Scientific Working Group on Digital Evidence

Best Practices for Vehicle Infotainment and Telematics Systems

12-F-004-3.2

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address

d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Best Practices for Vehicle Infotainment and Telematics Systems

Table of Contents

1. Purpose

The purpose of this document is to describe best practices for the collection, preservation, and acquisition of data contained within infotainment and telematics systems installed in vehicles. The intended audience is first responders and examiners involved in the collection and analysis/examination of digital data from vehicles. For the purposes of this document, the term "collection" refers to any operations involved in the gathering, seizing, etc., of items to be examined/analyzed.

2. Scope

This document provides basic information on the acquisition of data from vehicle infotainment and telematics systems.

In-vehicle infotainment (IVI) is an integrated Electronic Control Unit (ECU) installed in vehicles that delivers content for entertainment and informational purposes. Infotainment systems generally connect a user to their digital world (i.e., iOS CarPlay, Android Auto).

Telematics includes external wireless connections to and from a vehicle for data and information transfer. Telematics can be embedded within the vehicle (i.e., OnStar) or through a tethered device via USB or Bluetooth. Besides just using it for connectivity, a telematics system may also access and store the data from a tethered device (e.g., contacts, SMS).

Some vehicles contain both an IVI and a telematics system.

For the purposes of this document, the term "examiner" is used broadly to refer to individuals who have specialized training, knowledge, skills, and abilities that allow them to handle a wide range of technical issues related to digital forensics, and who may be performing technical tasks to include collections, acquisitions, analysis, or combinations thereof.

3. Limitations

This document is not all-inclusive, does not contain information relative to or in support of specific commercial products, is not intended to be a training manual or to specify operating procedures, and the ideas, concepts, and technical aspects of acquiring and analyzing data from IoT devices are strictly related to what was available at the time this document was created.

Research should be done on each vehicle and scenario prior to interaction to ensure as many variables as possible are considered. This may include understanding what tools may be needed, how and where the analysis will take place, how the vehicle will be transported or maintained in - place, etc.

4. Additional Considerations

The safety of first responders is always the priority. Power to modules, such as the Airbag Control Module, may cause the deployment of the airbag if it is removed incorrectly. There may also be a risk of electric shock when attempting to remove internal components that have power.

Vehicles that have been involved in an accident may have broken or misplaced parts that could harm an individual attempting a module removal. This could also include the presence of hazardous materials (i.e., biological hazards or flammable liquids). Follow your agency's or industry standard protocols for handling hazardous materials and proper use of Personal Protective Equipment (PPE). Vehicles with high-capacity batteries, such as all-electric and hybrids, may also pose additional hazards due to high voltage amperage that should be considered.

Be aware of potential liability concerns regarding reinstallation of any module. Improper reinstallation may cause the device or vehicle not to function properly.

5. Securing Evidence and Preserving Data

Infotainment and telematics systems present unique challenges to law enforcement due to a number of factors. These factors may include the physical size of the evidence, differences in hardware designs and manufacturers, limited information on the underlying software and proprietary operating systems, encrypted media associated with Digital Rights Management (DRM), data located in various cloud resources/locations, rapid changes in technology, complexity and inaccessibility of components of interest, etc.

5.1 Physical Seizure and Preservation

Responders/examiners should be aware that, especially in the case of a crash, some important components may have become separated from the vehicle. As many of the vehicle components as possible should be gathered and maintained with the vehicle as part of securing and seizing the vehicle, to include any peripherals and incidentals. Evidence should be handled according to agency policy and a chain of custody properly executed and maintained.

Peripherals and other devices that may accompany a vehicle may include:

- Key fob(s) and cards
- Dash camera(s)
- RFID passes for gates and tolls
- On-board Diagnostics v2 (OBD-II or OBD2) Dongles
- Mobile devices (e.g., cell phones, Amazon Auto, Bluetooth speakers)
- GPS
- Laptops, tablet, or other linked peripherals and devices

5.2 Data Preservation

Responders/examiners should be aware that the vehicle’s digital systems are like any other digital device/system and therefore must be handled appropriately to prevent data modification/destruction. A modern-day vehicle will contain multiple computers and networks (e.g., Wi-Fi, cellular, Bluetooth) and therefore the examiner should take reasonable measures to

disconnect or isolate those elements (e.g., disconnect the vehicles battery, disconnect antennas or cellular modems, remove SIM cards). If it is suspected that relevant cloud data may exist (whether by the vehicle manufacturer or a third party), measures should also be taken to preserve it.

ECUs constantly draw power from a vehicle's battery, even while the ignition switch is in the "off" position. Many ECUs, like the infotainment and telematics systems, utilize key components, such as an unlock event or doors opening/closing as cues, to enter low-power mode or start a power-up procedure. Minimizing the number and duration of power cycles helps preserve data.

Processing a vehicle for physical evidence may cause additional power cycles, resulting in the loss of relevant data. To mitigate this risk, a responder/examiner should discuss these requirements and the order in which they should be performed with the investigator and crime lab personnel to avoid inadvertent destruction of physical and digital forensic evidence.

Typically, the order should be to document any on-screen data, digital readouts, displays, etc., and properly shut down the vehicle to allow the ECUs to correctly power-down (aka perform a graceful shutdown) before processing physical evidence (e.g., latent prints, DNA, Gunshot Residue), being careful as well not to disturb/contaminate the potential physical evidence that may exist. Document the date and time these steps are performed and note any differences between known good time and any time being displayed by the vehicle systems.

Vehicles may not be synced to a timeserver. The vehicle local time may not be accurate to real time. If possible, document the vehicle's time and, if enabled, time zone.

Each vehicle will be slightly different and require individual methods performed for proper handling. However, general guidelines are often available for classes of vehicles. For example, the following are general guidelines for properly shutting down and preserving the data for most cars and trucks that have original equipment manufacturer [OEM] infotainment/telematic systems installed.

- Turn off the vehicle, disengage the hood latch (if planning on disconnecting the battery), and exit with all key fobs (placing them and any other collected items capable of signal transmission into faraday isolation).
- Close all doors.
- Open the driver's door for 5 seconds.
- Close the driver's door and wait approximately 2 minutes.
- Disconnect battery or place the vehicle into transport mode, if applicable.

To verify that the vehicle was completely shut down, ensure the center stack of the vehicle, as well as the instrument cluster and interior/exterior lights have been off for 30-45 seconds after all doors were closed. Wait 60 seconds after all of the components have shut down before removing power to any of the ECUs.

5.2.1 Car and Truck Preservation Process and Flow Chart

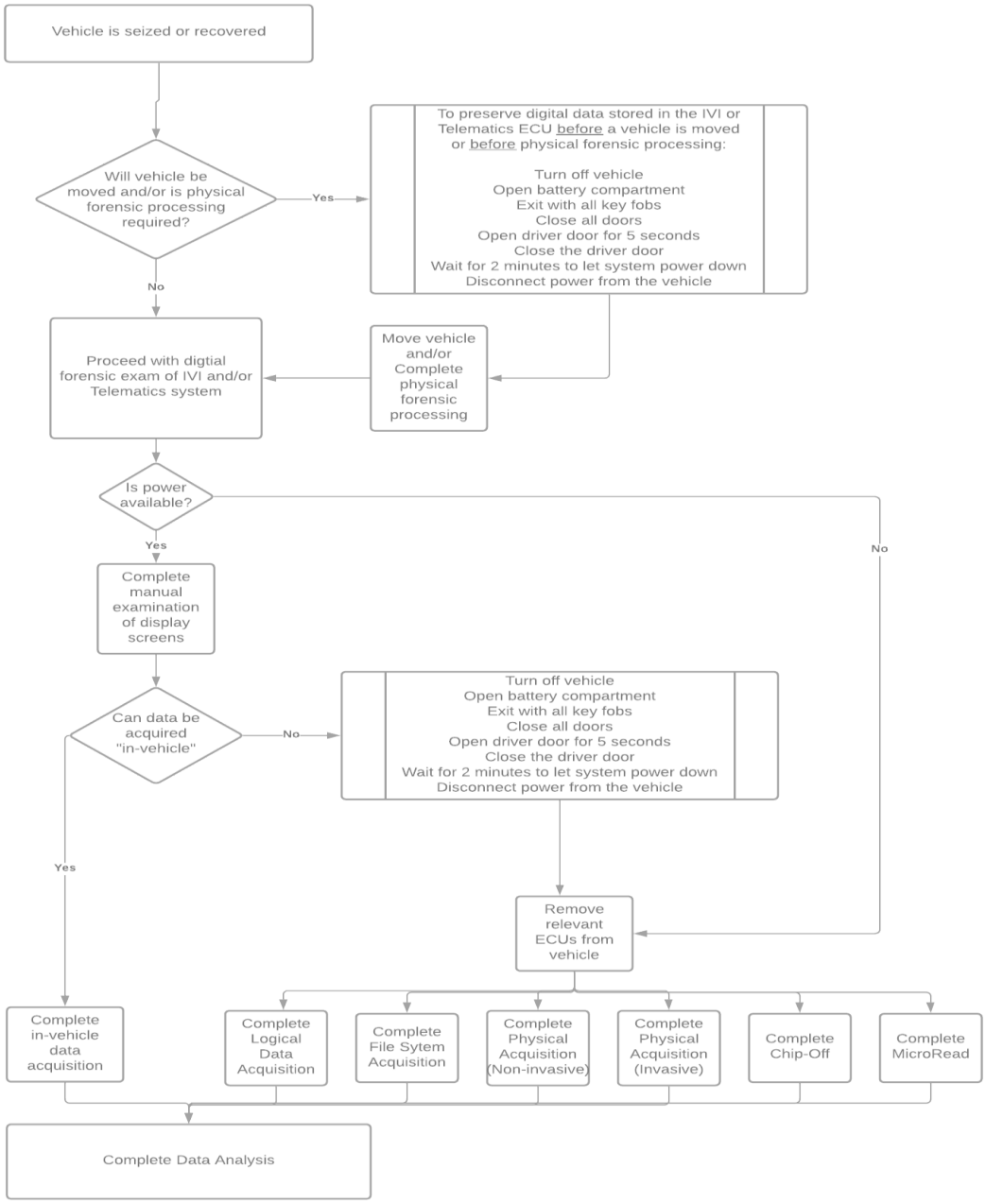

Figure 1. Car and Truck Preservation Process and Flow Chart (Chart Credit: SWGDE)

6. Data Acquisition and Analysis

Infotainment and telematics systems can contain a variety of storage media, including removable media onboard flash memory, and hard drives. Manufacturer's documentation or third party documentation such as device registration organizations or independent researchers can help identify relevant features, functions, and possible data storage locations.

Some systems must still be installed in the vehicle for data acquisition and examination, while some require the systems to first be removed. Data extraction is also not always possible due to limitations in hardware and software availability. In these instances, a visual examination (such as taking pictures with a camera) of any active screen/system may be required. Invasive procedures, such as chip-off may be required. See SWGDE Best Practices for Internet of Things (IoT) Seizure and Analysis, 2016-02-08 SWGDE Best Practices for Chip-Off, and 2017-02-21 SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices for additional applicable information.

6.1 Equipment Preparation

"Equipment" in this section refers to the non-evidentiary hardware and software the examiner utilizes to conduct data acquisition and analysis of the evidence. Equipment and so ftware applications should be validated to ensure proper performance.

Removing the system from the vehicle to acquire the data may require the following:

- Appropriate removal tools (spudgers, drivers, etc.)
- A vehicle network simulator to replicate network traffic for full system functionality
- Adjustable DC power supply with metered variable output for powering the evidence
- Appropriate protective measures/equipment (grounding cables, PPE, etc.)

6.2 Data Analysis

Analysis of data can be conducted using a variety of tools and should be performed in accordance with your organization's best practices.

6.2.1 Artifacts

Data of importance may include but is not limited to:

- Vehicle/System Information\
    - Serial Number
    - Part Number
    - VIN Number(s)
    - Build Number
    - FCCID

- Installed Application Data
  - Weather
  - Traffic
  - Facebook
  - X (Formerly Twitter)
- Navigation Data
  - Tracklogs and Trackpoints
  - Saved Locations
  - Previous Destinations
  - Autopilot logs
  - Active and Inactive Routes
- Device Information
  - Device IDs
  - RFID
  - Calls
  - Contacts
  - SMS
  - Audio
  - Video
  - Images
  - Wi-Fi Access Point Information
- Events
  - Doors Opening/Closing
  - Lights On/Off
  - Bluetooth Connections
  - Wi-Fi Connections
  - USB Connections
  - System Reboots
  - GPS Time Syncs
  - Odometer Readings
  - Gear Indications
- User Data
  - Driver profile
  - Facial recognition logs
  - Voice recognition
  - Alcohol blood content logs

- Embedded Telecommunications Device
  - IMEI
  - ICCID
  - IMSI

7. Access of Paired Devices through Infotainment Systems

Acquisition of data from vehicle infotainment and telematics systems may include accessing and acquiring data of paired devices through iOS CarPlay or Android Auto. A phone that was previously paired with the infotainment system may automatically connect to the infotainment system, through either iOS CarPlay or Android Auto, when the device is within Bluetooth range. This will give access to contacts, messages, call history, and more. The previously paired device may connect when the phone is locked. This is a method for viewing data on a locked phone without needing to know how to unlock the phone.

8. Additional Resources

The listed resources below provide information that may prove helpful to the examiner.

CAN in Automation. "History of CAN technology." *CAN-CiA*, https://www.can-cia.org/can-knowledge/history-of-can-technology. Accessed 15 May 2023.

International Organization for Standardization. *Road Vehicles - Diagnostic Systems – Requirements for Interchange of Digital Information*. ISO 9141:1989, International Organization for Standardization, 1989.

International Organization for Standardization. *Road Vehicles — Controller Area Network (CAN)*. ISO 11898-1:2015, International Organization for Standardization, 2015.

International Organization for Standardization. *Road Vehicles - Interchange of Digital Information on Electrical Connections Between Towing and Towed Vehicles*. ISO 11992-2:2023, International Organization for Standardization, 2023.

Leen, Gabriel, and D. Heffernan. "Expanding automotive electronic systems." Computer, vol. 35, no. 1, 2002, pp. 88-93.

Scientific Working Group on Digital Evidence. *Best Practices for Chip-Off*. SWGDE 15-F-002-1.0, SWGDE, 2016, https://www.swgde.org/15-f-002/.

Scientific Working Group on Digital Evidence. *Best Practices for Internet of Things (IoT) Seizure and Analysis*. SWGDE 23-F-003-1.0, SWGDE, 2023, https://www.swgde.org/23-f-003-draft/.

Scientific Working Group on Digital Evidence. *Best Practices for the Acquisition of Data from Novel Digital Devices*. SWGDE 16-F-003-2.0, 2016, https://www.swgde.org/16-f-003/.

Society of Automotive Engineers. Class B Data Communications Network Interface. SAE J1850_202212, SAE International, 2022.

Society of Automotive Engineers. Recommended Practice for a Serial Control and Communications Vehicle Network. SAE J1939_202306, SAE International, 2023.

9. History

Revision	Issue Date	History
1.0	9/13/2012	Initial draft for public comment.
1.0	2/11/2013	Edit/format for publishing as Approved. (Original title: SWGDE Best Practices for Vehicle Navigation and Infotainment System Examinations).
2.0 DRAFT	1/14/2016	Technical updates performed and significant content changes were made throughout. Retitled as: SWGDE Best Practices for Vehicle Infotainment and Telematics Systems. Voted for release as a Draft for Public Comment.
2.0	2/8/2016	Formatting and technical edit performed for release as a Draft for Public Comment.
2.0	6/9/2016	SWGDE voted to publish as an Approved document.
2.0	6/23/2016	Formatted and posted as an Approved document.
3.0 DRAFT	1/14/2021	Draft created to add new sections and updated content. Released for public comment.
3.0	1/13/2022	Released for publication.
3.1 DRAFT	9/21/2023	Draft created to add new sections and updated content.
3.2 DRAFT	5/15/2024	Formatting for all of the document; added section 7.
3.2	6/12/2024	SWGDE voted to approve as Draft for Public Comment. Formatted for release as Draft for Public Comment.
3.2	11/6/2024	SWGDE approved as a Final Document.