacy.

August 11–12, 2025 • Seattle, WA, USA

978-1-939133-49-6

Open access to the Proceedings of the 3rd USENIX Symposium
on Vehicle Security and Privacy is sponsored by USENIX.

WIP: A Black Box System for Automotive Digital Forensics

Muhammad Yusuf Bambang Setiadji
Cardiff University

Eirini Anthi
Cardiff University

Theodoros Spyridopoulos
Cardiff University

Gareth Davies
Thales - United Kingdom

Abstract

Modern vehicles through increased connectivity are growingly susceptible to cybersecurity threats. Research has demonstrated vulnerabilities exploitable via infotainment systems, underscoring the need for robust automotive digital forensics. However, automotive digital forensic lags behind mature computer forensics, facing challenges such as lack of standardized guidelines, specialized tools, and technical limitations in current logging systems. These limitations, such as trigger-based recording, inadequate time synchronization, and insufficient trust preservation, compromise the reliability and legal admissibility of digital evidence. This paper presents a novel black box system designed to overcome these challenges by integrating GPS-based time synchronization and continuous Electronic Control Unit authentication leveraging Unified Diagnostic Services. Extending beyond traditional vehicle logging, Event Data Recorder, the proposed system features expanded memory capacity and data collection. Rigorous testing, including continuous authentication, stress tests, and functional analyses, demonstrates the enhanced capabilities of our black box in ensuring data integrity and credibility. These improvements strengthens the credibility of forensic evidence for legal proceedings involving connected vehicles.

1 Introduction

Modern consumer vehicles are increasingly internet-connected, with projections estimating over 400 million connected vehicles by 2025, up from 237 million in 2021 [1]. Consumers are embracing these vehicles for their perceived safety and efficiency in navigating traffic.

However, greater connectivity also brings increased vulnerability [2], particularly in the automotive sector. Infotainment systems, often the primary point of connectivity, serve as entry points for hackers to remotely access vehicles. This has been demonstrated in studies targeting Jeep [3], Tesla [4], and BMW [5], all of which began with exploits of infotainment or communication modules. Additionally, [6] found that nine out of twelve Internet-exposed automotive devices had access to in-vehicle networks—highlighting the security risks.

These vulnerabilities are particularly concerning in the context of real-world incidents. According to the US National Highway Traffic Safety Administration (NHTSA) Standing General Order on Crash Reporting [7], from 2019 to 2024, 3,979 incidents involved vehicles equipped with Level 2 ADAS or ADS. Tesla led with 2,146 incidents, followed by Waymo (415) and General Motors (219). While not all involved connected vehicles, Tesla's high incident count and known security weaknesses [4] raise a critical question: can we entirely rule out hacker involvement in connected vehicle incidents?

A major challenge in automotive digital forensics is data collection, as highlighted by [8]. Few studies have proposed reliable forensic tools or extraction techniques, and the lack of established guidelines or standards renders the field relatively immature. Mathew et al. [9] identifies several potential data sources, including the Event Data Recorder (EDR), telematics/infotainment (T/I) systems, Electronic Control Units (ECUs), eCALL units, key fobs, cameras, and Vehicle Control History (VCH) data. However, extracting data is complicated by the diversity of vehicle designs, requiring specialised tools. Additionally, both EDR and VCH are trigger-based systems—data is only recorded following predefined events (e.g., a collision) and may be overwritten if no trigger occurs.

Beyond collection challenges, technical limitations in current logging systems further complicate digital forensics. A lack of global time synchronisation across ECUs leads to inconsistencies in event reconstruction, weakening the accuracy of forensic timelines. The absence of trust preservation mechanisms, such as continuous ECU authentication, raises concerns about data authenticity, as logs could originate from unauthorised sources. Notably, the T/I system—identified by [9] as a key source of time and location data—is also a common target for cyberattacks, as it often serves as the primary access point. As a result, data from T/I systems may not meet forensic credibility standards due to possible compromise. These shortcomings not only hinder reliable data extraction

and analysis but also threaten the legal admissibility of digital evidence.

To address these critical gaps, this study proposes a novel black box system to improve forensic readiness in modern vehicles. While similar systems exist, none, to our knowledge, integrate global time synchronisation and continuous ECU authentication. By enabling accurate, authentic, and comprehensive data collection, the system reduces risks related to CAN frame chronological ordering and unauthenticated ECU, offering a more reliable foundation for forensic investigations. The main contributions of this study are:

1. Design and Development of a Novel Black Box
   The proposed black box system uses two sources for timekeeping: GPS time and the logger system clock. This dual-source time helps ensure that the timestamps on the logged data are accurate and available. Additionally, the system utilises Unified Diagnostic Services (UDS) for trust preservation, which verifies that the ECU is indeed legitimate.

2. Enhanced Forensic Readiness
   By extending the data collection beyond traditional CAN bus messages to include globally synchronised time and location information, the system enables more comprehensive event reconstruction. Additionally, unlike Event Data Recorder (EDR) systems, which according to [10] should store twenty seconds of data at 10 Hz, the proposed logger features a larger and more flexible memory capacity that is adaptable to the installed storage.

3. Increased Forensic Data Credibility
   Forensic data serve a crucial role in ensuring legal admissibility in courts. By supplementing recorded data with time and location information, along with continuous authentication, the credibility of forensic evidence can be significantly enhanced [11]. This feature particularly benefits the court by enabling more informed decisions based on the gathered data. Such improvements are essential for the integrity of the justice system as they contribute to fair and accurate outcomes in legal proceedings.

The remainder of this paper is structured as follows: Section II reviews related work on automotive loggers and digital forensics. Section III details the development methodology, while Section IV outlines the technical design. Section V presents testing and results, Section VI discusses the findings, and Section VII concludes the paper.

2 Related Works

Digital forensics in modern vehicles has advanced considerably, yet key challenges persist—particularly in time synchronisation and trust preservation. This section reviews notable research contributions and their limitations, highlighting the need for a more robust approach to forensic readiness.

Mobile-Based Forensic Solutions. Mansor et al. [12] introduced DiaLOG, a mobile app based on the EVITA project, aimed at securing data transmission by allowing only authorised mobile devices to connect to the vehicle. While it ensures data integrity and privacy, its reliance on the under-adopted EVITA framework and costly hardware security modules (HSMs) limits scalability and practical deployment.

In-Vehicle Network Monitoring and Data Recording. Lee et al. [13] proposed the T-Box, a data recorder that uses Shamir's secret sharing and blockchain to protect in-vehicle logs. However, it overlooks time synchronisation and assumes all IVN messages are trustworthy—making it vulnerable to spoofing and lacking zero-trust safeguards.

Forensic Frameworks for Autonomous Vehicles. Hoque et al. [14] developed AVGuard, a forensic investigation framework for autonomous vehicles. AVGuard utilises hash chains, Bloom filters, and log entries from various autonomous driving (AD) modules, with proof of creation using public-key cryptography. AVGuard primarily focuses on developing a forensic framework for autonomous driving (AD) module logging while ensuring data integrity. However, the framework lacks detailed technical implementation regarding critical aspects such as time synchronization mechanisms. Furthermore, it inherently trusts all AD modules during the logging process. In contrast, our proposed approach provides comprehensive technical specifications and implements continuous authentication to address these limitations.

Event Data Recorder (EDR) Analysis. Lee et al. [15] highlighted methods for extracting EDR data to support accident reconstruction. However, the absence of standardised tools, Data Storage Systems for Automated Driving (DSSAD) in most vehicles, and limited data scope reduces its effectiveness. Logs from other security systems are needed for a complete forensic picture.

Vulnerabilities in EDR Systems. Kurachi et al. [16] revealed that EDR data can be tampered with or overwritten and lacks diversity in data types. It is also susceptible to spoofing through fake CAN messages, raising concerns about its reliability in forensic contexts.

Trusted Execution Environments (TEEs) and Blockchain. Kang et al. [17] proposed TB-Logger, which uses Trusted Execution Environments (TEEs) and blockchain for secure logging. While it strengthens integrity and chain-of-custody, it fails to address time synchronisation and key management—leaving ECU spoofing risks unresolved.

Public Audits for Vehicle Data. Li et al. [18] presented a forensic scheme allowing public audits of vehicle data. Despite enhancing transparency, it omits time synchronisation and ECU key management, leaving the system exposed to spoofing and data manipulation.

The reviewed literature demonstrated significant progress in vehicle forensics, particularly in data integrity and secure log-

ging. However, several critical gaps remain in the literature.

- Time Synchronisation: None of the reviewed works adequately address the need for independent and reliable global time synchronisation, which is essential for accurate event reconstruction.
- Trust Preservation: Existing cryptographic approaches often neglect Zero Trust principles, leaving networks vulnerable to persistent malicious attacks [19]. Continuous authentication is critical to verify ECU, which is the source for every CAN frame.
- Comprehensive Logging: Many proposed systems focus on specific components (EDR) and fail to introduce additional features that would support fundamental requirements of a digital forensic, e.g. time synchronization and trust preservation.

These gaps underscore the need for a forensic readiness approach that integrates independent time synchronisation, trust preservation, and comprehensive logging to ensure accurate, authentic, and admissible digital evidence in modern vehicles. Table 1 summarises these challenges and our proposed solution.

Table 1: Summary of Automotive Digital Forensics Research

Ref.	Key Approach	Core Contribution	Limitations
[12]	Mobile forensic app (DiaLOG)	Secure device auth	Data integrity and EVITA dependency; HSM cost issue.
[13]	IVN monitoring (T-Box)	Blockchain secure logging	No time sync; trusts all CAN messages.
[14]	Autonomous vehicle forensic framework (AVGuard)	Hash chain secured logs	Missing time sync and ECU key management.
[15]	EDR analysis methods	Accident reconstruction	EDR data incomplete.
[16]	EDR vulnerability study	Demoed tampering and spoofing	CAN messages is spoofable
[17]	TEE and blockchain logger	Protection for data integrity and chain of custody	No time sync and ECU key management
[18]	Public audit scheme	Transparent vehicle data verification	Lacks time sync and ECU key management
This work	Forensic black box	GPS time sync ZTA logging	Addresses time sync and trust gaps.

3 Research Methodology

This section outlines the methodology based on the Design Science Research (DSR) paradigm [20]. The black box system is developed through iterative cycles of design, implementation, and validation to improve vehicle forensic readiness. Guided by DSR principles, the process defines the objectives, framework, and evaluation methods. This study begins with the "Identify Problem" stage, following a Problem-Centred Initiation. The DSR process steps are as follows:

1. **Identify Problem**: Insufficient data for Automotive Digital Forensic.
2. **Define Objectives**: Develop a system to increase vehicle digital forensic readiness.
3. **Design and Development**: Black box logger with added GPS time, location, and ECU authentication.
4. **Demonstration**: Proof of concept with commercially off the shelf hadware and custom software.
5. **Evaluation**: Asses effectiveness, performance, and security. From this particular step, it is possible for the DSR process to cycle around to step "Define Objectives" or "Design and Development".
6. **Communication**: Submitted to journal or conference.

4 Artefact Description

This section outlines the black box system architecture, features, and alignment with the research objectives.

4.1 Black Box at a Glance

Before introducing our proposed black box, we first review the general features of black box systems. Due to the absence of mature automotive standards, we reference established aviation practices and adapt relevant principles. According to aviation standards [21], black boxes typically include the following features:

- Crash-Survivable Memory;
- Continuous Data Recording with Pre-Event Buffering;

- Tamper-Proof Design;
- Multimodal Data Capture;
- Independent Power Supply.

The automotive sector is developing its own standards and best practices to address the unique challenges of road vehicles, while also drawing insights from data recording systems in other transport sectors, such as aviation. Based on [22], the general features of an automotive black box include:

- Tamper-Evident Enclosure;
- High Frequency Sampling;
- Submersion Resistance;
- Time Synchronisation;
- Multi-Type Data Recording.

Black box systems offer various advanced features, but this study focuses on three essential functions: time synchronisation, multi-type data recording, and continuous authentication—key to ensuring reliable forensic evidence and supporting legal admissibility.

4.2 Design Details

The black box system comprises three core components: a hardware module, a GPS module, and an authentication system. This minimal yet efficient configuration meets the research objective of improving vehicle cybersecurity and forensic readiness. The hardware module is compact and designed for easy integration into an existing vehicle CAN network, either via the OBD-II port or direct connection to the CAN High/Low terminals.

Operating independently from the vehicle's network, the black box maintains its integrity even if primary systems are compromised. It functions as the central processing and storage unit, interfacing with the GPS module for time and location data and managing UDS communication for continuous ECU authentication.

For the proof of concept, a Raspberry Pi 5 with 4GB RAM and an RS485 CAN Hat were used. The software runs on Raspberry Pi OS, with the logging application developed in Python. An illustration of the setup is shown in Figure 1B.

Although the UDS protocol was not initially intended for continuous authentication, our research demonstrates its feasibility based on industry adoption criteria by Nowdehi et al. [23]. UDS offers key advantages: it requires no additional hardware beyond the proposed logger, ensures full backward compatibility with existing vehicle systems, and meets essential adoption requirements such as maintenance support, implementation feasibility, and low system overhead. We repurpose UDS Security Access and Firmware Version Query (Services 0x27 and 0x22) to enable continuous authentication by inferring ECU state. This method retains all native ECU diagnostic functions while adding security verification without disrupting normal operations or requiring vehicle modifications.

According to [24], CAN 2.0 supports up to 1 Mbps, though most real-world applications use 500 kbps. This research adopts 500 kbps as the operating rate to justify using the Raspberry Pi 5. While not inherently real-time, the Raspberry Pi can be enhanced with real-time patches for reliable message handling. Its GPIO pins support CAN controllers, and SPI/I2C interfaces allow easy integration with CAN transceivers. Additionally, it uses SocketCAN, a Linux kernel-integrated CAN interface, to ensure reliable logging at 500 kbps.

The GPS module provides time synchronisation and positioning in our proof of concept, which uses the DIYMall VK-162 G-Mouse. This module was chosen for its cost-effectiveness, accuracy, and compatibility with the Raspberry Pi [25]. The black box software reads GPS output and appends time and location data alongside CAN data and the internal clock (used as a secondary time source). Both timestamps are recorded simultaneously to provide redundancy and ensure reliable temporal data in case of failure in either system.

We argue that continuous ECU authentication aligns with Zero Trust Architecture (ZTA) principles. By verifying firmware versions via UDS, the system ensures only authorised and up-to-date software is active, supporting ZTA's identity verification model. Continuous UDS-based checks help detect ECU tampering or unauthorised updates, reinforcing ZTA and enhancing overall vehicle security [26].

For our continuous authentication proof-of-concept, a CAN network simulates three critical ECUs (Engine Control, Brake Control, Airbag Control Modules) using three Arduino Uno boards with MCP2515 CAN transceivers. This minimal subset, validated by prior research for generalisability [27, 28, 29], generates crash-relevant data (speed, braking, impact) crucial for forensics, as non-critical ECUs do not significantly impact authentication outcomes. The Arduino Uno platform, chosen for its standardised use in automotive prototyping and reliable CAN bus simulation in peer-reviewed studies [30], facilitates this simulation which is illustrated in Figure 1A. Each ECU executes a challenge-response protocol, broadcasting its firmware version upon successful authentication, with these responses logged alongside regular CAN traffic.

4.3 Impact of Artefact on Research Objectives

The black box system directly addresses the research objectives outlined in this study in the following key areas:

1. Enhancing Automotive Digital Forensic Readiness. The system ensures digital forensic readiness for in-vehicle networks by collecting admissible digital evidence from authenticated sources with synchronized timestamps.

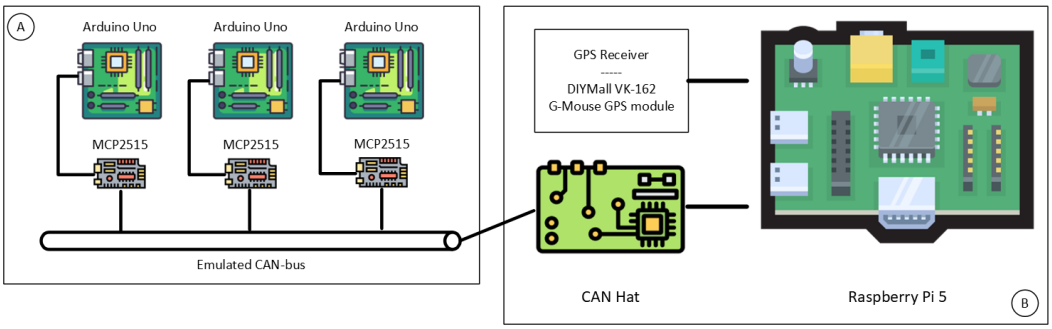

Figure 1: Hardware Module and ECU Simulation

2. Ensuring Global Time Synchronisation. To ensure log credibility, the proposed black box introduces an independent time synchronization mechanism, a capability currently absent in existing systems.

3. Enabling Continuous ECU Authentication. Aligning with Zero Trust Architecture, the black box periodically authenticates ECU firmware integrity using the UDS protocol.

In summary, the black box system fulfills the research objectives by providing a secure, reliable, and efficient solution for automotive digital forensics. Critically, it has the ability to reconstruct event, that will aid in determining accident causes, distinguishing between driver error, manufacturing defects, and cyberattacks, thus addressing a key research objective.

5 Prototype Implementation and Validation

This section details the prototype implementation, developed to demonstrate the feasibility of the proposed black box system, and its validation, which tested the system's limits. Two distinct simulation environments were established: a simulated vehicle environment using multiple Arduinos as ECU simulators, and a pre-existing car simulator in our university lab to represent a real vehicle environment.

5.1 Prototype Implementation

To approximate real-world conditions, as direct implementation in an actual car is currently infeasible, the testing environment utilized components standard in modern vehicles, including an OBD-II port, CAN bus protocol, and a real vehicle instrument cluster. As depicted in Figure 2, Euro Truck Simulator 2 provided in-game telemetry data, captured by SimHub and transmitted via USB to an Arduino CAN Translator. This translator converted telemetry into CAN frames compatible with the instrument cluster, which recognizes manufacturer-specific CAN frames. The CAN translator's output fed both the instrument cluster and the OBD-II port, where the proposed black box was connected. Prior automotive research has validated the use of Euro Truck Simulator 2 and its supporting devices for generating telemetry outputs and realistic driving scenarios as a cost-effective and scalable alternative to real-world data collection [31, 32].

Six distinct logs of varying duration were collected from

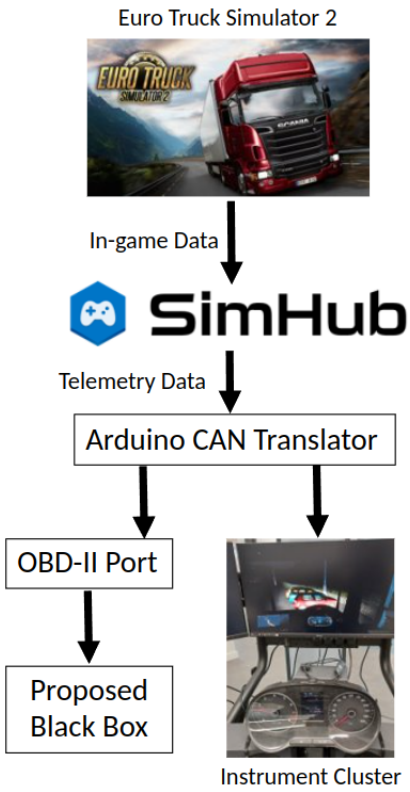

Figure 2: Car Simulation Setup

the car simulation setup, encompassing both stationary and moving in-game vehicle scenarios. Notably, the stationary vehicle logs consistently yielded a higher data volume than

Table 2: Logs From Car Simulation Setup

Status	Log Size	Top Three CAN ID
Moving Vehicle, 17 Minutes Logs	64.8 MB	800, 1136, 80
Moving Vehicle, 15 Minutes Logs	56.9 MB	800, 1136, 80
Moving Vehicle, 4 Minutes Logs	13.8 MB	800, 80, 1136
Stationary Vehicle, 30 Minutes Logs	160 MB	800, 1136, 80
Stationary Vehicle, 30 Minutes Logs	158 MB	800, 80, 1136
Stationary Vehicle, 5 Minutes Logs	77.28 MB	800, 1136, 80

Table 3: UDS Authentication - Legitimate

UDS Authentication Exchange	Explanation
`ID: 1792, Data: 2701, DLC: 2`	Enabling security access, black box to ECU.
`ID: 1792, Data: 670112, DLC: 3`	ECU send seed: 0x12.
`ID: 1792, Data: 270244, DLC: 3`	Black box responds with key generated from seed: 0x44
`ID: 1792, Data: 6702, DLC: 2`	Security access granted, ECU to black box
`ID: 1792, Data: 2276312E3200, DLC: 6`	ECU sends firmware version: v1.2

those from the moving vehicle. Analysis of the captured CAN bus traffic revealed a consistent frequency pattern in CAN IDs, with the same three identifiers consistently exhibiting the highest transmission rates. Please refer to Table 2 for the details. These logging results demonstrate the effectiveness of our proposed black box system in consistently capturing and recording CAN frames across different vehicle states, validating its reliability as a logging mechanism regardless of whether the vehicle is stationary or in motion.

Following the validation of the logging capabilities, we assessed the GPS functionality of the black box to ensure accurate time and location data integration. Each log entry contained the following information (position data obfuscated to protect contributor privacy):

1. System time: `2025-02-10T11:40:37`
2. GPS time: `2025-02-10T11:40:37`
3. Position: `Lat:xx.487819155 - Lon:yy.15166174`
4. CAN Frame: `ID: 320, Data: 000000c24bd05000, DLC: 8`

The final implementation test focused on continuous ECU authentication. Table 3 details the UDS authentication exchange logged by the black box (left column), starting with security access initiation (SID "27", Data: 2701) and the response (SID "67", Data: 670112) [33]. Simulated across three Arduino ECUs (CAN IDs 1792-1794), the log snapshot demonstrates the black box's concurrent success in UDS authentication and separate-thread logging, with message explanations provided in the right column for clarity.

5.2 Prototype Validation

The validation phase assessed the prototype's performance and suitability for digital forensics. This subsection presents the testing methodology, results analysis, and proof of concept for both the logging system and ECU authentication. The prototype underwent three tests: ECU Authentication, Performance Analysis, and Functional Analysis.

ECU authentication was initially tested by introducing an unauthorised ECU (Table 4). Two scenarios were observed: (1) communication failure due to an unrecognised security access CAN ID trigger (Table 4, Possibility 1), and (2) identification as illegitimate due to an incorrect firmware version despite a valid seed key (Table 4, Possibility 2). In both cases, the black box precisely timestamped and geolocated all message exchanges. As a passive logging system, the black box recorded these illegitimate UDS authentication attempts without generating alarms or flags.

The second phase stress-tested the black box by transmitting 6,000 CAN frames at 1ms intervals (1,000 frame per second) from an Arduino. Three configurations were used: a single-Arduino baseline for reference; a dual-Arduino setup to assess doubled load; and a triple-Arduino setup simulating peak CAN network traffic.

To ensure statistical validity, the dual-transmitter configuration was tested nine times, while the triple-transmitter setup was limited to five trials due to consistent anomalies observed at triple the CAN frame rate—indicating the system had reached its performance threshold. Further testing was unlikely to yield additional insights. The test results are as follows:

1. **Single Arduino**. No packet loss, no anomalies;
2. **Two Arduino**. Packet loss was observed in nine test runs, with the number of lost packets recorded as follows: 2, 1, 6, 5, 20, 14, 0, 8, and 0. No anomalies were detected during these tests.
3. **Three Arduino**. Packet loss was recorded across five tests, with the number of lost packets being 9, 520, 165, 4, and 285 respectively. Anomalies were also detected

Table 4: UDS Authentication - Illegitimate

UDS Authentication Exchange	Explanation
Possibility (1)	
ID: 1792, Data: 2701, DLC: 2	Enabling security access, black box to ECU.
ID: 1792, Data: 2701, DLC: 2	Enabling security access, black box to ECU.
ID: 1792, Data: 2701, DLC: 2	Enabling security access, black box to ECU. No response from ECU.
Possibility (2)	
ID: 1792, Data: 2701, DLC: 2	Enabling security access, message is from black box to ECU.
ID: 1792, Data: 670112, DLC: 3	ECU send seed: 0x12.
ID: 1792, Data: 270244, DLC: 3	Black box responds with key generated from seed: 0x44
ID: 1792, Data: 6702, DLC: 2	Security access granted, message is from ECU to black box.
ID: 1792, Data: 223030303000, DLC: 6	ECU sends firmware version: 0000. Incorrect firmware version.

for messages with ID 4, with 4, 8, 2, 1, and 4 anomalous packets identified in each test.

The black box, handling 1,000 frame per second in single-Arduino stress tests, showed a significant margin over our automotive simulation rig's, Figure 2, where it outputs 493-514 frames per second (51.4% throughput), suggesting resilience to packet loss under simulated loads. This margin suggests that the proposed black box system is unlikely to experience packet loss or anomalies under simulated vehicular network loads. It is vital to understand that the black box logger is programmed to passively capture all CAN frames in transit without differentiating between specific ID. However, while these findings are encouraging, it is crucial to acknowledge that this assumption is based on controlled laboratory conditions, therefore requires further validation in diverse real-world scenarios.

Furthermore, the observed anomaly of CAN frames with ID 4 during stress tests holds significant implications for digital forensic investigations. These anomalous frames can compromise data integrity through false information, obfuscate malicious commands by their unexpected appearance, and distort established communication patterns, thereby complicating the accurate reconstruction of events. Hence, it is important to determine the origin of these anomalous frames and to evaluate whether enhancing the black box logging capabilities could effectively mitigate such issues.

To minimise vehicle disruption, continuous authentication should be scheduled during low-activity periods [34] (below 30% bus utilisation). Leveraging non-intrusive UDS diagnostics [35], the UDS authentication tests (Table 3) demonstrated a negligible 1% average bus load increase (5 extra messages/ECU), preserving real-time performance and ensuring data integrity for forensic investigations.

The third validation is a functional analysis that would demonstrate the functionality of our proposed approach, although it is paramount to understand the CAN frame structure in advance. From [36], it can be concluded that the CAN frame structure lack timestamp, because it primarily focus on transmission and arbitration. Hence, timestamps should come from an external source. This practice is reflected in recent automotive research, where artificial intelligence and machine learning studies routinely augment CAN-logged datasets with external timestamp data prior to processing, as evidenced by recent works [37, 38].

Figure 3 shows a typical CAN frame structure, which notably lacks timestamp data. This fundamental limitation of the CAN protocol highlights the motivation for our proposed black box. Key improvement is the integration of timestamps during data capture (rather than after logging), which preserves exact event in chronological order. The difference can clearly be visible when comparing Figure 3 (raw CAN frame without timing data) and Figure 4 (the proposed black box log with timestamps). In Figure 4, the last line precisely records when an attack occurred - a capability missing in standard CAN frame.

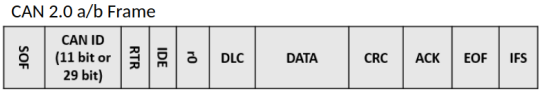

Figure 3: CAN 2.0 Frame [36]

6 Discussion

This study successfully demonstrates a feasible black box system for automotive digital forensic readiness. The prototype effectively integrated ZTA via continuous ECU authentication and precise time synchronisation, addressing current forensic gaps. Stress testing confirmed robust performance up to 2,000 packets per second, confirming its capability to handle real-world vehicular conditions.

The results indicate that this black box significantly enhances vehicle security and forensic capabilities. Continuous authentication maintains a legitimate ECU inventory on the CAN bus, while logging provides temporal evidence of unauthorised modifications or intrusions. The dual time-synchronisation mechanism provides reliable temporal data, which is crucial for forensic investigations. These findings

Figure 4: Log Snippet - Replay Attack

```
SNIP - GPS:2025-02-14T15:29:57.000Z - Lat:15.487819155 - Lon:23.15166174 - ID: 1792, Data: 2701, DLC: 2
SNIP - GPS:2025-02-14T15:29:57.000Z - Lat:15.487819155 - Lon:23.15166174 - ID: 1792, Data: 670112, DLC: 3
SNIP - GPS:2025-02-14T15:29:57.000Z - Lat:15.487819155 - Lon:23.15166174 - ID: 1792, Data: 270244, DLC: 3
SNIP - GPS:2025-02-14T15:29:57.000Z - Lat:15.487819155 - Lon:23.15166174 - ID: 0000, Data: 2701, DLC: 3
```

suggest the system improves cybersecurity and strengthens the legal admissibility of vehicle digital evidence.

The comprehensive logging capabilities of the black box system enable forensic investigators to attribute accident causation with greater certainty. By maintaining records of the ECU firmware version, CAN bus traffic, and temporal data, the system can distinguish between the following:

1. Driver-related incidents through logged driver inputs and vehicle responses, e.g. data from brake and acceleration control, can reveal if driver inputs were consistent with the accident scenario;

2. Consistent anomalies or failures in a specific ECU may indicate manufacturing defects, allowing forensic analysts to trace back to potential design or production issues;

3. Unauthorized ECU modifications or unexpected behaviour in vehicle systems can be indicative of hacking attempts, with authentication logs providing evidence of tampering.

This multilayered data collection approach, combined with guaranteed data credibility through ZTA, provides investigators with reliable evidence for determining accident responsibility. For instance, sudden brake failure can be traced to driver error (through input logs), manufacturing defects (through ECU performance history), or malicious interference (through ECU authentication logs).

Unlike existing literature focused on post-collection processing [13, 14, 17, 18], which overlook the possibility of ECU spoofing during collection, this research addresses the gaps of legal admissibility and zero-trust architecture in automotive forensics. The proposed system implements ZTA through continuous ECU authentication to ensure data source integrity. Furthermore, integrated time and position data enhance evidential weight, meeting legal admissibility requirements [39]. This forensic readiness approach advances beyond existing post-collection analysis by authenticating evidence sources and including temporal data for legal proceedings.

This study holds key implications for both the automotive industry and digital forensics. For manufacturers, the proposed black box offers a scalable cybersecurity enhancement without impacting CAN bus performance. For forensic analysts, it enables reliable collection and verification of digital evidence, improving investigation accuracy. This dual utility makes the system a valuable asset for securing automotive networks and supporting legal processes.

The viability of the proposed system for industrial adoption can be evaluated against the five key requirements established by Nowdehi et al. [23]. The following analysis demonstrates the manner in which the proposed system addresses each requirement.

1. Cost-effectiveness. A proof-of-concept black box logger was constructed for less than £120 using commercial off-the-shelf (COTS) components. Implementation costs can be further reduced through bulk procurement and industrial-scale manufacturing.

2. Backward compatibility: The prototype is programmed to be compatible with CAN 2.0A protocol, supporting 11-bit identifiers. Although theoretically plausible, empirical validation remains necessary for newer CAN protocols (CAN 2.0B, CAN-FD, and CAN-XL).

3. Support for vehicle repair and maintenance: The system's non-intrusive design ensures minimal impact on routine vehicle maintenance and repair procedures. The device operates independently of the existing vehicle systems and requires no modification to the established service.

4. Sufficient implementation details: The system is a plug-and-play architecture, minimising deployment complexity and technical barriers to adoption. This approach ensures straightforward integration into the existing vehicular CAN networks.

5. System overhead: The authentication mechanism generates minimal network overhead, utilising a maximum of five UDS frames per ECU during successful authentication. This represents an insignificant proportion of the CAN bus channel capacity (520 frames per second), ensuring a negligible impact on network performance.

7 Conclusion and Future Works

In conclusion, this study addresses the critical gaps in automotive digital forensics through the development of a novel black box. By incorporating GPS-based time synchronisation, continuous ECU authentication, and comprehensive data collection capabilities, the system improves upon the

existing logging mechanisms. The integration of temporal and spatial data coupled with authentication mechanism enhances the credibility and legal admissibility of forensic evidence. These advancements are particularly valuable in court proceedings where the reliability of digital evidence is paramount. Furthermore, the system's expanded memory capacity and improved data collection mechanisms provided investigators with a more complete picture of vehicle-related incidents. As the automotive industry continues to evolve towards increased connectivity, forensic capabilities will become increasingly vital.

While the prototype effectively confirmed the essential functions of the black box system, certain limitations are identified and require further exploration. For example, the simulated environment, although effective for initial testing, may not fully represent the complexities of real-world vehicular networks. Future research should focus on three key areas: logged data integrity and security, memory modules with high environmental resilience (e.g. crash resistant), and privacy compliance for handling evidence. Additionally, long-term reliability assessments under various operational conditions are crucial for ensuring sustained performance. These improvements can contribute to a more robust and trustworthy system that can effectively address the evolving challenges of vehicle connectivity and cybersecurity.

Acknowledgements

We thank the Indonesia Endowment Fund for Education (Lembaga Pengelola Dana Pendidikan, LPDP) for providing the scholarship opportunity. Additionally, we would like to thank Thales - UK for their technical research support and industry insights.

References

[1] Martin Placek. *Topic: Connected cars worldwide*. Dec. 2023. URL: https://www.statista.com/topics/1918/connected-cars/.

[2] Yara Amelia Contijoch. *Increasing Connectivity Means Increasing Civilian Vulnerability in Developed and Developing Countries*. 2020.

[3] Charlie Miller and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle". In: *Black Hat USA* 2015.S 91 (2015), pp. 1–91.

[4] Sen Nie, Ling Liu, and Yuefeng Du. *FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS*. Black Hat, 2017.

[5] Zhiqiang Cai, Aohui Wang, and Wenkai Zhang. *0-days and Mitigations: Roadways to Exploit and Secure Connected BMW Cars*. Keen Security Lab, 2019.

[6] Takahiro Ueda et al. "An Internet-Wide View of Connected Cars: Discovery of Exposed Automotive Devices". In: Association for Computing Machinery, Aug. 2022, pp. 1–8. DOI: 10.1145/3538969.3543802.

[7] *Standing General Order on Crash Reporting | NHTSA — nhtsa.gov*. https://www.nhtsa.gov/laws-regulations/standing-general-order-crash-reporting. [Accessed 05-02-2025].

[8] Kim Strandberg, Nasser Nowdehi, and Tomas Olovsson. "A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection". In: *IEEE Transactions on Intelligent Vehicles* 8.2 (2023), pp. 1350–1367. DOI: 10.1109/TIV.2022.3188340.

[9] Mathew Nicho et al. "A crime scene reconstruction for digital forensic analysis: An SUV case study". In: *International Journal of Digital Crime and Forensics (IJDCF)* 15.1 (2023), pp. 1–20.

[10] U.S. National Highway Traffic Safety Administration. *Event Data Recorders*. https://www.federalregister.gov/documents/2024/12/18/2024-29862/event-data-recorders. Dec. 18, 2024. (Visited on 04/29/2025).

[11] Céline Vanini et al. "Was the clock correct? Exploring timestamp interpretation through time anchors for digital forensic event reconstruction". In: *Forensic Science International: Digital Investigation* 49 (2024), p. 301759. DOI: 10.1016/j.fsidi.2024.301759.

[12] Hafizah Mansor et al. "Log your car: The non-invasive vehicle forensics". In: IEEE, Aug. 2016. DOI: 10.1109/TrustCom/BigDataSE/ISPA.2016.162.

[13] Seungho Lee et al. "T-Box: A Forensics-Enabled Trusted Automotive Data Recording Method". In: *IEEE Access* 7 (2019), pp. 49738–49755. DOI: 10.1109/ACCESS.2019.2910865.

[14] Mohammad Aminul Hoque and Ragib Hasan. "AVGuard: A Forensic Investigation Framework for Autonomous Vehicles". In: *ICC 2021 - IEEE International Conference on Communications*. 2021, pp. 1–6. DOI: 10.1109/ICC42927.2021.9500652.

[15] Yousik Lee and Samuel Woo. "Practical Data Acquisition and Analysis Method for Automobile Event Data Recorders Forensics." In: *J. Internet Serv. Inf. Secur.* 12.3 (2022), pp. 76–86.

[16] Ryo Kurachi et al. "Evaluation of automotive event data recorder towards digital forensics". In: *2022 IEEE 95th Vehicular Technology Conference*. 2022, pp. 1–7.

[17] Dongwoo Kang and Hyo Jin Jo. "TB-logger: secure vehicle data logging method using trusted execution environment and blockchain". In: *IEEE Access* 11 (2023), pp. 23282–23292.

[18] Jiangtao Li et al. “In-Vehicle Digital Forensics for Connected and Automated Vehicles With Public Auditing”. In: *IEEE Internet of Things Journal* (2023).

[19] Yuanhang He et al. “A Survey on Zero Trust Architecture: Challenges and Future Trends”. In: *Wireless Communications and Mobile Computing* 2022.1 (2022), p. 6476274. DOI: 10.1155/2022/6476274.

[20] Marcus A. Rothenberger Ken Peffers Tuure Tuunanen and Samir Chatterjee. “A Design Science Research Methodology for Information Systems Research”. In: *Journal of Management Information Systems* 24.3 (2007), pp. 45–77. DOI: 10.2753/MIS0742-1222240302.

[21] Waleed Raza et al. “Flight Data Recorders: Past, Present, and Future”. In: *IEEE Aerospace and Electronic Systems Magazine* 39.9 (2024), pp. 120–145. DOI: 10.1109/MAES.2023.3335333.

[22] “IEEE Standard for Motor Vehicle Event Data Recorder (MVEDR)”. In: *IEEE Std 1616-2021 (Revision of IEEE Std 1616-2004)* (2021), pp. 1–184. DOI: 10.1109/IEEESTD.2021.9654153.

[23] Nasser Nowdehi, Aljoscha Lautenbach, and Tomas Olovsson. “In-Vehicle CAN Message Authentication: An Evaluation Based on Industrial Criteria”. In: *2017 IEEE 86th Vehicular Technology Conference*. 2017, pp. 1–7. DOI: 10.1109/VTCFall.2017.8288327.

[24] He Li et al. “Cumulative Message Authentication Codes for Resource-Constrained IoT Networks”. In: *IEEE Internet of Things Journal* 8 (2021), pp. 11847–11859. DOI: 10.1109/JIOT.2021.3074054.

[25] Salam Dhou et al. “An IoT Machine Learning-Based Mobile Sensors Unit for Visually Impaired People”. In: *Sensors* 22.14 (2022). ISSN: 1424-8220. DOI: 10.3390/s22145202.

[26] John Anderson et al. “A Zero-Trust Architecture for Connected and Autonomous Vehicles”. In: *IEEE Internet Computing* 27.5 (2023), pp. 7–14. DOI: 10.1109/MIC.2023.3304893.

[27] Zachary King. “Investigating and securing communications in the Controller Area Network (CAN)”. In: *2017 International Conference on Computing, Networking and Communications (ICNC)*. 2017, pp. 814–818. DOI: 10.1109/ICCNC.2017.7876236.

[28] Hyo Jin Jo et al. “MAuth-CAN: Masquerade-Attack-Proof Authentication for In-Vehicle Networks”. In: *IEEE Transactions on Vehicular Technology* 69.2 (2020), pp. 2204–2218. DOI: 10.1109/TVT.2019.2961765.

[29] Hyeran Mun, Kyusuk Han, and Dong Hoon Lee. “Ensuring safety and security in CAN-based automotive embedded systems: A combination of design optimization and secure communication”. In: *IEEE Transactions on Vehicular Technology* (2020), pp. 7078–7091.

[30] Jia Zhou et al. “Clock-Based Sender Identification and Attack Detection for Automotive CAN Network”. In: *IEEE Access* 9 (2021), pp. 2665–2679. ISSN: 21693536. DOI: 10.1109/ACCESS.2020.3046862.

[31] Cheol-jin Kim et al. “End-to-end deep learning-based autonomous driving control for high-speed environment”. In: *The Journal of Supercomputing* 78.2 (2022), pp. 1961–1982.

[32] SimHub Team. *SimHub: Racing Dashboard and Hardware*. https://www.simhubdash.com/. Accessed on 2025-02-15.

[33] Martin Falch. *UDS Protocol Tutorial - Unified Diagnostic Services*. https://www.csselectronics.com/pages/uds-protocol-tutorial-unified-diagnostic-services. Accessed on 2025-02-15.

[34] Nicolas Navet, Y-Q Song, and Françoise Simonot. “Worst-case deadline failure probability in real-time applications distributed over controller area network”. In: *Journal of systems Architecture* (2000), pp. 607–617.

[35] Sekar Kulandaivel et al. “CANdid: A Stealthy Stepping-Stone Attack to Bypass Authentication on ECUs”. In: *ACM J. Auton. Transport. Syst.* (Apr. 2024). DOI: 10.1145/3657645.

[36] Steve Corrigan HPL. “Introduction to the controller area network (CAN)”. In: *Application Report SLOA101* (2002), pp. 1–17.

[37] Byung Il Kwak, Jiyoung Woo, and Huy Kang Kim. “Know your master: Driver Profiling-based Anti-theft method”. In: *PST 2016*. 2016.

[38] Brooke Lampe and Weizhi Meng. “can-train-and-test: A curated CAN dataset for automotive intrusion detection”. In: *Computers & Security* 140 (2024), p. 103777. DOI: 10.1016/j.cose.2024.103777.

[39] John Tan. *Forensic readiness*. 2001.