MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

Guidelines on Data Preservation for Passenger Cars

December, 2024

DISCLAIMER

The purpose of this document is to provide generic guidance and suggested processes for data preservation from passenger cars to support case investigations. It was developed based on input from the relevant agencies, a compilation of the best available information, knowledge and field experience to provide guidance to law enforcement officers so that activities are performed in a consistent and standardized manner.

This document should be used as a reference. However, differences may exist between the procedures referenced in this document and what is appropriate under field-specific conditions related to car data seizure. For the avoidance of doubt, the use of this document shall not in any way create or be relied upon to give rise to, any rights or obligations that may be enforceable in any legal matter whether civil or criminal, specifically concerning the seizure and preservation of data from passenger cars.

Any products, manufacturers or organisations referenced in this document are presented for informational purposes only and do not in any way constitute approval or endorsement by CyberSecurity Malaysia.

COPYRIGHT AND CONFIDENTIALITY STATEMENT

DOCUMENT OVERVIEW

The digital age is increasingly impacting all areas of society, including the automotive industry, which is undergoing significant transformation. Modern passenger cars are now incorporating electronics and electric powertrains, replacing traditional internal combustion engines. This evolution has generated valuable data on performance, personal usage, and additional information such as video, Global Positioning System (GPS) tracking, and infotainment. This Guideline has been developed to specifically address the preservation of data found in passenger cars. Today, the digital data available in passenger cars can provide critical information that may be valuable in a court of law. This document outlines a standardized and effective approach for investigators and digital forensic analysts to ensure the successful preservation of critical evidence from passenger cars, ultimately contributing to successful prosecutions and supporting the advancement of research in this field.

DOCUMENT PURPOSE

The purpose of this document is to provide guidance to the Malaysian Law Enforcement Agency (LEA) in seizing and preserving data from passenger cars. This document is applicable to LEA operating under different operational frameworks. The statements in this document are made in general so that they can be adopted by various LEA. As each agency may have its own process, the agency may need to elaborate further on each statement to suit specific operational needs.

DOCUMENT SCOPE

The scope of this document is on data preservation on passenger cars, and does not incorporate data preservation on other types of vehicle such as heavy vehicles (lorry, trucks, buses), or motorcycles. The data that is covered in this guideline includes Event Data Recorder (EDR) data such as vehicle speed, brakes status, occupant seat belts as well as data from infotainment device which may include personal data of car owner such as contact list, call logs, messages, social media feeds and navigation history of everywhere the vehicle has been. Therefore, it is crucial to include a section on Personal Data Protection Act (PDPA) in this guideline.

ACKNOWLEDGEMENT

This document was developed by Digital Forensics Department, CyberSecurity Malaysia in collaboration with Malaysian Institute of Road Safety Research (MIROS) as well as Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA) to address challenges in conducting forensic investigation on passenger cars.

TABLE OF CONTENT

LIST OF TERMINOLOGIES

EDR	Event Data Recorder is a specialized device embedded within modern vehicles that captures critical data related to the vehicle's performance and occupant safety just before, during, and after a collision.
Infotainment	Infotainment system in passenger cars refers to the in-vehicle entertainment and information features. Infotainment system stores data which can include GPS location, navigation history, call logs, contacts, text messages, media files, and information from connected mobile devices.
GPS	Global Positioning System is a tracking system to track location.
Telematics	Telematics systems are primarily focused on vehicle data and communication.
OSINT	Open-Source Intelligence Tool to conduct intel gathering for the case and car.
OBD Port	On-Board Diagnostics and is a computer system inside of a vehicle that tracks and regulates a car's performance. This on-board computer system collects information from the network of sensors inside the vehicle, which the system can then use to regulate car systems or alert the user to problems.
OBD-II	On-Board Diagnostics II is the second generation of the OBD system.
ACM	Airbag Control Module is a specific type of ECU focused on airbag deployment and recording crash data. In the event of a crash, the ACM records information such as speed, brake application, seatbelt status, and the timing of airbag deployment, which can be critical for accident reconstruction.
EV	Electric Vehicle is a vehicle powered entirely or partially by electricity.
Hash Values	Hash value is a unique code generated from digital data (e.g., a file) using a mathematical function.
DVD	Digital Versatile Disc is a type of optical disc that can store larger amounts of data
CD-R	Compact Disc-Recordable is a type of CD that allows one-time recording of data. Once data is "burned" onto a CD-R, it cannot be changed or erased, which is useful for forensic evidence preservation.
Ignition state	The ignition state indicates whether the vehicle's ignition is on, off, or in an intermediate position. This status helps determine if the engine was running, if electrical systems were active, or if any accessories were powered on at a given time.

Black Boxes	In vehicles, a "black box" refers to the Event Data Recorder (EDR) or similar device that records critical information during a crash or other significant events.
Aftermarket technologies	Aftermarket technologies in passenger cars are devices added by owners or third parties, which can range from GPS trackers and telematics systems to dash cams and driver-assistance tools.
Key Fobs	Key fobs in modern passenger cars are more than just keys; they are small, data-storing devices with embedded electronics that communicate with the car's systems.
ECU	Electronic Control Units in a vehicle is a computerized component that controls and manages various systems in a vehicle. It receives real-time input from sensors that measure parameters like engine timing, vehicle temperature, and vehicle speed.
ECU Imaging	ECU in imaging processes data from various sensors and makes real-time decisions.
ECM	Engine Control Module is a primary controller for the engine. It manages fuel injection, ignition timing, emissions, and other parameters to optimize engine performance and efficiency.
TCM	Transmission Control Module is an electronic device that manages a vehicle's transmission, whether it's manual or automatic.
ABS	Anti-lock Braking System is a safety system designed to prevent wheel lock-up during braking, allowing the driver to maintain steering control.
Traction Control	Traction control systems help prevent wheel spin during acceleration. It works by monitoring wheel speed and reducing engine power or applying brakes to the spinning wheels.
ACU	Airbag Control Unit is responsible for monitoring crash conditions and deploying airbags when necessary.
BCM	Body Control Module manages various electronic functions within the vehicle's body, including power windows, door locks, interior lighting, and more.
ADAS	Advanced Driver-Assistance Systems is a electronic systems in vehicles and a type of data stored in ECU.
G-Force	G-force is a measurement of acceleration that can be experienced in a car when it accelerates, brakes, or turns.
e-SIM	An embedded SIM (e-SIM) is a small chip that allows a car to connect to cellular networks without a physical SIM card. e-SIMs can enable connectivity for features like telematics, vehicle tracking, and infotainment services, providing real-time data and communication capabilities.

Lidar scan	Light Detection and Ranging is a remote sensing technology that uses laser light to measure distances and create detailed, high-resolution 3D maps of the environment.
CD Bunner	A CD burner is a device or software that allows users to write data onto a compact disc (CD).
Pelican Red Bag	Pelican Red Bag is a durable, weather-resistant storage bag often used by law enforcement and forensic teams to transport evidence and sensitive materials securely.
Forensic triage tool	Forensic triage tool is a software that helps to quickly and efficiently process digital evidence from a variety of devices.
Speedometer	Speedometer is a gauge that indicates the current speed the vehicle is traveling.
Tachometer (RPM gauge)	Tachometer is a device that measures the rotational speed of a shaft or disk, usually in revolutions per minute (RPM).
GPS modules	Global Positioning System modules are devices that receive signals from satellites to determine the precise location of a vehicle.
FTK Imager	A forensic imaging tool used to create exact copies of digital evidence, such as hard drives or memory cards.
VLC Player	A versatile media player capable of playing a wide range of audio and video formats.
Write Blocker	A write blocker is a tool that allows digital forensics investigators to examine data storage devices without modifying the data.
BOSCH CDR 900	BOSCH Crash Data Retrieval (CDR) 900 tool is used to access and download data from the Event Data Recorders (EDRs) in vehicles.
Berla iVe	Berla iVe is a forensic software tool used to extract, analyse, and report data from automotive systems and devices, including infotainment systems and teematics units.
Initial stage	The initial stage typically refers to the first phase of an investigation or forensic process, where initial assessments are made, and evidence is collected.
Anti-static	Anti-static refers to materials or techniques that prevent the buildup of static electricity, which can damage sensitive electronic components. This is to ensure that data is not corrupted or lost due to electrostatic discharge.
Metadata	A set of data that describes and gives information about other data.
SHA-256	Secure Hash Algorithm 256-bit is a cryptographic hash function that produces a fixed-size 256-bit (32-byte) hash value from input data of any size.

Triage information	Triage information refers to the preliminary assessment and categorization of digital evidence in an investigation. This process is to evaluate data sources to identify which evidence is most relevant or critical to the case.
Throttle position	Throttle position refers to the angle of the throttle valve in an internal combustion engine, which regulates the amount of air entering the engine.
CCTV	Closed-circuit television (CCTV) also known as video surveillance is the use of closed-circuit television cameras to transmit a signal to a specific place, on a limited set of monitors.
JSPT	Jabatan Siasatan dan Penguatkuasaan Trafik (JSPT)
PDRM	Polis Diraja Malaysia
MIROS	Malaysian Institute of Road Safety Research

1. UNDERSTANDING DATA SOURCE IN PASSENGER CARS

1.1 Overview of Data in Modern Passenger cars

As technology advances, modern passenger cars are increasingly equipped with sophisticated electronic systems that generate and store a significant amount of data. This data provides insights into vehicle operations, driver behaviour, and even external environmental conditions. For law enforcement and digital forensics analysts, this information is invaluable for investigations, especially in cases involving accidents, criminal activities, or other incidents. The integration of Global Positioning System (GPS), telematics, infotainment systems, and advanced driver-assistance systems (ADAS) has made it possible to gather detailed information that was previously inaccessible.

However, data from modern passenger cars also presents unique challenges. The diversity of systems, data formats, and security measures means that law enforcement agencies need specialized knowledge and equipment to effectively retrieve, preserve, and interpret this data. Additionally, proper data handling and preservation techniques are essential to maintain the integrity of evidence for legal purposes. As vehicles grow increasingly sophisticated, the need for standardized guidelines on car data preservation has become paramount.

Data preservation for passenger cars involves the systematic process of identifying, collecting, and safeguarding digital information stored within a vehicle's various systems. This practice is crucial in forensic investigations, as the data can provide valuable insights into the circumstances surrounding an incident, such as accidents or criminal activities.

Preservation methods include:

a. **Securing the Vehicle:** Ensuring that the vehicle is in a controlled environment to prevent tampering or accidental data loss.

b. **Data Extraction:** Using specialized tools to retrieve information from various electronic systems, including the telematics unit, infotainment system, and event data recorder.

c. **Documentation:** Keeping detailed records of the data extraction process, including the methods used, the data collected, and the condition of the vehicle at the time of extraction.

Effective data preservation not only maintains the integrity of the evidence but also complies with legal and procedural requirements, ensuring that the information can be reliably used in investigations and legal proceedings. **The scope of this guideline is on digital data investigation, and will not cover physical and scene investigation.**

1.2 Types of Data Stored in Passenger cars

Modern vehicles are equipped with a variety of electronic systems that collect and store significant amounts of data. Understanding these data types is crucial for effective data preservation during investigations. The following categories of data are typically found in contemporary vehicles:

a. Event Data Recorder (EDR) or Black Boxes

b. Telematics and Infotainment System

c. Airbag Control Module (ACM)

d. Key Fobs e. Dash cams (Front and Rear)

e. Aftermarket technologies

These lists are non-exhaustive. Vehicle manufacturers always aim to improve vehicle safety and overall function, which may lead to additional data sources for forensic investigations. However, for the purpose of this guideline, the aims of data preservation are at EDR and Infotainment System in passenger cars.

1.2.1 Event Data Recorder (EDR) Information

An Event Data Recorder (EDR) is a specialized device embedded within modern vehicles that captures critical data related to the vehicle's performance and occupant safety just before, during, and after a collision. EDRs are designed to provide valuable insights into the circumstances surrounding an accident. These devices are designed to record crucial metrics, including vehicle speed at the time of impact, whether and how hard the brakes were applied, and the position of the throttle to indicate any acceleration or deceleration attempts by the driver. EDRs also log seatbelt usage, showing whether occupants were wearing seatbelts, and record the timing and deployment status of airbags, which can indicate the severity of the crash and help establish whether the vehicle's safety systems functioned correctly. The EDR captures the deceleration force experienced during the collision, providing insight into the impact's intensity.

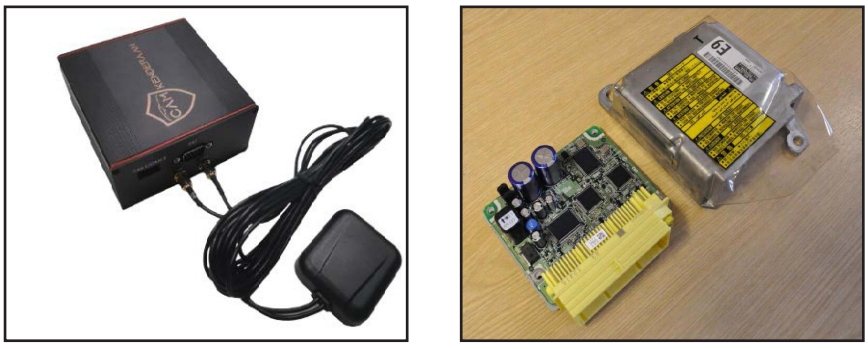

Figure 1. Example of EDRs or also known as Vehicle Black Box. The first image showcases vehicle blackbox developed by CyberSecurity Malaysia and UMPSA under a CAMKenderaan Project.[1]

1 CAMKenderaan Project is a project developed to strengthen digital forensics capabilities in vehicle forensics investigation.

1.2.2 Infotainment System

An infotainment system in passenger cars refers to the in-vehicle entertainment and information features. Infotainment system stores data which can include GPS location, navigation history, call logs, contacts, text messages, media files, and information from connected mobile devices. Modern infotainment systems can interact with smartphones, streaming services, navigation apps, and voice-activated assistants, all of which generate and store substantial data. Infotainment data is valuable in forensic investigations, as it can reveal a vehicle's movements, user interactions, and potentially critical timestamps.

This information can be used as evidence in criminal cases, accident investigations, or insurance claims, especially when understanding the timeline and location details are crucial.

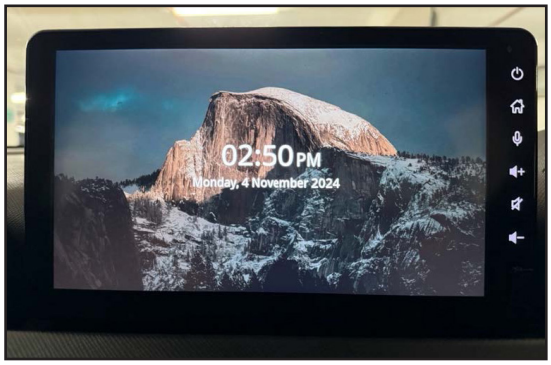

Figure 2. Example of infotainment systems in passenger cars.

1.2.3 Airbag Control Module (ACM)

The **Airbag Control Module (ACM)** is a critical component in modern vehicles, specifically responsible for managing and deploying airbag systems in the event of a crash. It monitors sensors placed throughout the vehicle, such as impact and seat occupancy sensors, to determine when to activate the airbags to protect occupants. Beyond its role in airbag deployment, the ACM also serves as a valuable source of data for vehicle investigations, particularly crash investigations. The ACM is crucial in vehicle investigations because it provides reliable, real-time data on vehicle and driver actions, safety system performance, and crash dynamics.

This data helps investigators reconstruct incidents, assess liability, and verify the function of safety systems, making it invaluable for accident reconstruction, legal cases, insurance assessments, and vehicle safety research.

Figure 3. Sample of ACM photo [2]

2 https://www.autokey.ie/garage-services/acm-airbag-control-module/

1.2.4 Key Fobs

Key fobs in modern passenger cars are more than just keys; they are small, data-storing devices with embedded electronics that communicate with the car's systems. In forensic investigations, key fob data can provide valuable insights into a vehicle's usage and access, especially in cases involving theft, unauthorized use, or reconstructing events around a crime or accident. Key fob data can help establish an accurate timeline of events by revealing when the vehicle was accessed or started. This is crucial in cases where timing needs to be correlated with other evidence or events, such as in criminal investigations or accident reconstructions. However, not all vehicles store detailed data on key fobs, and the extent of data available depends on the vehicle's make, model, and year.

Figure 4. Key Fobs of modern passenger cars stored data such as entry and lock/ unlock history, ignition and engine start information, battery and fob status information and many more.

1.2.5 Dashboard cameras (Front and Rear)

Dash cams, or dashboard cameras, can provide a wealth of information that is extremely valuable in forensic investigations. These cameras are designed to record the road ahead (and sometimes the interior or rear of the vehicle) and can capture critical details about driving events, accidents, and even environmental conditions. Dash cams can provide valuable data for forensic investigations which include video footage, audio recordings (if enabled), date and time stamps, speed and acceleration data, G-force and impact data (in advanced models), event markers and emergency recordings and many more. In forensic contexts, dash cam data is highly valued for its direct visual evidence and real-time documentation, making it an essential tool for accident investigation, legal cases, and insurance claims. The footage is also useful in situations where corroborating evidence is needed, as it can confirm or contradict testimonies and provide a precise, unbiased record of events.

Figure 5. Dash cams can provide valuable information to the law enforcement and forensics analyst in accident investigation and criminal investigation.

1.2.6 Aftermarket Technologies

Aftermarket technologies in passenger cars are devices added by owners or third parties, which can range from GPS trackers and telematics systems to dash cams and driver-assistance tools. These devices can store a wide array of data relevant in forensic investigations, particularly when trying to reconstruct events, assess driver behavior, or investigate unauthorized vehicle usage. Aftermarket technologies range from GPS trackers, driver assistance and collision avoidance systems up to self-driving technologies which claim that the technology can convert a standard car to an autonomous vehicle.

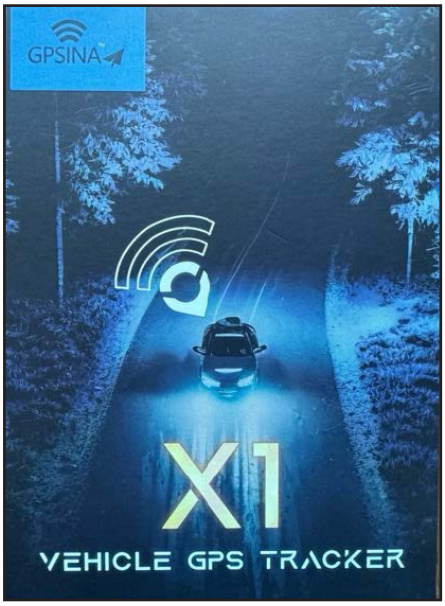

Figure 6. Example of aftermarket technology

1.2.7 Summary

Table 1. Summary of data that can be extracted from different types of devices stored in a car

Type of devices	Types of stored data
Event Data Recorder (EDR)	• Pre- and post-crash data, including vehicle speed, brake application, throttle position • Airbag deployment status and seatbelt use • Impact forces, change in velocity (delta-v) • Time from crash to airbag deployment
Infotainment	• Call logs, contacts, and SMS data (if phone connected) • GPS navigation history and recent destinations • Bluetooth connections and paired devices • Multimedia usage data (radio, music apps, etc.)
Airbag Control Module (ACM)	• Crash data related to airbag deployment • Speed and acceleration information at the time of impact • Status of seatbelt pretensioners and occupancy detection • Engine RPM and throttle position just before impact
Key Fobs	• Last known locking/unlocking activity • Recent vehicle starts and stops • Keyless entry/access events • Vehicle proximity data (if equipped)
Dash cams	• Video footage of the road and vehicle interior (if dualchannel) • Date and time stamps of recorded events • GPS coordinates and vehicle speed overlay • Audio recordings (in some models)
Aftermarket Technologies (e.g., GPS trackers, OBD-II dongles)	• Continuous GPS location data • Driving behavior data, such as acceleration, braking, and cornering (telematics) • Engine diagnostic codes and maintenance data • Fuel consumption and trip duration

2. UNDERSTANDING DATA PRESERVATION IN PASSENGER CARS

2.1 Overview of Digital Forensics Methodology to Preserve Data in Passenger cars

In vehicle forensics, digital forensics methodology is tailored to analyze data from various automotive systems to extract evidence related to vehicle operation, driver behavior, and incident reconstruction. With the increasing complexity of modern vehicles, which integrate multiple digital and connected systems, vehicle forensics requires a structured approach that adapts traditional digital forensics principles to the unique environment of automotive data. Below is a digital forensic principles that would be applied to data preservation in passenger cars.

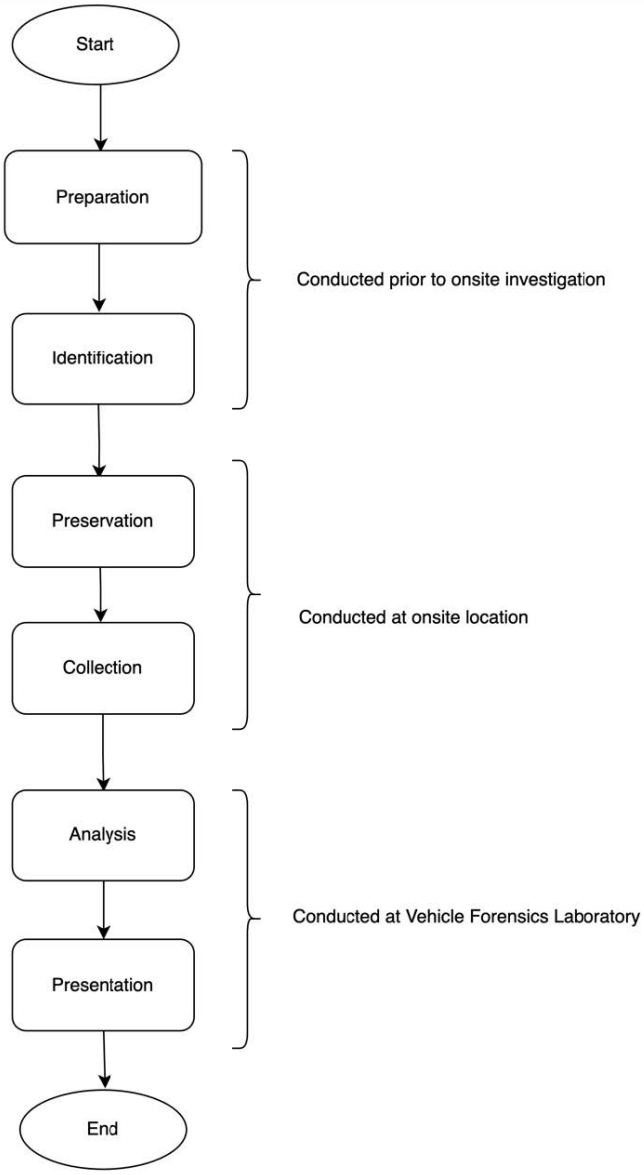

Figure 7. Process flow of Digital Forensics Methodology

The Digital Forensics Methodology could be applied in data preservation of passenger cars. However, in the context of vehicle forensics, each car model, brand and year it is produced plays a vital role in data preservation for passenger cars. In this guideline, the scope does not cover the diversities of car model, brand and year, however the guideline will provide a general basis of preservation for passenger cars. Table 2 below shows the digital forensics processes as well as general description of the processes. Each process will be further elaborated in the next section.

Process	Description
2.1.1 Preparation	**Objective Identification:** Define the purpose of the investigation—whether it is for accident reconstruction, crime/ fraud investigation, or compliance verification. **System Inventory:** Understand the vehicle's make, model, and year, as well as its digital architecture. This includes identifying systems such as Electronic Control Units (ECUs), infotainment systems, telematics, GPS modules, and any aftermarket additions (e.g., dash cams, OBD-II devices). **Legal and Compliance Considerations:** Establish compliance with legal and regulatory requirements for accessing and analyzing vehicle data. Adherence to privacy laws, data protection regulations, and manufacturer-specific policies is essential.
2.1.2 Identification	**Label the car:** It is important to label the car following the agency's case number. Label the data source component as well such as the OBD port, or the ACM components of the car. **Document everything:** The condition of the car, the data source components, the environment of the car should be recorded thoroughly. Maintain a detailed chain of custody for all digital evidence, including any extracted ECUs, hard drives, or data storage devices. This documentation is essential for validating the authenticity of the evidence if presented in a legal context.
2.1.3 Preservation	**ECU Imaging:** ECUs store critical data related to engine performance, braking, steering, and safety systems. Using manufacturer-specific tools, forensic investigators acquire a bit-by-bit image of the ECU to maintain data integrity. **Infotainment System Extraction:** These systems may contain GPS locations, call logs, media history, and Bluetooth connection data. Specialized forensic software or manufacturer-provided access tools are used to extract relevant files without altering the system. **Telematics and GPS Data Collection:** Telematics units and GPS modules often log detailed route history, speed, and geolocation data. Investigators use proprietary or open-source tools to capture this information. **Aftermarket Devices:** Capture data from any additional devices, such as dash cams or OBD-II adapters, which may contain video, audio, trip logs, and diagnostic data. For dash cams, retain video files and associated metadata.

2.1.4 Collection	If data preservation at onsite location is not possible, conduct evidence collection at the premise. **Carefully remove the unit:** Once the unit has been identified, documented and labelled, remove the unit carefully. Register, package, label and seal the unit to be brought to the vehicle forensics laboratory for further analysis. **Document everything:** Ensure to keep record of each process to maintain the chain of custody and ensure evidence integrity is preserved at all times.

Table 2. Process flow of Digital Forensics Methodology and its description

3. PREPARATION

Common sites for conducting data preservation from modern vehicles include police stations, commercial garages, residential driveways, public parking areas and vehicle forensics laboratories. The onsite area depends on the types of cases that are investigated. Therefore, it is crucial to be prepared prior to onsite investigation in order to conduct data preservation for passenger cars successfully. Preparation on data preservation for passenger cars requires a few important steps as per figure 8 below.

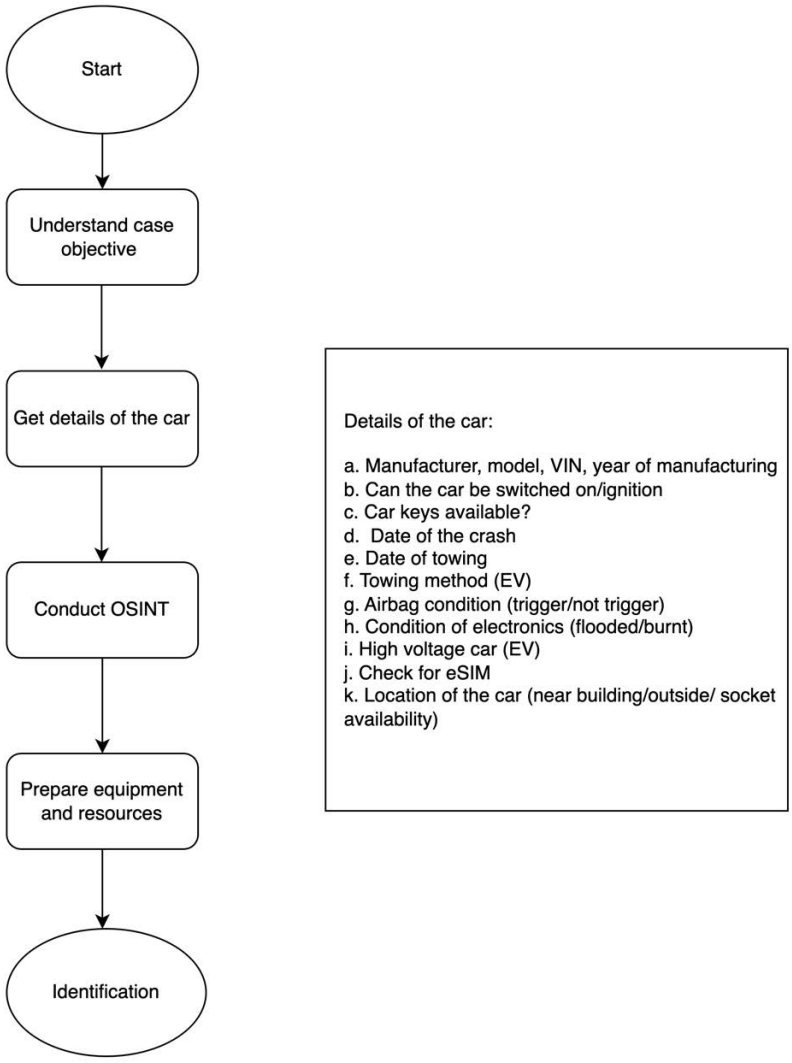

Figure 8. Process flow for preparing for onsite investigation

3.1 Understand Case Objective

The first step of preparing for onsite investigation in the case of vehicle forensics is to understand the case objective or background of the case. Understanding the case objective in vehicle forensics is crucial for investigators, as it guides the entire forensic examination process and helps ensure that evidence is collected, analyzed, and presented effectively. Therefore, the first element in the

investigation process is to define the case objective.

1. Purpose of Investigation: Determine whether the objective is to establish facts related to an accident, theft, or criminal activity involving a vehicle.
2. Scope of the Investigation: Clearly outline what aspects of the case will be investigated, such as vehicle dynamics, driver behavior, or potential mechanical failures.

Investigation Aspect	Key Questions
Purpose of Investigation	
3.1.1 What happened?	What are the details of the incident (e.g., accident, theft, fraud, vandalism)?
3.1.2 What caused the incident?	Was there a mechanical failure, human error, or external factors involved?
3.1.3 Who are the parties involved?	Who are the drivers, passengers, witnesses, and victims?
3.1.4 What are the legal implications?	Are there any legal considerations that need to be addressed (e.g., liability, insurance claims)?
3.1.5 What evidence is needed?	What types of evidence will help establish the facts of the case (e.g., speed of the car, braking (intentional or not), occupant seat belt, on-the-phone driving)?
Scope of Investigation	
3.1.6 What types of incidents are covered?	Are we investigating only this specific incident or similar incidents in a wider context?
3.1.7 Which areas of the vehicle are relevant?	Should we focus on the EDR system, or infotainment or require both data?
3.1.8 What time period is relevant?	Is the investigation limited to the time of the incident, or does it include prior history?
3.1.9 What geographical area is involved?	Are we investigating just the location of the incident or related locations (e.g., where the vehicle was last seen)?
3.1.10 What resources are available?	What personnel, tools, and equipment can be allocated to the investigation?

Table 3. Understanding Case Objective

3.2 Get Details of the Car

The second step of preparing for onsite investigation in the case of vehicle forensics is to get as much details as possible of the car involved in the incident. This step is crucial as it will determine successful data extraction and will help determine the equipment required prior to onsite investigation. Table 4 below outlines the recommended information gathering necessary.

Detail Category	Information Required
Vehicle Identification	• Vehicle Identification Number (VIN) • Make, model and year of the vehicle • Registration details (license plate number)
Ownership Information	• Vehicle ownership at the time of onsite investigation (does the police have the authority to conduct investigation? or require the owner's consent prior to data preservation?) • For insurance cases, does the insurance provider have legal authority to allow for data preservation?
Vehicle Condition	• Car key available? • Can the car be switched on or put in the ignition state? • OBD port available and not damaged? • Is the car registered as total lost (in the case of accident investigation) • What is the condition of the electronics inside the car? Is the car involved in a burnt/ flood/ high voltage incident?
Digital Data	• Identify what kind of data is critical for the investigation? Is it EDR data? Infotainment data? i.e. Do you need to know about speed, braking, throttle position of a vehicle? • Would GPS data suffice? i.e. Last known location, route taken?
Modifications and Accessories	• Third-party installed accessories available? Such as third-party Blackbox, dash cams, or self-driving car accessories?
Crash Evidence	• Damage assessment from any collisions (impact points, crumple zones) • Deployment of airbags or seat belt usage during the incident

Table 4. Some Key Questions in Gathering Information for the Car

3.3 Conduct OSINT

Apart from gathering necessary information regarding the car involved in the case, understanding about the case is equally important to ensure successful data preservation. Some key questions that arise in order to understand the case are:

Key Questions
3.3.1 When is the date of the crash? (in case of crash investigation)
3.3.2 When is the date of car towing?
3.3.3 What is the towing method? - This is important for Electric Vehicles (EV)
3.3.4 Where is the location of the car that is involved in the case? - This is important to understand socket availability
3.3.5 Is it a high voltage car? i.e. EV (might require different procedure and equipment)
3.3.6 Does the car have eSIM?
3.3.7 Study the car manual in case data preservation onsite could not be conducted and removing of Airbag Control Module (ACM) is required

Table 5. Some Key Questions in Intel Gathering for the Case and Car

The intel gathering process can be performed via internet search or by conducting an interview with the Investigating Officer. This process will ensure that sufficient information is collected prior to onsite investigation and in making sure that the right equipment is brought to the onsite location.

3.4 Prepare Equipment and Resources

Once details about the case background and the car have been established, it is important to prepare equipment required for onsite investigation and to form an Onsite Investigation Team. In order to ensure successful preservation of data from the car, below equipment is recommended to be prepared and brought to the onsite location. The recommended form for *Equipment Checklist Form* is in **Appendix A**.

Recommended Equipment
3.4.1 Forensic Workstation (A laptop equipped with forensic software) 3.4.2 Forensic Acquisition Tool (hardware and software) 3.4.3 Forensic triage tool or pre-analysis tool 3.4.4 Power Supply and extension plug 3.4.5 Car Battery 3.4.6 Camera 3.4.7 Plyers, cutters and scissors 3.4.8 CD Burner 3.4.9 Destination Storage i.e. CD-R, DVD, pen drive 3.4.10 Pelican Raid Bag (To fit in all cables necessary and tools) 3.4.11 Car Toolbox 3.4.12 iPad with Lidar scan technology 3.4.13 Drone 3.4.14 Comfort Equipment (mineral water, portable fan, umbrella, bucket hat) 3.4.15 Safety Equipment (reflective jacket, mask, glove) 3.4.16 Trolley wagon 3.4.17 Empty Box 3.4.18 Bubble Wrap

Table 6. Checklist for Onsite Investigation Equipment

Investigating car forensic cases requires expertise in several domains. To ensure a successful investigation, a team consisting of the following expertise is recommended to be formed:

Expertise	Description
Law Enforcement Investigator	Investigating Officer and the Raiding Officers who are in charge of the case e.g. JSPT, PDRM
Road Safety Expert	Experts on Road Safety and Kinematic/ Physical Forensic Investigation team e.g. MIROS
Digital Forensics Expert	Experts on digital forensic who can preserve and collect digital evidence e.g. CyberSecurity Malaysia
Vehicle Manufacturer Experts	In certain cases, it is recommended to have a representative/ expert from vehicle manufacturer to provide experts consultation for electronic components of vehicle involved in the case

Table 7. Suggestion of team members for Vehicle Forensics Onsite Investigation

Apart from equipment and an onsite investigation team, another important item to prepare prior to onsite investigation is to prepare for the required documents. Following are the recommended forms to be brought to onsite location:

1. *Consent Form* (Refer to **Appendix B**)
2. *Service Requisition Form* (Refer to **Appendix C**)
3. *Exhibit at Crime Scene Form* (Refer to **Appendix D**)
4. *Case Work Note* (Refer to **Appendix E**)

4. IDENTIFICATION

The general procedure for conducting onsite investigation on vehicle forensics is described in the following subsections.

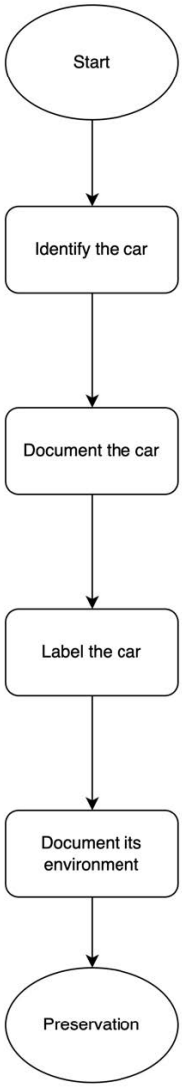

Figure 9. Process flow of conducting onsite investigation for vehicle investigation

4.1 Identify the Car

The first step in onsite investigation involving passenger cars is to identify the car. The car involved in the investigation would have several sub-components that required to be identified as well. Some components that are recommended to be clearly identified are the OBD port, the ECU/ ACM unit (if visible), the infotainment unit (if relevant to the case), the dash cams (if available), as well as third-party accessories (if relevant to the case).

Figure 10. The first step in onsite investigation is to identify the car

4.2 Document the Car

Next, document the car and its subcomponents. Each activity and steps are required to be documented in the *Case Work Note*.

It is recommended for a Forensic Analyst to take a photo of the car and its subcomponents at every angle using a quality camera. It is even better if the Forensic Analyst can scan the car using lidar sensor in Ipad latest version. Example of application that could be used for this purpose is a Polycam 3D Scanner. This can be downloaded from here: *https://apps.apple.com/us/app/polycam-3d-scanner-lidar-360/id1532482376*

Figure 11. Example of 3D Lidar Scanning for Car Involved in Crash for Onsite Investigation

For comprehensive information gathering, it is also recommended for Forensic Analysts to capture the car meter clusters and document it. This is important to help reconstruct the events leading up to the incident. The speedometer and tachometer (RPM gauge) can indicate the vehicle's speed and engine activity at the time of impact or just before the incident. This information helps assess whether speed was a factor in the accident. In some vehicles, the meter cluster might "freeze" certain readings (e.g., speed, RPM, fuel level) at the moment of impact. This snapshot can provide insights into the car's behaviour at the time of the accident. On top of that, the meter cluster information, when cross-referenced with data from the Event Data Recorder (EDR), helps validate the data, confirming aspects like speed, braking patterns, and throttle input, which can be critical for accurate accident reconstruction.

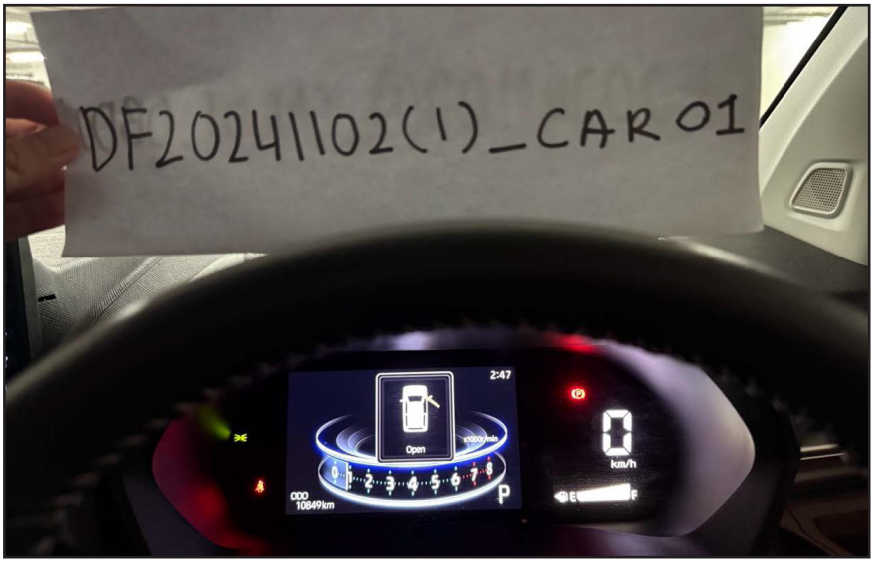

Figure 12. Example of meter cluster with car label taken for onsite investigation. Ensure that the “Odometer reading” is shown in the photo.

4.3 Label the Car

The car and its subcomponent should be labelled and tagged according to the agency's procedure. For example, the label and tag for the car and its subcomponents can be written following example below:

Car:

<Agency’s Code><Date of Investigation><Running number>_CAR<Exhibit number>

E.g:

DF20241102(1)_CAR01

Figure 13. Example of car label on identified car. Ensure that the plate number and case number are shown in the photo.

Car OBD:

<Agency's Code><Date of Investigation><Running number>CAR<Exhibit number>_OBD<Exhibit number>

E.g:

DF20241102(1)_CAR01_OBD01

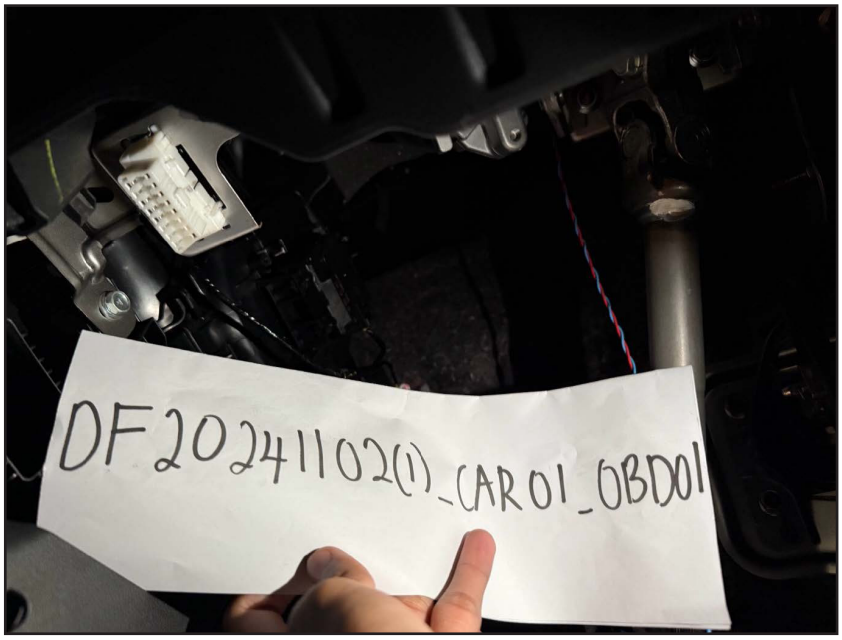

Figure 14. Example of OBD label on identified car. Ensure that the OBD interface and case number are shown in the photo.

4.4 Document its Environment

On top of documenting the car and its subcomponents, it is also important for Forensic Analysts to observe the scene and physical location of the car at the time of onsite investigation. The scene of the car needs to be recorded via quality photography or using a drone camera. This is important to ensure no external environmental factors could cause any impact to the car or subcomponent of the passenger cars.

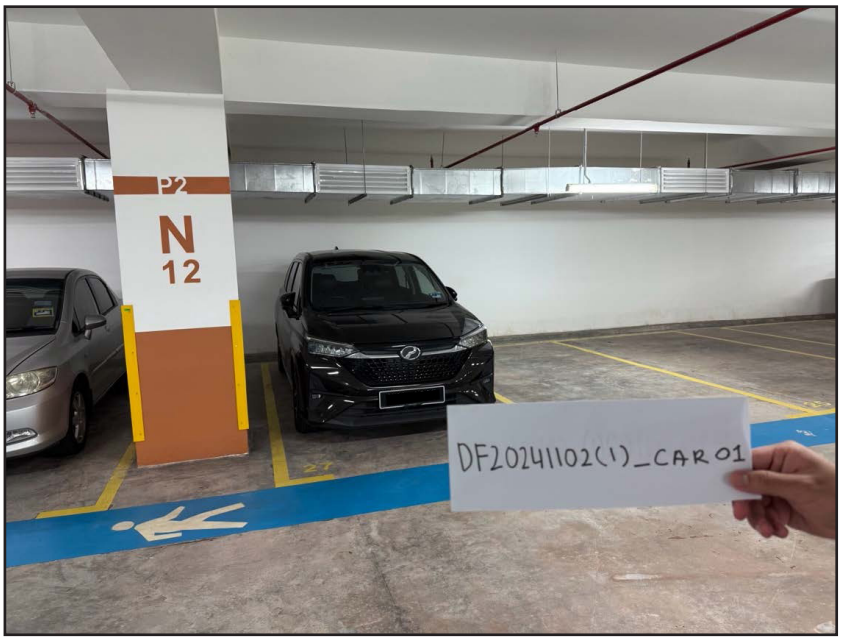

Figure 15. Example of photo that documented the environment of the identified car. Ensure that the Identified Car and the case number are shown in the photo.

5. PRESERVATION

The third step of Digital Forensics Methodology is preservation. In this section, the goal is to preserve relevant data required for investigation. Data preservation for passenger cars requires several equipment connected and communicated to the car in order to ensure successful data preservation. Important consideration when conducting data preservation for passenger cars is to get a *Consent Form* signed by the Investigating Officer or the Car Owner. Figure 16 below shows the recommended steps required in data preservation for passenger cars. The following subsection will discuss each step in detail.

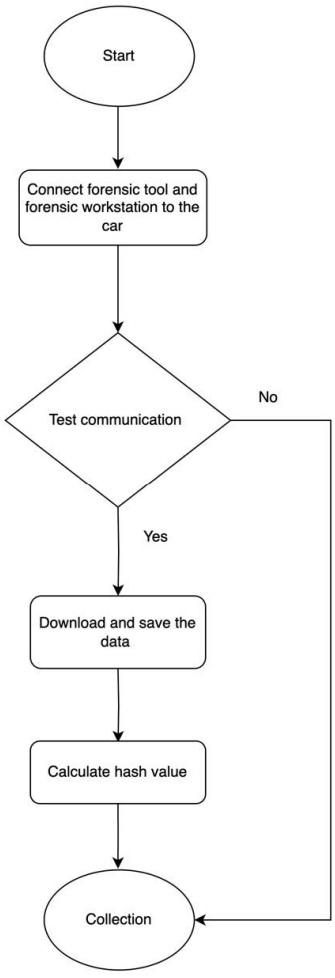

Figure 16. Recommended steps for data preservation

5.1 Connect Forensic Tool and Forensic Workstation to the Car

In the case of data preservation in passenger cars, there are two (2) commercial forensic tools typically used. For EDR data preservation, the most common tool is a crash data retrieval (CDR) tool which is a computer system that images the data from an airbag control module (ACM) after airbag deployment or other automotive incidents. Example of this forensic tool is BOSCH CDR 900. For infotainment data, the most common tool used is Berla iVe which is a forensic software tool used to analyze vehicle data.

To preserve the data of passenger cars, the first step is to connect a forensic tool to the forensic workstation. Forensic workstation is a laptop or rugged laptop used for onsite investigation. This forensic workstation shall be equipped with forensics software and relevant applications required for onsite activities such as FTK Imager, VLC Player, write blocker and many more. Since the connection of the forensic tool and forensic workstation to the identified car require power, it is recommended for Forensic Analysts to ensure that ample power has been supplied to the forensic tool and forensic workstation prior to onsite investigation to ensure successful data preservation. The connection diagram for forensic tool, forensic workstation and the identified car is as per Figure 17 below.

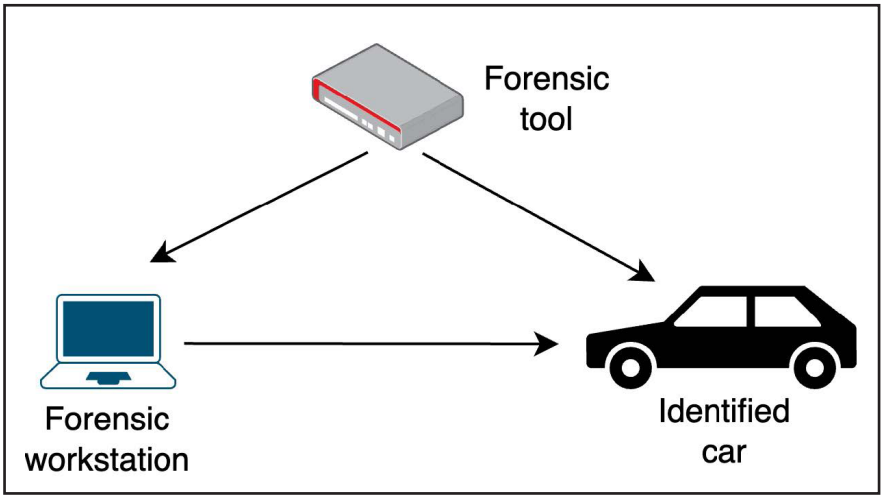

Figure 17. Connection Diagram between Forensic Tool, Forensic Workstation and Identified Car

5.2 Test Communication Between Forensic Tool and Forensic Workstation to the Car

Once a forensic tool and forensic workstation has been connected to the car, it is vital to test for communication of these devices. This is an important step to ensure that the identified car can communicate to the forensic tool and forensic workstation and transmit data. To perform this, follow the steps below:

Step 5.2.1 Switch on the car or put it in ignition state

Firstly, switch on the car. This step is important in order for the car to communicate to the forensic tool and forensic workstation. Therefore, at the initial stage of information gathering, it is vital for Forensic Analysts to know the condition of the car and especially if the car can be switched on and whether the car keys are available. If the car could not be switched on, then it is recommended for the Forensic Analysts to provide the car with additional power by using a battery charger. This can be achieved by having a power car battery charger, which could be purchased from a car accessories store.

Step 5.2.1 Test communication between Forensic Tool and Forensic Workstation

Once the car has been switched on, try to communicate the forensic tool and the forensic workstation to the car by turning on the forensic tool and forensic software in the forensic workstation. If enough power is supplied to all - forensic tool, forensic workstation and the car, the communication would be successfully established. However, if communication could not be established, try connecting the forensic tool and forensic workstation to the external power supply. It is recommended for Forensic Analysts to bring external power supply during onsite investigation in case there is no electrical power supply available at the onsite premise.

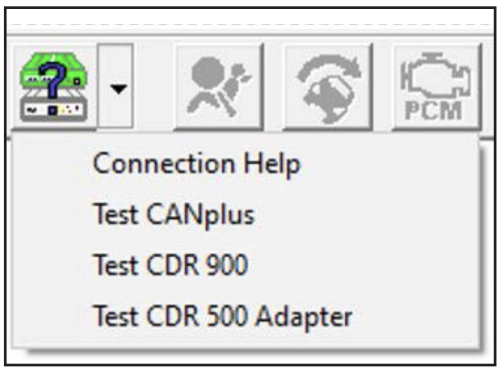

Figure 18. Example of Test Communication Button in BOSCH CDR software

Figure 19. Example of successful connection of forensic tool

Step 5.2.3 If no communication could be established

If no communication between the forensic tool and forensic workstation to the car could be established, then proceed to Step 4: COLLECTION.

5.3 Download and Save the Data in Native/ Proprietary and PDF Format

Once the communication has been established, download the car data into a forensic workstation. It is important to download and save the data in native/ proprietary format as well as PDF format. The aim is to maintain data integrity by preserving the exact format and structure of the original files. This helps avoid altering any metadata, timestamps, or file characteristics, which can be critical in investigations and for evidence authenticity in court. The downloaded files (including the hash values) are then burnt inside a DVD/ CD-R, packaged, labelled, and sealed following a forensically sound method.

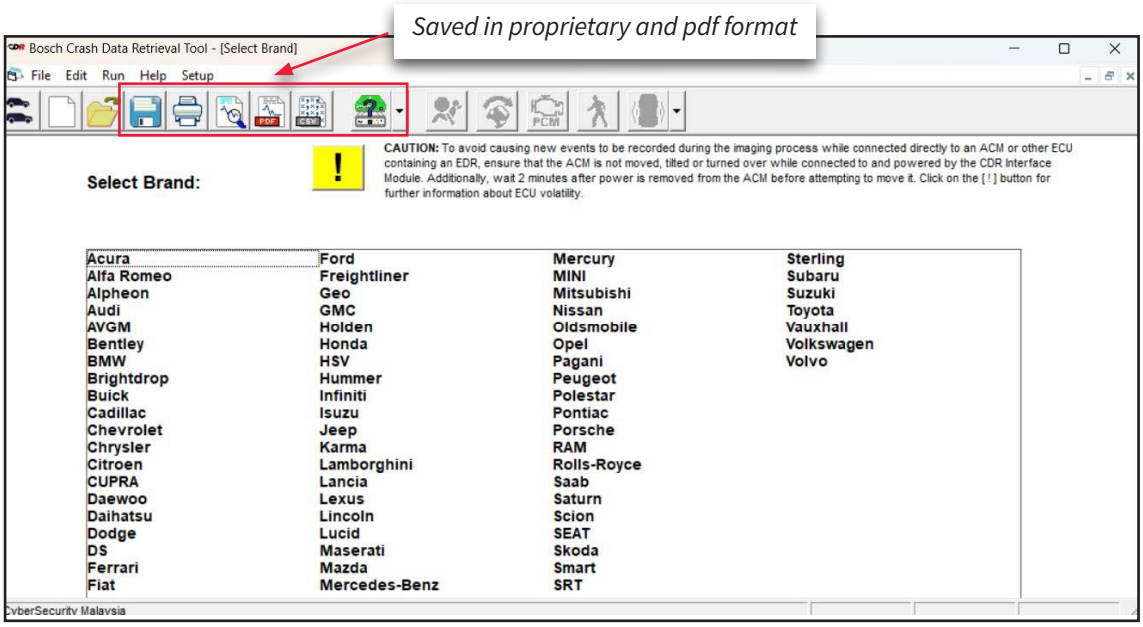

Figure 20. Example of options for saved data

5.4 Calculate Hash Value

Next, calculate the hash value of the files, both proprietary/ native and PDF format files. This can be performed using FTK Imager or any hash calculator available. Calculating the hash value of files is fundamental in digital forensics because it helps ensure the **integrity and authenticity** of digital evidence. A hash value is a unique, fixed-length string of characters generated by applying a mathematical function to a file. Even a small change in the file's content (like a single byte) will produce a completely different hash value. It is recommended to use **SHA-256 (Secure Hash Algorithm 256-bit)** due to its strong security properties and widespread acceptance in forensic and legal contexts.

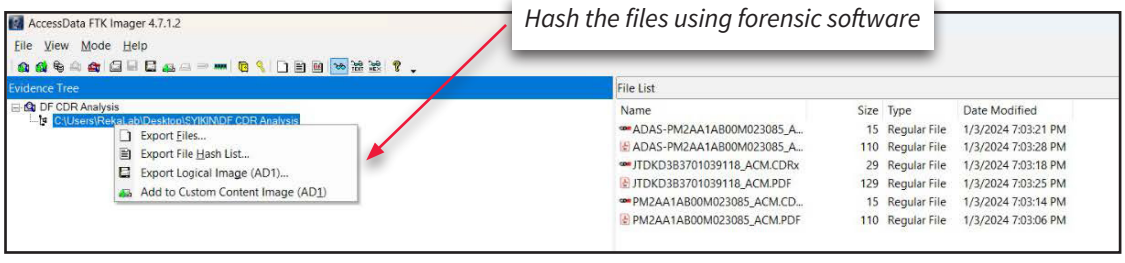

Figure 21. Example of hashing method using FTK Imager

6. COLLECTION

This method applies if preservation of data during onsite investigation fails. This method requires understanding of car components and interfaces in order to locate and identify car components that possess reliable and relevant data to assist investigation. However, this method should be applied **only in cases of utmost necessity**, where its use is critically essential to the objectives of the investigation. It is recommended to exhaust all alternative methods before resorting to this approach, due to the potential implications and resources involved. Important consideration when conducting data preservation for passenger cars is to get a *Consent Form* signed by the Investigating Officer or the Car Owner. The Risk Consideration and Mitigation is further elaborated in Section 11 of this document.

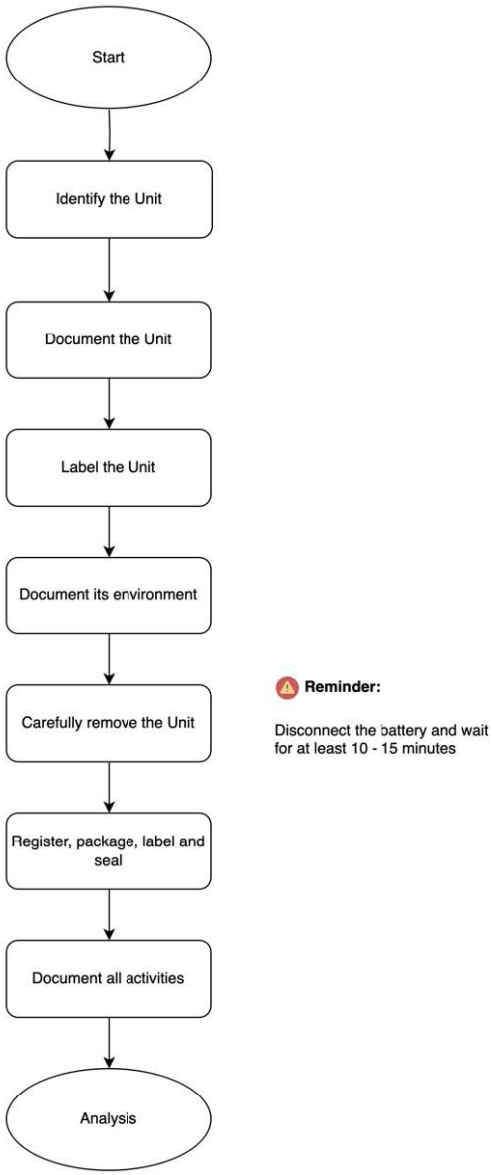

Figure 22. Steps to collect unit from car

6.1 Identify the Unit

Similar to the preservation step, the first step in the collection method is to identify the unit that is relevant to the investigation. There are many components of passenger cars that possess data for investigation, however it is difficult to preserve the data and decipher the data to a readable format. This requires commercial and specialized tools and would also depend on the brand, model and year of car manufactured. This also ties back to the background and case objective. What data would be relevant to the investigation and which components would need to be analyzed?

If preservation of data through the OBD interface of a car fails, it is recommended for Forensic Analysts to identify the location of the Airbag Control Module (ACM). Every brand, model and year of car manufactured would make a difference in the location of the ACM. Common location for ACM include:

Common Location of ACM	Description
Center Console:	Many vehicles place the ACM under the center console, usually near the gear shift or beneath the dashboard. This location helps protect the module in the event of a collision.
Under the Driver or Passenger Seat:	In some passenger cars, the ACM is located under the front seats. This placement allows for easy connection to various sensors and airbags throughout the vehicle.
Behind the Dashboard:	Another common location is behind the dashboard, often closer to the steering column or just above the pedals.
Floorboard Area:	In certain vehicles, the ACM is mounted to the floorboard area, usually in the middle section under the carpet. This provides stability and protection from direct impact.

Table 8. Common location of ACM in passenger cars

Therefore, it is recommended for Forensic Analysts to consult the car repair manual or manufacturer guidelines to get the exact location of the ACM, as it varies by make and model.

6.2 Document the Unit

Next, document the unit by taking a photo of the unit at all angles using a high quality camera and record each activity and steps in the *Case Work Note*. It is recommended for the unit to be documented prior to removing its outside of its casing.

Figure 23. Example of ACM Unit

6.3 Label the Unit

The unit should be labelled and tagged according to the agency's procedure. For example, the label and tag for the unit can be written following example below:

Car ACM:

<Agency's Code><Date of Investigation><Running number>CAR<Exhibit number>_ACM<Exhibit number>

E.g:

DF20241102(1)_CAR01_ACM01

Car Infotainment Unit:

<Agency's Code><Date of Investigation><Running number>CAR<Exhibit number>_UNIT<Exhibit number>

E.g:

DF20241102(1)_CAR01_UNIT01

6.4 Document its environment

On top of documenting the unit itself, it is also important for Forensic Analysts to observe the scene and physical location of the car at the time of onsite investigation. The entire environment of the unit including its casing needs to be recorded via quality photography. This is important to establish the condition of the unit prior to removing it.

6.5 Carefully Remove the Unit

Next, it is recommended for Forensic Analysts to wear proper gear to perform this activity as the steps needed would be hazardous if not performed correctly. Follow proper steps below:

Step 6.5.1 Disconnect the Battery

Always disconnect the car battery, and wait at least 10-15 minutes before working on the ACM. This allows any residual power to dissipate, reducing the risk of accidental airbag deployment. Step

6.5.2 Follow Manufacturer Instructions

Different passenger cars have specific procedures for removing the ACM. Following the manufacturer's guidelines ensures that you're using safe and correct techniques.

Step 6.5.3 Use Proper Tools and Grounding

Use the recommended tools to avoid damage to the module or surrounding components. Anti-static measures may be necessary to prevent static discharge, which could inadvertently trigger the airbags.

Step 6.5.4 Avoid Impacting the ACM

Handle the module carefully. Dropping, bumping, or mishandling it can damage its internal components or sensors, potentially rendering it unreliable or even triggering deployment. Step

6.5.5 Professional Assistance Recommended

If you are not experienced with airbag systems or vehicle electronics, consider seeking professional assistance. Airbag systems are complex and sensitive to interference. Since the ACM controls a crucial safety system, mishandling it can compromise safety, leading to potential injury or malfunction.

6.6 Register, Package, Label and Seal

Once the ACM or Infotainment Unit has been carefully removed, follow a forensically sound method to register, package, label and seal the unit. Place the label onto the unit, register the unit into Exhibit at Crime Scene Form and wrap the unit with a bubble wrap and package it inside a box . The package is then sealed and labelled again.

Figure 24. The unit is then register, package, label and seal as shown above

6.7 Document All Activities

It is important to document all activities performed during onsite investigation. The unit that has been packaged shall be recorded at all times, before and after it has been packed and sealed as well. The activities performed during onsite investigation shall be recorded in the *Case Work Note*.

7. ANALYSIS

This method is conducted at Vehicle or Digital Forensics Laboratory. This method is performed by analyzing the data retrieved from the car prior to report writing. The recommended analysis steps is shown in figure 25 below. **This guideline will not cover the detail steps for analysis.**

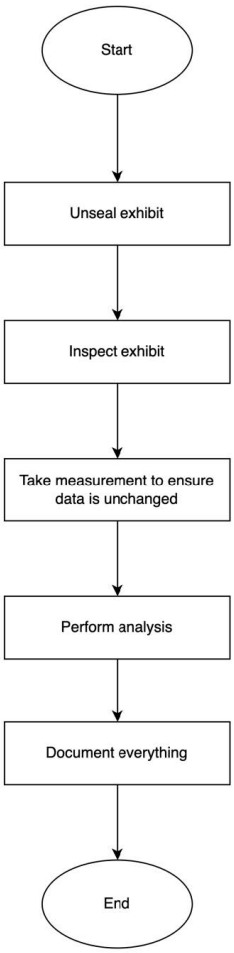

Figure 25. Recommended analysis steps

8. PRESENTATION

At the end of the onsite investigation, it is recommended for the Forensic Analysts to create a brief report of the activities conducted onsite. Now that digital evidence has been collected at the crime scene, investigators need to put the summary of the detailed activities in the form of a report. The goal of the reporting process is to present a clear, accurate, and comprehensive account of the investigation, ensuring that the results are understandable and usable by the prosecutors of the case or the higher management.

Report is usually written by the Forensic Analysts that handles the digital evidence. Table 8 shows the list of data to be documented in the report for the vehicle forensics onsite investigation.

Recommended Vehicle Forensic Report Content	
8.1	Car Details E.g. Brand, model, year manufactured, VIN number, plate number, Odometer status
8.2	Data Extracted E.g. ECU data, ACM data, Infotainment data, Dash cams footage, third-party accessories data
8.3	Damage Evidence E.g. Broken lights, impact points, crumple zone
8.4	Speed Profile Analysis E.g. Speed of vehicle, Acceleration calculation
8.5	Opinions and Recommendations Forensic Analysts to provide opinions and recommendations, if necessary
8.6	Other digital device information (Computer, mobile phone, CCTV) *discovered at crime scene Brand, model, manufacturer (Refer to best practices for seizing digital evidence)

Table 9. List of data to be documented related to the vehicle forensics onsite investigation

The chain of custody of the seized evidence must also be documented. Forensic Analysts may use the agency's *Exhibit at Crime Scene Form* to document the process of exhibit handling.

Now that the digital evidence has been collected, it needs to be analyzed in order to extract deleted data, recover any hidden data and reconstruct all the data into meaningful facts. Following the reporting process, investigators then submit the digital evidence to the vehicle forensics laboratory for the purpose of analysis.

9. SUBMISSION OF EVIDENCE TO VEHICLE FORENSICS LABORATORY

Digital evidence that needs forensic analysis can be submitted to a **CyberSecurity Malaysia's Vehicle Forensics Laboratory**. The purpose of sending the digital evidence to the forensic laboratory is for data preservation (in case of ACM collection), data recovery, data reconstruction and data correlation.

The following items need to be supplied to the laboratory when requesting for digital evidence analysis:

a. Case objective - clear scoping for the analysis
b. Triage information - data that has been collected at the crime scene
c. The digital evidence - Identified Car, Identified Unit, Dash Cams Unit

When submitting the digital evidence to the forensic lab, clear case objectives need to be supplied to the forensic laboratory. Examples of case objectives are as following:

a. to extract data from identified car involved in investigation
b. to extract data from ACM unit collected at onsite investigation
c. to extract information from the car or unit such as speed, braking status, throttle position, occupant seat belt status, etc

At the end of the analysis process, the laboratory will produce a forensic report. This report can be submitted to the prosecutor for case review. It can also be tendered into the court to support the case investigation.

10. REQUEST FOR DATA FROM CAR MANUFACTURER

If all method fails or the extracted data is insufficient or not complete, it is recommended for the Investigating Officer to request the data from the car manufacturer. Most car manufacturer has its own diagnostic tool that would be able to extract out the data from their car. The important data to be requested from car manufacturers are as follows:

Suggested Data to be Requested	
10.1	Vehicle Make and Model Specifics about the vehicle's capabilities and limitations
10.2	Speed Vehicle speed at different time intervals
10.3	Acceleration/Deceleration Patterns of rapid acceleration or braking
10.4	Steering Angle Input data for directional changes
10.5	Throttle Position How much the accelerator pedal was pressed
10.6	Brake Pressure Data on brake application force
10.7	Gear Position Current gear or transmission status
10.8	Cruise Control Settings If and when cruise control was active
10.9	Event Triggers Collision detection, airbag deployment, or sudden stops
10.10	Timestamp and GPS Location Exact time and place of incidents
10.11	Pre-Crash Data Few seconds of data before the incident, often stored in Event Data Recorders (EDRs)
10.12	Yaw Rate Rotational movement around the vertical axis
10.13	Seatbelt Status Whether the seatbelt was fastened

Table 10. List of requested data for Investigating Officer reference

11. RISK CONSIDERATION AND MITIGATION

When conducting a preservation of data from a car, it is vital to know the type of car that is being investigated. Especially to know whether the car that is being investigated is a fully Electric Vehicle (EV) or running on gas/ petrol. Some risk considerations and mitigations are listed below:

Risk Considerations and Mitigation	
11.1 Electric Vehicles	**11.1.1 High-Voltage Battery Risks:** EVs are powered by high-voltage lithium-ion batteries, which can range from 400 to over 800 volts. This high voltage poses a severe shock hazard. Handling or accidentally short-circuiting these batteries can result in electrical burns, fires, or even explosions. **11.1.2 Data Loss Risks:** EVs store data in various electronic control units (ECUs) and other modules that may reset, delete, or overwrite data when the vehicle powers down or experiences voltage drops. Attempting to power on the vehicle or interact with these systems without proper safeguards could lead to accidental data loss or corruption, complicating forensic investigations. **11.1.3 Fire and Toxic Gas Risks:** If damaged or improperly handled, EV batteries may release toxic gases or cause thermal reactions that can ignite surrounding materials. Handling EVs safely requires proper ventilation, fire suppression tools, and training in dealing with potential toxic fumes.

11.2 Removing ACM	**Unit 11.2.1 Risk of Airbag Deployment:** The ACM is responsible for controlling the airbags and other passive safety systems. Removing or handling the ACM without proper precautions can inadvertently trigger airbag deployment, which could cause injury due to the sudden force, even if the battery is disconnected. Airbags deploy with significant speed and force, potentially injuring nearby individuals. **11.2.2 Static Electricity Sensitivity:** Airbag systems are sensitive to static electricity. Any static discharge during the removal of the ACM could inadvertently trigger the airbag deployment mechanism. Proper grounding and handling procedures are necessary to reduce this risk. **11.2.3 Data Loss Risk:** From a forensic perspective, improperly removing the ACM can risk data loss or corruption, as the module may contain crash data and other critical information about the vehicle's recent events. Following safe extraction protocols is essential to ensure the integrity of data for forensic analysis.

Table 11. Risk Considerations and Mitigation for Performing Onsite Investigation for Car

For these reasons, data preservation in EVs and the need to remove the ACM should only be conducted by professionals trained in both EV handling and digital forensics, and who have access to specialized equipment and personal protective gear.

Another consideration for onsite investigation is to ensure the process conducted at the field site is witnessed by another officer.

REFERENCES

1. SWGDE Best Practices for Vehicle Infotainment and Telematics System, https://www.swgde.org/wp-content/uploads/2023/11/2022-01-13-SWGDE-Best- Practices-for-Vehicle-Infotainment-and-Telematics-Systems_v3.0.pdf
2. Issues of Vehicle Digital Forensics, https://www.researchgate.net/profile/Roman-Rak- 2/publication/347815849_Issues_of_Vehicle_Digital_Forensics/links/6028473c458515 8939a24d04/Issues-of-Vehicle-Digital- Forensics.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uRG93bmxvYWQiLCJwcmV2aW91c1BhZ2UiOiJwdWJsaWNhdGlvbiJ9fQ

APPENDIX A: EQUIPMENT CHECKLIST FORM

CamKenderaan

EQUIPMENT CHECKLIST

Please tick (√) on the left side of Equipment Column for each equipment taken. On the Quantity Taken column, please fill in the amount of equipment taken. For the Quantity Return column, the DF Technical Assistant will check whether the personnel had returned the same amount of equipment taken. Please fill in Section A upon taking equipment and Section B upon returning equipment.

Equipment		Quantity		Equipment		Quantity	
		Taken	Return			Taken	Return
	CDR 900				**Berla**		
	Cable Power Adapter				Cable Power Adapter		
	Power Supply & Power Switch				Power Supply & Power Switch		
Equipment		**Quantity**		**Equipment (Dongle)**		**Quantity**	
		Taken	**Return**			**Taken**	**Return**
	Sarotech				Encase		
	Power Cable				Axiom		
	USB Cable				Berla		
	Fire Wire Cable				Virtual Crash		
	SATA Adapter				FTK		
Equipment		**Quantity**		**Consumable Item**		**Quantity**	
		Taken	**Return**			**Taken**	**Return**
	Tool-Box (Small)				Exhibit Label Sticker		
	Memory Card Reader				Hard-Disc		
	Extension Plug 3-Pin				Compact Disc (CD)		
	Digital Camera				Digital Video Disc (DVD)		
	Extension Plug 2-Pin				SCSI Signal Cable		
	Laptop and Charger				Empty Box		
	Drone				Mineral Water		
	Extension DVD Drive				Umbrella		
	Macbook				Reflective Jacket		
	Ipad				Mask		
	Pendrive				Glove		

AUTHORISATION			
SECTION A (Upon Taking Equipment)		**SECTION B** (Upon Return Equipment)	
Name		**Name**	
Date		**Date**	
Name		**Name**	
Date		**Date**	

APPENDIX B: CONSENT FORM

CONSENT FORM FOR ACCESS AND DATA EXTRACTION OF VEHICLE EVENT DATA RECORDER (EDR) AND PERSONAL DATA

PARTY REQUESTING CONSENT:

[Name of Agency/Department] : _____

[Address] : _____

[Phone Number] : _____

[Email Address] : _____

PARTY PROVIDING CONSENT (Data Subject):

Name: : _____

NRIC/Passport Number : _____

Address : _____

Phone Number : _____

Email Address : _____

LEGAL BASIS FOR REQUEST:

This request for access and extraction of vehicle and personal data is being made pursuant to the lawful authority vested in the [Agency/Department's Name] under the following legal provisions:

1. The Road Transport Act 1987 (Act 333
2. The Penal Code (Act 574)
3. Other relevant statutory authority under Malaysian Law

APPENDIX B: CONSENT FORM (CONTINUED)

UNDERSTANDING AND ACKNOWLEDGEMENT

1. I acknowledge that my personal data and vehicle data may be accessed and extracted for the purpose specified above.
2. I understand that data extraction process may require limited access to certain parts of my vehicle's interior, and I release [Agency/Department Name] from liability for any reasonable damage incurred to access the components as stated above.
3. I acknowledge that any data collected from my vehicle may be used as evidence in any investigation and may be shared with relevant authorities or any other law enforcement agencies or government bodies for verification and case processing purposes.
4. I acknowledge that this authorization is voluntary, and I have the right to refuse to provide consent. By signing below, I confirm that no coercion, threats, or promises have been made to induce my consent.
5. I understand that [Agency/Department Name] will take reasonable steps to preserve all collected data and components and provide me with a copy of this authorization upon request.
6. A photocopy of this signed authorization shall be considered as valid as the original.

Signatures	**Witness Signature (if required)**
Signature of Owner/ Authorised Representative	Signature of Witness
Full Name :	Full Name :
NRIC No :	NRIC No :
Date :	Date :

APPENDIX C: SERVICE REQUISITION FORM

CamKenderaan

SERVICE REQUEST FORM (SRF)

CASE INFORMATION		
Case No:	**Service Category:**	**Type of Request:**
Related Case No:	☐ Collision Investigation ☐ Criminal Investigation ☐ Fraud Investigation	☐ Lab ☐ On-site
Case Type:	**Act:**	

CUSTOMER INFORMATION	
Customer Reference No:	
Customer Name:	
Address:	**Contact No:**
	Email:

Case Objective(s):
DISCLAIMERS Digital Forensics Department (DFD) of CyberSecurity Malaysia's Customers agree, prior to any work being performed, that DFD will determine the scope of work, the type of examinations to be performed, and the items need to be examined and analyzed. DFD acknowledges that each case is unique and will provide the most appropriate analysis possible.

APPENDIX D: EXHIBIT AT CRIME SCENE FORM

EXHIBIT at CRIME SCENE FORM (ECS)

DFD		Customer			
FR Case No.		Name		Agency	
		Email		Address	
DF Case No.		Phone			

The following exhibits were identified at the crime scene and tagged as in the column 'Exhibit Label'. The details of exhibits are as following:

Table 1: Primary Source
(PLEASE WRITE IN CAPITAL LETTERS)

Primary Source ID	Exhibit Label	Unique Identifier (Serial Number or any Marking)	Manufacturer & Model	Condition	Location	Remarks (Write 'Make copy' if you create OS and proceed to Table 2)
1						
2						
3						
4						

The following table is to be filled in IF the Primary Source was forensically copied at crime scene. The related exhibit is forensically copied, put into a container and tagged as in the column Logical. The container is then put into a physical device tagged as in the column Physical; as following:

Table 2: Original Source
(Forensic copy of the Primary Source)

No	Physical			Logical		Remarks
	Exhibit Label	Unique Identifier (Serial Number or any Marking)	Manufacturer & Model	Folder/File Name	Primary Source ID	
1						
2						
3						
4						

CHAIN OF CUSTODY

By signing the following column, you are aware that:

1. The exhibits (Original Source) are now under your custody. The responsibility of the CHAIN OF CUSTODY shall be yours.
2. The forensic copy of the Primary Source is made in a forensically sound manner, and it shall serve as the ORIGINAL EXHIBIT. Extreme caution shall be taken to ensure that NO TAMPERING is made to this device.
3. The ORIGINAL EXHIBIT shall be SEALED by CSM before it is handed over to you.

Hand over by:	Received by:
_____ Name: NRIC/Passport No: Date & Time:	_____ Customer's Name: NRIC/Passport No: Date & Time:

APPENDIX E: CASE WORK NOTE

CASE WORK NOTE

DFD Case Number:

LIST OF ACTIVITY				
No	**Date & Time**	**Tools**	**Activity**	**Attachment**

In the case other Analyst writes thereport, the Analyst must read this pageand put down initial: ----------	In the case other Analyst provides testimony in court, the Analyst must read this page and put down initial: ----------

SECTION A: CYBERSECURITY MALAYSIA REVIEWER APPROVAL

This document has been prepared by Digital Forensics Department, CyberSecurity Malaysia and intended to be used by Forensic Analysts in CyberSecurity Malaysia. This document also serves as a guideline for other agency that has vehicle forensics capability to perform onsite investigation with regards to car.

Prepared by:

Sharifah Nurul Asyikin Syed Abdullah
Digital Forensics Senior Analyst/ Vehicle Forensics Manager
Digital Forensics Department
CyberSecurity Malaysia

Date: 26/11/2024

Reviewed by:

Dr. Sarah Khadijah Taylor
Head of Research and Development
Digital Forensics Department
CyberSecurity Malaysia

Date: 26/11/2024

Verified by:

Tajul Josalmin Bin Tajul Ariffin
Head, Digital Forensics Department
CyberSecurity Malaysia

Date: 27/11/2024

Approved by:

Mohd Zabri Adil Bin Talib
Head of Division, Responsive Technology and Services
CyberSecurity Malaysia

Date: 27/11/2024

SECTION B: STAKEHOLDER SIGN-OFF

This document has been prepared by Digital Forensics Department, CyberSecurity Malaysia and intended to be used by Forensic Analysts in CyberSecurity Malaysia. This document also serves as a guideline for other agency that has vehicle forensics capability to perform onsite investigation with regards to car.

Reviewed by:

Ir. Ts. Ahmad Noor Syukri Zainal Abidin
Lead Principal Crash Reconstructionist
Vehicle Safety & Biomechanics Research Centre Malaysian Institute of Road Safety Research (MIROS)

Date: 19/12/2024

Reviewed by:

Dr. Mohamad Heerwan Bin Peeie
Senior Lecturer, Fakulti Teknologi Kejuruteraan Mekanikal dan Automotif
Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA)

Date: 19/12/2024

THIS PAGE IS INTENTIONALLY LEFT BLANK

THIS PAGE IS INTENTIONALLY LEFT BLANK

CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan
Malaysia

Tel: +603 8800 7999
Fax: +603 8008 7000
Email: enquiry@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

@cybersecuritymy
CyberSecurityMalaysia
cybersecurity_malaysia
CyberSecurityMy

MINISTRY OF DIGITAL