**International Journal of Environmental Sciences**
ISSN: 2229-7359
Vol. 11 No. 18s, 2025
https://www.theaspd.com/ijes.php

# A Digital Forensics Framework For Vehicles

**Ashish Kumar Sharma[1*], Sumitra Singar[2],Vishwas Bhardwaj[3]**

[1*]*Research Scholar, Bhartiya Skill Development University, Jaipur*
[2]*Assistant Professor, Bhartiya Skill Development University, Jaipur*
[3]*Assistant Director, State Forensic Science Laboratory, Jaipur*

***Abstract:***
*Vehicle digital forensics is a rapid growing sub domain of cyber forensic investigations on vehicles involved in crimes or in accidental cases. It focuses on collection, extraction and analysis of the digital evidence preserved from a vehicle subject.*
*Modern vehicles are becoming more and more computers themselves by incorporating many advance technologies like ECUs, Infotainment system, ADAS system, Telematics and GPS systems, ABS, Traction and Rollover control etc.,*
*On one side these advanced enhancements push more safety and convenience while other side they bring new vulnerabilities and challenges in digital forensic investigations. While a normal personal car may have around 40 ECUs, a luxury or sports car may have even more than 150 ECUs and this number itself vary for heavy vehicles used in long distance transport along with millions of lines of codes for enabling the overall integrated vehicle system. It further fuels the complexity of a vehicle internal digital and electronic system and imposing many challenges in their forensic examination even more when no fully functional and well accepted vehicular forensic framework is in place.*
*In this paper we propose a comprehensive digital forensic framework for modern vehicles. Vehicle digital forensic framework will provide a systematic guideline to conduct digital forensic investigation on any subject vehicle by acquiring data from advance digital and electronic equipment and sensors such as Event Data Recorder (EDR), Telematics and GPS systems etc., It will also provide invaluable insights for law enforcement and accident reconstruction experts. This framework aims to provide actionable insights to investigators, ensuring accurate and efficient resolution for digital forensic investigations of modern vehicles.*

***Keywords:*** *Forensic Framework, Cyber Forensics Framework, Automobile Digital Forensics, Event Data Recorder, Vehicle Forensics.*

## I. INTRODUCTION

Use of advance digital and electronic systems such as Event Data Recorders (EDRs), GPS, Telematics and Infotainment systems, etc., generates huge amount of potential digital evidence, which helps in vehicle digital forensic examination in road accidents and other criminal activities where a vehicle is involved. This amount and size of data varies significantly from vehicle to vehicle based upon the type of brand, model of vehicle and the respective technologies used. For example, in Electric Vehicles (EVs), there are more electronic parts than the traditional vehicles using Internal Combustion Engines (ICEs) and a typical sport car may produce even more digital data. The digital data extracted from vehicles can be found crucial in investigating accidents, insurance fraud, cyber-attacks, and other criminal incidents.

However, the complexity of these systems and lack of standardized forensic procedures pose significant challenges for forensic investigators. The Law Enforcement Agencies (LEA), find it very difficult to perform digital forensic investigation considering the complex and heterogeneous nature of these data sets. This need for a structured approach of collecting and analyzing the digital data, has developed automobile digital forensics as a specialized field.

Vehicle digital forensics is an emerging branch of forensic science, which concentrates on the retrieval, analysis, and interpretation of data generated by vehicles involved in traffic collisions, insurance fraud and other related crimes. By leveraging modern technologies, such as telematics, vehicle event data recorders, and GPS systems, automobile forensics provides invaluable insights for law enforcement and accident reconstruction experts.

This paper reviews the current state of vehicular digital forensics in place, highlights the key areas of interest, and proposes a framework for conducting a structured vehicle digital forensic investigations. This research work focuses on current methodologies, challenges, and future advancements in the field.

**1. Key Areas in Automobile Forensics**

**1.1. Event Data Recorders (EDRs)**:

EDRs, often referred to as the "black box" of vehicles, capture critical data during crashes, including speed, braking, airbag deployment, and engine performance.

**1.2. Telematics, GPS Systems & Data Logging**:

- Telematics systems in vehicle are responsible to track and log its GPS location, speed, and driving behavior. These systems play an essential role in understanding the context of accidents and criminal activities.
- Retrieval of data from telematics systems, including: Vehicle speed, acceleration, and braking patterns.
- Battery performance metrics for EVs, such as state of charge (SOC) and temperature.
- GPS and route data for contextual understanding of incidents.

**1.3. Infotainment Systems**:

The digital interfaces in modern vehicles store data about driver interactions, which can be critical in cases involving distracted driving or criminal intent.

**1.4. Cybersecurity Considerations**

- Electric vehicles often feature advanced connectivity such as over-the-air updates, integrated applications, and cloud data synchronization, which not only increases the potential sources of forensic evidence but also broadens opportunities for attacks and tampering.
- Electric vehicles present new security challenges because their battery management systems (BMS) and charging interfaces are susceptible to specialized cyberattacks, such as “leaky battery” side-channel attacks, forcing forensic investigators to identify and address these emerging attack methods.
- Analysis of cybersecurity logs and network traffic to identify breaches.

## II. CHALLENGES IN AUTOMOTIVE DIGITAL FORENSICS

The rapid adoption of modern automotive technologies has outpaced the development of corresponding digital forensic capabilities. There is a pressing need for a standardized framework that can guide forensic investigations in the current regulatory environment. The following challenges are observed in vehicle digital forensics examinations as given below:

- **Lack of Standardized Procedures:** One of the significant gap is the absence of any standardized set of procedures for conducting vehicle digital forensics. Without any standardization and well accepted framework investigations may be inconsistent across forensic labs making them further challenging their acceptability in legal proceedings.
- **Diverse Vehicle Ecosystem**: India's automotive market includes a wide array of vehicles from various manufacturers, each with distinct digital architectures and proprietary systems.
- **Various Stakeholders**: Identification and level of interest of various stakeholders over the evidence’s confidentiality, integrity and privacy are yet to be mapped.
- **Legal and Regulatory Framework:** The absence of regulations for digital evidence in vehicles complicates forensic investigations and the admissibility of evidence in Indian courts.
- **Data Integrity and Authenticity**: To uphold the integrity of vehicle data, it must be protected from alteration during the processes of collection and analysis. Improper handling or storage of data can lead to inaccuracies and could potentially compromise the investigation.
- **Resource Constraints**: Limited access to advanced forensic tools and trained personnel, poses significant challenges, particularly in rural and underdeveloped regions.

## III. OBJECTIVES

The primary objectives of this research are:

- To propose a digital forensic framework for vehicles.

## IV. LITERATURE REVIEW

The digital forensics legal regulations are still evolving in India. The Information Technology Act, 2000, and its amendments helps at some extent, specific regulations addressing automotive digital forensics is still needed. These regulations are essential for digital evidence to be accepted in court. [1]

The Government of India's view and efforts in the direction of vehicle digital forensics is progressive now. It has finalized a draft for Automotive Industry Standard (AIS) titled as "Uniform provisions concerning the approval of vehicles with regards to Event Data Recorder (EDR)" highlighting the significance of digital evidence extracted from a vehicle's EDR devices.

"13-AIS_192_DF_August_2024" is intended to ensure that Event Data Recorders (EDRs) in vehicles will gather information in a way that will make it immediately accessible for crash investigations and will evaluate the performance of a vehicle's safety systems. This data will help all stake holders to understand the conditions causing vehicle crashes and injuries, which will in turn support the vehicle designs to be more reliable and safer. [2]

Computer Forensic Investigative Process by Pollitt, M et al, is made up of four phases which are acquisition, identification, evaluation and admission. It was more focused on extraction rather than on other phases of digital forensics. [3]

In [4], G. Palmer at al. presented a Digital Forensic Research Workshop (DFRWS) Model which is made up of six phases which are Identification, Collection, Examination, Record, Analysis, and Presentation phase.

In [5], Reith et al. has proposed "Abstract Digital Forensic Model (ADFM): Derived from the above mentioned DFRWS model, it adds three additional phases in the six phases making it nine and they are Preparation, Approach Strategy, and Returning Evidence.

In [6], Ankit et al. has proposed Integrated Digital Investigation Process (IDIP). This model is made up of the following phases namely Readiness, Deployment, Physical Crime Scene, and Digital Crime Scene Investigation.

In [7], X. Feng et al. has proposed a "Generic Digital Forensic Investigation Framework for IoT" that was tailored to IoT environments, it incorporates four processes—Proactive, IoT Forensics, Reactive, and Concurrent processes.

All of the above mentioned models, more or less similarities can be observed in the processes of evidence acquisition or collection, preservation, identification, examination or evaluation and presentation phase. The newly developed IDIP model, shows greater relevance to Smart City AAVs (Autonomous and Automated Vehicles). This is due to its ability to address potential attacks originating from physical, cyber, or combined sources, as it incorporates provisions for all such scenarios.

In [8], A. Philip et al. proposed a framework which facilitates from deep learning and blockchain technology and specially made for crashes and traffic incidents. An accident warning system is theorized for vehicles by processing various data inputs such as road conditions, lights, climate variables, software/ hardware variables along with driving patterns and many other traffic things. With the help of machine learning and artificial intelligence it is possible to forecast the standard or optimal parameter values for safe driving requirement. Steering focus towards [25], another innovative approach is introduced facilitating by a permission-based blockchain in vehicle digital forensic framework specially curated for diverse data set collection, loging health data from smart wearables along with automotive diagnostics data. This approach integrates the Vehicular Public Key Infrastructure (VPKI) into the blockchain additionally offering membership and privacy benefits.

In [9] by M. Hossain et al., presented a distinctive approach. He proposed an IoV data collection forensic framework for a distributed and decentralized network along with other mobile entities, benefitted by available secure storage mechanisms. Their offering encompasses the orchestration of digital evidence collection, coupled with an algorithm which ensures its data integrity verification for the validation of digital evidence.

In [10], K. Buquerin et al. have proposed an IoV forensic framework. This is made up of four digital forensic phases and that are forensic readiness, data acquisition or retrieval, data analysis, and reporting or documentation. A practical illustration utilizes the On-Board Diagnostics II (OBD-II) port as a data collection interface, with the help of a network monitoring and packet capture software WireShark Packet Capture (PCAP) file is captured and its corresponding hash value is documented. This compound data forms the basis for subsequent analysis and report generation.

In [11], C. Alexakos tried o address the challenges of integrating digital forensics within the context of the Internet of Vehicles (IoV).

In [12-13], Valjarevic et al worked by acknowledging the absence of standardized data formats and a dynamically shifting network topology. This is why authors have introduced a tool the digital forensic process model making it forensic ready. It seamlessly integrated into the nIoVe framework. This tool substantiates forensically valid data collection, facilitating event reconstruction for legal proceedings while also fostering the ability to predict and counteract potential anomalies, including cyber-attacks.

In [14-15], R. Altschaffel et al. and S. Kiltz advocate the adoption of a Desktop IT forensic process model which is outlined and aligned with Event Data Recorders (EDRs), to enshroud the automotive domain. This multifaceted process unfolds through strategic and operational preparatory measures, leading to data gathering, investigation, analysis, and comprehensive documentation. Notable tools, usage scenarios, and data acquisition avenues from various automotive components are detailed.

Concluding the synthesis, [16] by T. Hoppe et al. furnishes an overarching perspective of the vehicle digital forensics framework. This narrative emphasizes the judicious use of a secure data recorder tasked with logging pertinent navigation data transmitted over the vehicle's Controller Area Network (CAN) bus. The amalgamation of route details, speed metrics, and positional information facilitates the reconstruction of vehicle routes for post-incident analysis, while also attributing indices that can potentially corroborate or absolve individuals in relation to incidents.

In [17], Breda & Janos, (2018) have proposed a 4-layered forensic model (Application, Presentation, Media management and Physical layers). In this framework the sheer volume of data and the quality of the evidence data are not considered properly. Hence, evidence integrity is overlooked which causes a requirement of IoT forensic friendly framework to be designed, that solves another big forensic challenge of identification and classification of evidence data which is more relevant to the subjected case.

In [18], Bouchaud, Grimaud & Vantroys, (2018) have given a 4 layered (sensor, network, cloud and API/GUI) forensic model. This framework is primarily focused upon the Identification and the classification of myriad IoT devices and data. Also, a layered weighted analysis of evidence sources is done based on production cost, human cost, engineering cost and alteration cost of the evidence data. Forensic readiness process is missing in this framework.

In [19], Kebande et al., (2018) have proposed an integrated digital forensic investigation framework for Internet of Things system. This framework if formed as an extension of the digital forensic investigation framework (DFIF-IoT) model, which has 4 layers but IDFIF-IOT model has nine phases. But this forensic model is missing the capability of pre-incident detection, nor identifies critical forensic aspects by a prototype implementation. This framework does not offer comparative analysis with other models. Standards of procedure are also missing.

In [20], Kebande & Ray, (2016) have again proposed a Digital Forensic Investigation Framework for Internet of Things. This framework has three separate and one concurrent modules as given below

a. Proactive process module: planning and preparation
b. IoT forensics process module: cloud, network and device level forensics
c. Reactive process module: initialization, acquisition and investigation
d. Concurrent module: finding authorization, documentation

This model supports forensic readiness. This model framework had tried to accumulate all other frameworks but it is yet to verify and validate by others in a practical environment.

In [21], Zawoad & Hasan, (2015) have proposed a FAIoT (forensic aware internet of things) framework is proposed in this paper. It is theorized that a centralized and reliable evidence repository could be used for collection and analysis. In this paper, a secure logging scheme is specially designed for various IoT devices. HDFS (Hadoop distributed file system) is used here, two very important modules - secure evidence preservation and secure provenance (logs of "chain of custody") are proposed. Access to evidence is provided through APIs in read-only format to the investigators and law enforcement agencies. Major issues are with integrity and cloud storage as parties can collide to alter the evidence.

In [22], Banerjee, Lee, Chen, & Choo, (2018) have approached to isolate untrusted devices from IoT system by setting up an abstraction layer and each activity is then will be recorded into a blockchain for any further forensic requirement. This device can rejoin the IoT system post validation. This forensic model is not tested in a constrained environment. Overheads, time and cost and performance are needed to be evaluated.

In [23], Al-Sadi, Chen, & Haddad, (2018) has proposed an IoT forensic framework that classifies the IoT architecture in 3 layers as top, middle and bottom and then to use open source software in their forensic analysis. No forensic readiness process is there. There are multiple vendors involved and data is generated in big volume, so identification and data filtering of most relevant evidence from the most relevant resource is necessary for redundancy.

In [24], Goudbeek, Choo, & Le-Khac, (2018) have proposed a 7 Phases Framework for forensics of HAS (home autonomous system), Phase 1: Preparation off-site, Phase 2: Search for a home automation system on-site, Phase 3: Preserve the HAS "as is", wherever possible, Phase 4: Understanding the specific home automation system, Phase 5: Check security level, Phase 6: Locate and acquire evidential data, Phase 7: Process/analyze seized data. However, this forensic framework is failed to offer the digital forensic readiness process. No Forensic friendly data format is available hence it is based on investigator's skill only and rigorous training will be a must. In this framework, there is nothing for evidence on the cloud platform. Hence it cannot be applied to automotive digital forensics.

In [25], Malek, (2017) has given a theoretical framework based on LoS, NBT and 3-Zones of IoT system, and a case management platform is given too. This framework has no forensic readiness process and it is yet to test and implement in a real-time environment. This framework has not covered legal considerations.

In [26], Jesse Lacroix (2017) in his thesis, has discussed the extractable type of data, the infotainment system and available data in them, types of software and hardware resources available and their soundness, and problem-related with OEMs. The key aspects are maintaining integrity and chain of custody. In this research work, the author has not discussed the idea of "Forensic by Design" or "Forensic Friendly" in the device development life cycle for OEMs. Maintaining integrity has also become a challenge for the researchers. Many challenges can be tackle with the most cost effective manner if the whole infra could be made forensic friendly. Updates will be available on time; Software will support data extraction from more electronic devices, sensors, reporting will be more easy and efficient.

In [27], Lacroix et al. (2016) in his research paper, have explored the potential of vehicular digital evidence, examining what information is stored and what it can reveal about an end user and their actions. Forensic challenges in Mobile and Ad Hoc Networks are also discussed. It was found that the infotainment system will play a greater role in providing digital evidence of automobiles.
From the frameworks proposed above, several key observations can be made:

- Each model builds on the insights and experiences of its predecessors.
- Certain models share similar methodologies or approaches.
- Some focus on different elements of the investigative process.

To strike an effective balance, it is crucial to maintain a clear focus on the primary objective: generating solid, admissible evidence that can be presented in a court of law.

## V. PROPOSED AUTOMOTIVE DIGITAL FORENSICS FRAMEWORK

The previous section has highlighted many key forensic frameworks. Building on this foundation, we are proposing a new vehicle digital forensic framework. A well-designed automobile digital forensics framework is essential in maintaining consistency, efficiency, and accuracy in digital forensic investigation of automotive systems.

### 5.1. Framework Overview

The proposed framework is designed to provide a structured approach to automotive digital forensics in India. It is built upon further extending the foundational seven phases of digital forensics, which are Preparation, Identification, Preservation, Extraction, Analysis, Documentation and Presentation phases as given in figure1. These different phases can be understand as given below:

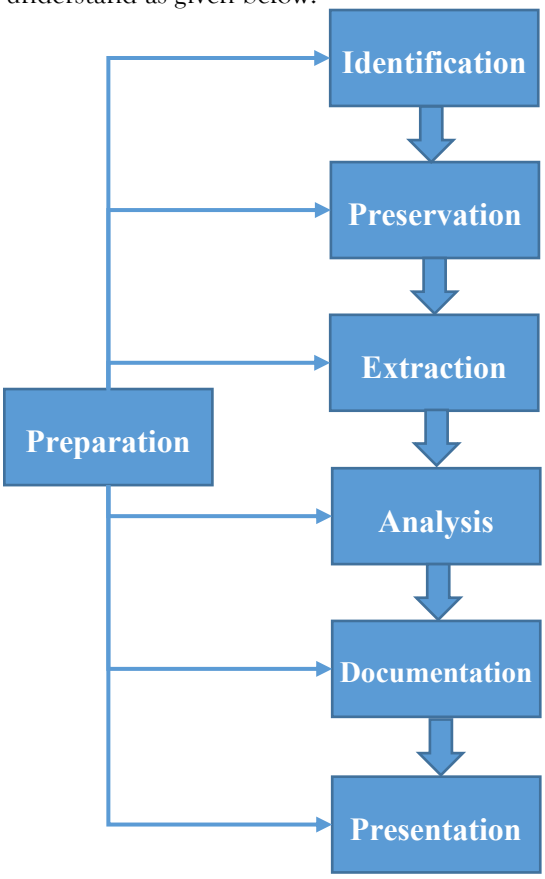


**Figure1.** 7 Phases of Vehicle Digital Forensics Framework

**5.1.1. Preparation**: This phase is responsible for ensuring the overall quality of the forensic examiners, examination and for minimizing the potential associated procedural and technical challenges as given in figure.2. It should include the following:

**a.** Standards used in the organization (forensic SOPs etc.,).
**b.** Pre-existing policies to help in the investigation process (laws recommending EDR and maintaining copyright free evidence etc.,).
**c.** Training of examiners/investigators (for identification of source of evidence, search and seizures, maintaining chain of custody etc.,).
**d.** Legal advice as and when required which depends on case to case.
**e.** Notification to the all correct authorities.
**f.** Technical and procedural documentation of all previous such incidents for any cross reference.
**g.** Planning for how to approach a particular vehicle as they differ from brand to brand and model to models moreover.
**h.** If possible a faraday cage case for preventing any change in GPS and relevant information.
**i.** Maintaining chain of custody in all key phases as in preservation, acquisition, analysis and documentation phases of forensic investigations.


**Figure2.** Preparation phase

A reference document is required for available automotive brands\ models to help investigators in identifying the desired devices, sensors, who either creates or stores digital data of forensic relevance, extraction and preservation methods and connectivity ports etc., It could be made by either mandating for manufacturers as a legal requirement to run business or research works funded by Government/ Private agencies. Since, modern vehicles generate and rely on diverse data sources some of them are as below:

- Sensors: LiDAR, Inertial Measurement Unit (IMU), ECU, occupant, radar, TPMS, cameras, ultrasonic sensors, break and airbag deployment sensors, etc.,
- Onboard Systems: Vehicle control units, event data recorders (EDRs), and infotainment systems.
- Connectivity Modules: GPS sensors, cloud (data stored or in transit) and telematics systems.

- Cloud Services: Data stored in manufacturer or third-party cloud platforms

**Identification:** It is to recognize and characterize potential source devices for evidence, inside or outside the vehicle which means data on Internet cloud or by other vehicles passing by as given in Figure 3.

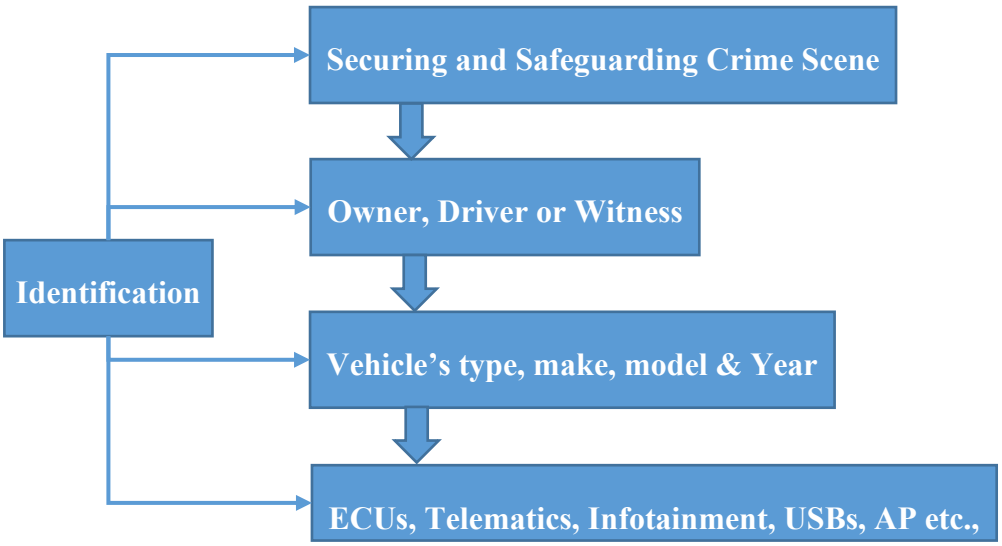


**Figure 3.** Identification Phase

Steps which should be followed are as given below:

- Securing and safeguarding the crime scene is first and very important step.
- Identification of evidence sources: Identifying the relevant data sources within the vehicle which includes:
- Identification of persons or organizations for owner/ driver details of the vehicle or witnesses.
- Identification of the specific EV make, model, and year to anticipate relevant sub-systems.
- Identification of type of electronic and digital devices such as ECUs, infotainment systems, telematic units, various sensors and external devices such as smartphones connected to the vehicle or cloud networks which may holds potential digital evidence and their state of findings.
- Identification of the type of digital data that these devices may hold and which may vary from device to device.

By documenting these sources, it can be ensured that nothing is overlooked before the investigation starts. [28-29]

**5.1.2. Preservation:** The purpose of this phase is to protect the data integrity to prevent tampering or any accidental alteration as given in figure 4. The key considerations under this phase are as given below:

**a. Seizure of devices:** It is the process of seizing of devices from a vehicle which are either used in a crime or faced an accident, as identified in the previous phases. In automotive environment, sometimes it might not possible to independently seize and seal the evidence devices as they might be the integral part of the vehicle itself and might contain volatile data. It will require expert's assistance in handling them. Data might also be stored in cloud servers in certain cases e.g. fleet management software, telematics etc.,
Every device seized should have been sealed in proper way and labeled with all relevant information like date and time of seizure in presence of two witnesses along with first responder's name, signature and seal mark etc.,

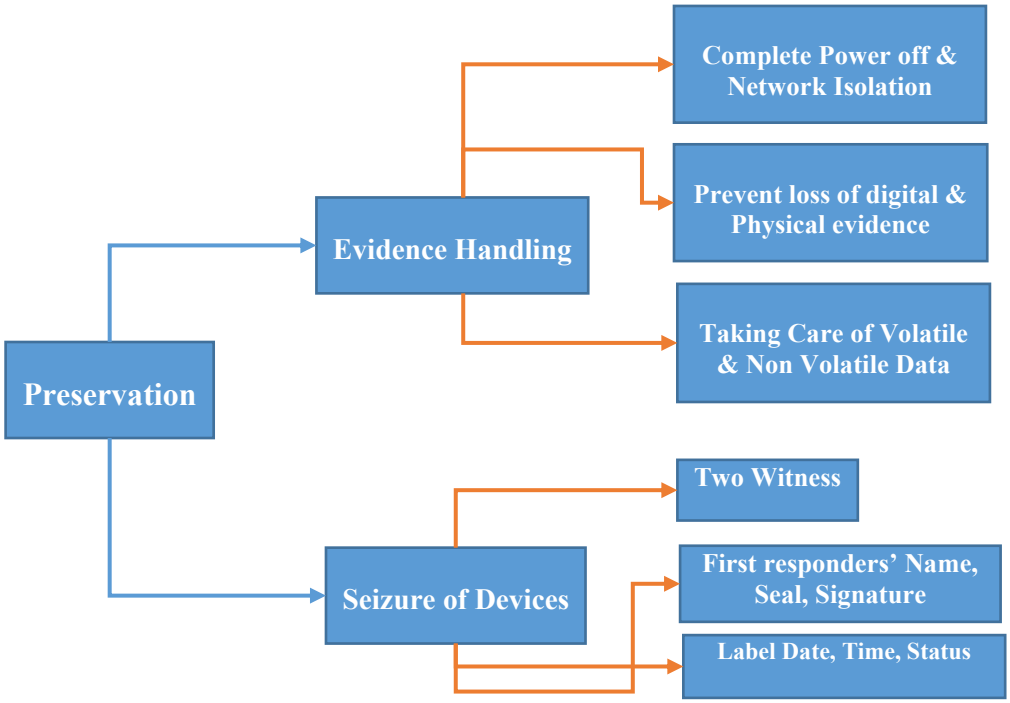


**Figure 4.** Preservation Phase

**b. Evidence Handling:** As per forensic guidelines from Interpol, before collecting evidence, reviewing legal authority and obtaining additional authorization is needed. Infotainment and telematics systems may exist as separate or integrated ECUs, requiring careful handling to prevent any data loss, especially since ECUs continuously draw power from the vehicle battery. Power cycles triggered during physical evidence processing (e.g., fingerprint or DNA collection) can lead to data loss. Telematics and infotainment systems pose challenges also due to variations in hardware design, proprietary software, encryption (e.g., DRM), and rapid technological changes. Data extraction may require specialized tools, and visual examination might be necessary if traditional methods fail.

To mitigate this, up to some extent, investigators should document or photograph on-screen data, shut down the vehicle completely and isolate it from wireless networks (Wi-Fi, Bluetooth, cellular) to preserve any volatile data available.

- In order to preserve digital evidence, the following steps should be followed when shutting down a vehicle:

– Maintain a document with the date and time of the procedure.
– Vehicle should be turned off and remove all keys.
– Open the driver's door for 5 seconds after closing all doors properly.
– Now the driver's side door should be closed for approximately two minutes to pass.
– Vehicle should be disconnected from power (e.g., battery disconnection or transport mode activation).
– Ensure a complete shutdown, by letting the center stack, instrument cluster, and remaining lights set off for at least 30-45 seconds after closing the doors. If possible, forensic examiners should wait for at least 60 more seconds to finalize this process smoothly.
– For Electric Vehicles (EVs), volatile data should also be considered by prioritizing the acquisition of volatile and semi-volatile data (e.g., RAM, recent BMS/fault logs) due to risk of loss during power-down events.

- The key guidelines for the first responder/ forensic investigator are as given below:

– Follow the existing agency policy and maintain the chain of custody.
– ECU state should be preserved before physical evidence processing.
– Coordinate with investigators and forensic lab personnel to prevent the destruction of digital and physical evidence (e.g., DNA, fingerprints).
– Take precautions against biological contaminants and physical damage.

– Prevent external connections (cellular, Wi-Fi, Bluetooth) by isolating the vehicle (e.g., disconnecting antennas, removing SIM cards).
Proper adherence to these protocols ensures the integrity of evidence in vehicle forensic investigations. [30-32]

**5.1.2. Extraction**: The process of retrieving electronically stored information from the seized devices without altering original content. [28,32]

**a. Data Extraction Techniques:** Various techniques can be employed for data extraction, including direct access to ECUs via OBD-II ports, chip-off, extraction from infotainment systems, connected devices, and directly from EDR module. These choices of technique depend heavily on the specific vehicle type and the nature of the investigation.

**b. Data Types or Artefacts:** As per the guidelines given by Interpol, some of the artefacts that can be obtained are given below for reference: [30]
- **Vehicle system information:** Chassis number, Engine number, Vehicle Identification Number (VIN), TPMS.
- **Installed application data:** Weather, Traffic, Facebook, Twitter, and YouTube.
- **Connected devices:** Cell phones, portable media devices and USB storage, memory cards, Wi-Fi Aps, Bluetooth/Wi-Fi/USB connections.
- **Navigation data:** Travel logs, last saved locations, previous destinations, active and inactive routes, GPS coordinates & Time syncs.
- **Device details:** Device IDs, call logs, contact lists, text messages, Audio, Video, Image files etc.,
- **Events data:** Speed, acceleration, brake uses, airbag deployment, ignition on/off, doors opening and closing
- **Diagnostic data:** Fault codes, coolant temperature, engine rpm, fuel used, intake air pressure, intake manifold absolute pressure etc.,

**c. Data Types or Artefacts (in case of EVs):**
- **Battery Management System (BMS):** Acquire logs recording charge/discharge cycles, cell voltages, temperature anomalies, and fault events. [33]
- **Infotainment & Telematics:** Extract user profiles, navigation history, Bluetooth pairings, and cloud/app transactions.
- **Charging Infrastructure:** When accessible, collect charging station logs for session times, locations, and ID correlations.
- **Cloud/Remote Sources:** Submit lawful requests to manufacturers or service providers if data is thought to be synched beyond the vehicle.

**d.** Tools: Use specialized tools like forensic software to retrieve data from EDRs, telematics, infotainment systems and from cloud storages. Some of the enterprise based solutions are Berla iVe and Bosch Crash Data Retrieval (CDR). JioMotive is another device launched by Jio in India which performs data logging and can make a car smart. While it is not a forensic tool itself, it can provide a wide range of telematics data. Apart from that tools like Forensics Toolkit (FTK), Encase, and Autopsy are also good choices for data analysis.

**e. Data Protection:** Ensure integrity and privacy of the extracted data by storing them as per industry standards. Write-blockers and enterprise software solutions are the most helping resource here.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 18s, 2025
https://www.theaspd.com/ijes.php

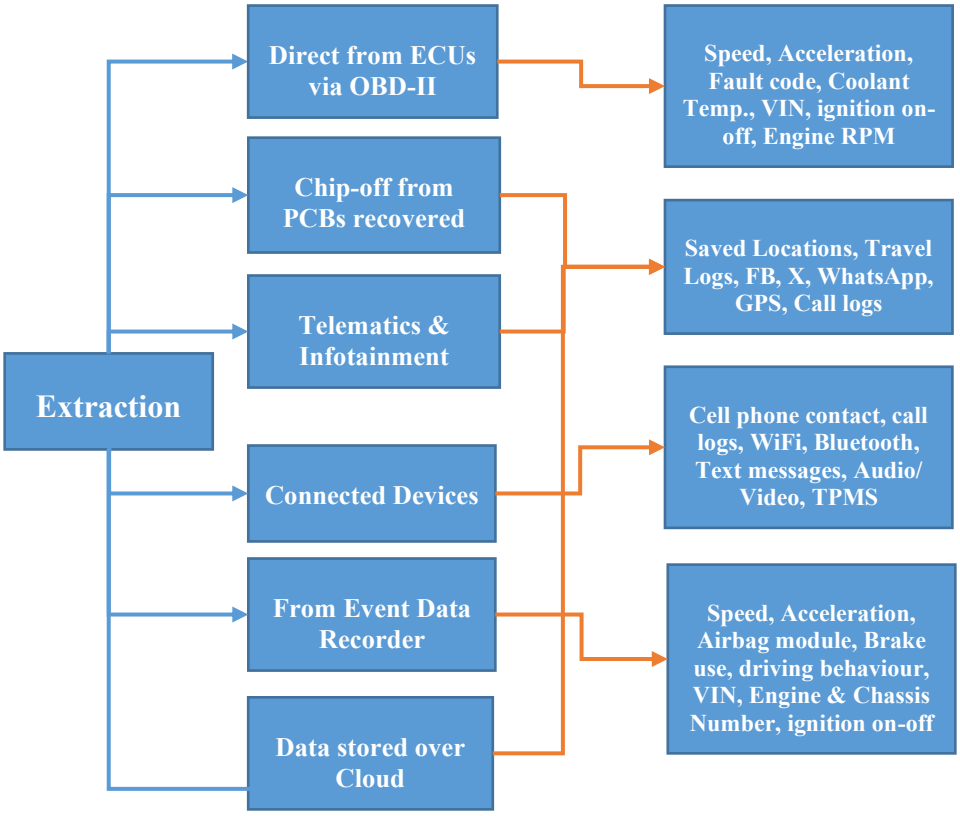


**Figure 5.** Extraction Phase

**5.1.3. Analysis**: The process of examining the extracted data to identify relevant evidence and to recreate events as given in figure 6. [28-29] It involves below mentioned steps:

**a. Data Parsing and Interpretation:** To obtain meaningful information, the acquired EDR data requires thorough parsing and interpretation. It helps to determine vehicle speed, brake usage, and seatbelt status before the crash. Forensic examiners analyse telematics logs to look for remote commands or signs of hacking. Infotainment data might reveal locations visited prior to the incident or recent calls made, helping to clarify the situation or verify alibis. This may involve decoding proprietary data formats, analyzing log files, and correlating data from multiple sources.

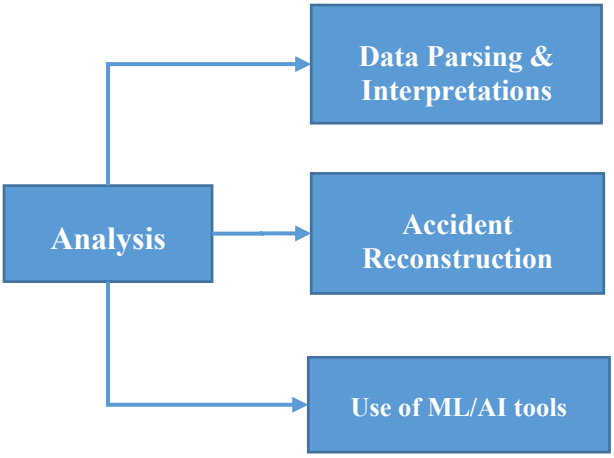


**Figure 6. Analysis Phase**

**b. Forensic Tools**: Analyze the collected data using forensic analysis tools that support the interpretation of EDR data, GPS routes, and infotainment logs. Tool selection varies based on the unique demands of each investigation.
**c. Accident Reconstruction:** Utilize accident reconstruction software to simulate vehicle behavior based on the collected data, corroborating physical evidence from the crash site.
**d. Use of Machine Learning Tools/Methods:** Use of machine learning models to analyze sensor data and infer vehicle behavior.
**e. For EVs:** analysis should consider the followings:
- **Timeline Construction:** Correlate BMS, charging, and user activity logs to reconstruct events (e.g., travel routes, charging behavior, anomalies).
- **Security Event Detection:** Identify anomalies or patterns suggestive of tampering, unauthorized access, or cyberattacks specific to EV systems.
- **Cross-System Correlation:** Leverage information from multiple subsystems to validate findings and ensure consistency.

**f. For Autonomous Vehicle (AV)**: Forensic examiners should try additionally to look for evidence for:
- Identification of potential cyberattacks or unauthorized access to AV systems.
- Analysis of network traffic logs and system event logs to detect anomalies.

**5.1.4. Documentation**: This is another critical phase of vehicle digital forensics. In this stage a comprehensive, clear and concise report should be prepared documenting the entire forensic process, including the methods used, the data acquired, and the findings as per figure 7. It should also clearly differentiate between native data, user activity, and system-generated events. [29,31]

**5.1.5. Presentation:** It is presenting the forensic findings in a simple and concise manner, often in the form of a forensic report. This report should be well-structured, easy to understand, and support the conclusions drawn from the analysis for the law enforcement, legal professionals, and the judiciary involved, as given in figure 7.. e.g., an analysts compile a report that outlines as below: [29,31]
- What data was found, and from which systems?
- Chain of custody details.
- Major findings, for example, detection of speeding or breaches of system security.
- This report can be accompanied by documentation, graphics (e.g., crash reconstruction charts), and a disclosure of forensic methods to support credibility and transparency in court

Expert testimony: it is a process of verification and validation of the evidence by domain experts. For critical cases, senior forensic experts should be required to testify the findings, by explaining the methodologies and tools used in the forensic examination.

## VI. DISCUSSION

### Effectiveness & Limitations

The proposed framework provides a structured approach to automotive digital forensics, addressing the unique challenges posed by the automotive ecosystem. The framework's effectiveness can be enhanced by improving the preparation phase to strengthen its applicability in real-world scenarios. The framework's effectiveness is also highly depending on the availability of trained professionals with appropriate forensic tools. In addition to this the lack of standardized procedures and regulations may continue to pose challenges in conducting forensic investigation which may further be required to use feedback from examiners for continuous improvement.


**Figure 7.** Documentation and Presentation phase

## VII. CONCLUSION

As technologies used in modern vehicles are continuously evolving, the importance of a robust vehicle digital forensic framework establishes even more. The proposed framework addresses the lack of standardization and procedural challenges in performing vehicle digital forensic investigations, which aims to enhance the effectiveness, accuracy and reliability of the vehicle forensic evidence in court of law. Government and Law enforcement agencies should invest more in forensic training and development of indigenous forensic tools. Law enforcement agencies, researchers, and policymakers must collaborate to standardize automobile forensic procedures and ensure the ethical use of vehicle data in investigations. Researchers must address challenges like data privacy, system compatibility, and the development of new tools for data retrieval and analysis. By implementing standardized protocols, building collaboration, and investing in capacity building a resilient system can be made which will be capable of addressing current and future challenges in automotive digital forensics.

## REFERENCES:

1. Information Technology Act, 2000, Government of India.
2. https://morth.nic.in/sites/default/files/ASI/13-AIS_192_DF_August_2024.pdf
3. Pollitt, M. (1995). "Computer Forensics: An approach to evidence in cyberspace". Baltimore: MD. Pp. 487-491.
4. DFRWS (2001) "Workshop 1 – A Framework for Digital Forensic Science". In: G. Palmer, ed. A Road Map for Digital Forensic Research. New York: DFRWS, pp. 15-16.
5. Reith, C. and Gunsh,C. . (2002) "An Examination of Digital Forenisc Models". International Journal of digital Evidence, vol. 1 (no. 3), pp. 1 - 6.
6. Ankit, A., Gupta, M., Gupta, S. and Prof. Gupta. (2011). "Systematic Digital Forensic Investigation Model". International Journal of Computer Science and Security (IJCSS). 5 (1), pp. 1-14.
7. X. Feng, E. S. Dawam, and D. Li, "Autonomous vehicles' forensics in smart cities," in Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov., 2019, pp. 1688–1694.
8. Philip and R. Saravanaguru, "Secure incident & evidence management framework (SIEMF) for Internet of Vehicles using deep learning and blockchain," Open Comput. Sci., vol. 10, Nov. 2020, Art. no. 408.
9. M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the Internet of Vehicles (IoV)," in Proc. IEEE Int. Congr. Internet Things, 2017, pp. 25–32.
10. K. K. Gomez Buquerin, C. Corbett, and H.-J. Hof, "A generalized approach to automotive forensics," Forensic Sci. Int.: Digit. Investigation, vol. 36, 2021, Art. no. 301111. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281721000056
11. C. Alexakos, C. Katsini, K. Votis, A. Lalas, D. Tzovaras, and D. Serpanos, "Enabling digital forensics readiness for Internet of Vehicles," Trans. Res. Procedia, vol. 52, pp. 339–346, 2021.

12. Valjarevic and H. Venter, "A harmonized process model for digital forensic investigation readiness," in Proc. Adv. Digit. Forensics IX, G. Peterson and S. Shenoi, Eds., 2013, pp. 67–82.
13. CORDIS, "A novel adaptive cybersecurity framework for the Internet-of- Vehicles," Accessed: Apr. 21, 2021. [Online]. Available: https://cordis. europa.eu/project/id/833742
14. R. Altschaffel, K. Lamshöft, S. Kiltz, and J. Dittmann, "A survey on open automotive forensics," in Proc. 11th Int. Conf. Emerg. Secur. Inf., 2017.
15. S. Kiltz, J. Dittmann, and C. Vielhauer, "Supporting forensic design - A course profile to teach forensics," in Proc. 9th Int. Conf. IT Secur. Incident Manage. IT Forensics, 2015, pp. 85–95.
16. T. Hoppe, S. Kuhlmann, S. Kiltz, and J. Dittmann, "IT-forensic automotive investigations on the example of route reconstruction on automotive system and communication data," in Proc. Int. Conf. Comput. Saf., Rel., Secur., 2012, vol. 7612, pp. 125–136
17. G. Bréda and P. János, "Forensic Functional Profile of IoT Devices – Based on Common Criteria," pp. 261–264, 2018.
18. F. Bouchaud, G. Grimaud, and T. Vantroys, "IoT Forensic," Proc. 13th Int. Conf. Availability, Reliab. Secur. - ARES 2018, pp. 1–9, 2018.
19. V. R. Kebande et al., "Towards an integrated digital forensic investigation framework for an IoT-based ecosystem," Proc. - 2018 IEEE Int. Conf. Smart Internet Things, SmartIoT 2018, pp. 93–98, 2018.
20. V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," Proc. - 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, FiCloud 2016, pp. 356–362, 2016.
21. S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," Proc. - 2015 IEEE Int. Conf. Serv. Comput. SCC 2015, pp. 279–284, 2015.
22. M. Banerjee, J. Lee, Q. Chen, and K. R. Choo, "Blockchain-based Security Layer for Identification and Isolation of Malicious Things in IoT : A Conceptual Design," 2018.
23. M. B. Al-Sadi, L. Chen, and R. J. Haddad, "Internet of Things Digital Forensic Investigation Using Open Source Gears," Conf. Proc. - IEEE SOUTHEASTCON, vol. 2018–April, 2018
24. A. Goudbeek, K. K. R. Choo, and N. A. Le-Khac, "A Forensic Investigation Framework for Smart Home Environment," Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018, pp. 1446–1451, 2018.
25. A. T. Framework, "An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I :," 2017.
26. Lacroix, J. (2017). Vehicular Infotainment Forensics: Collecting Data and Putting It into Perspective, (June 2016)
27. Lacroix, J., El-Khatib, K., & Akalu, R. (2016). Vehicular digital forensics: What does my vehicle know about me? DIVANet 2016 - Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Co-Located with MSWiM 2016, 59–66. https://doi.org/10.1145/2989275.2989282
28. K. Strandberg, N. Nowdehi and T. Olovsson, "A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection," in IEEE Transactions on Intelligent Vehicles, vol. 8, no. 2, pp. 1350-1367, Feb. 2023.
29. Z. Chen et al., "Digital Forensics for Automotive Intelligent Networked Terminal Devices," in IEEE Transactions on Vehicular Technology, vol. 73, no. 4, pp. 5128-5138, April 2024.
30. https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf
31. K. Strandberg, U. Arnljung and T. Olovsson, "The Automotive BlackBox: Towards a Standardization of Automotive Digital Forensics," 2023 IEEE International Workshop on Information Forensics and Security (WIFS), Nürnberg, Germany, 2023, pp. 1-6.
32. R. Kurachi, T. Katayama, T. Sasaki, M. Saito and Y. Ajioka, "Evaluation of Automotive Event Data Recorder towards Digital Forensics," 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 2022, pp. 1-7.
33. Khaneghah, M.Z, Alzayed, M., Chaoui, H., "Fault Detection and Diagnosis of the Electric Motor Drive and Battery System of Electric Vehicles. Machines, 2023, 11, 713, https://doi.org/10.3390/machines11070713