Scientific Working Group on Digital Evidence

SWGDE Best Practices for Vehicle Infotainment and Telematics Systems

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall 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; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

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 the SWGDE cover page containing the disclaimer.
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 create date) of the document and mention 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 forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) 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 change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents 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.

SWGDE Best Practices for Vehicle Infotainment and Telematics Systems

Table of Contents

1. Purpose

The purpose of this document is to describe best practices for acquiring the data contained within infotainment and telematics systems installed in motor vehicles. The intended audience is first responders and/or others involved in the collection of digital data from vehicles.

2. Scope

This document provides basic information on the logical and physical acquisition of infotainment and telematics systems installed by the original equipment manufacturer (OEM) as a standard option or additional option for a specific trim level.

3. Limitations

This document was prepared with the resources available at the time of publication. This document is not intended as a step-by-step guide for conducting data recovery for vehicle systems nor should it be construed as legal advice.

4. Evidence Collection and Processing

Infotainment and telematics systems present unique challenges to law enforcement due to differences in hardware designs and manufacturers, limited information on the underlying software and proprietary operating systems, encrypted media associated with Digital Rights Management (DRM), and rapid changes in technology. Acquisition options may be limited by hardware and software available to facilitate the data extraction. A visual examination of an active screen/system may be required if other techniques are unsuccessful.

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 destruction. A modern day vehicle will contain multiple computers and/or networks and therefore the examiner should take reasonable measures to isolate the vehicle from wireless networks (e.g. wifi, cellular, bluetooth, etc.).

4.1 Evidence Preservation

Electronic Control Units (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 the power up procedure. Minimizing the number and duration of power cycles helps preserve volatile data stored on ECUs.

Processing a vehicle for physical evidence may cause additional power cycles resulting in the loss of relevant volatile data from the ECUs. To mitigate this risk, document the on-screen data and properly shut down the vehicle to allow the ECUs to correctly power down *before processing physical evidence (e.g. latent prints, DNA, GSR, etc.)*.

The following are general guidelines for properly shutting down a vehicle to preserve evidence. Document the date and time these steps are performed.

- Turn off the vehicle and exit with all key fobs
- Close all doors
- Open the driver's door for 5 secs
- Close the driver's door and wait ~ 2 minutes.
- Disconnect vehicle power (e.g. disconnect battery or place the vehicle into transport mode)

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.

4.2 Evidence Handling

Review legal authority prior to handling and collecting evidence, ensuring any restrictions are noted. If necessary during the collection phase, obtain additional authority for evidence outside the original scope.

Infotainment and telematics systems may consist of separate ECUs located in different locations within a vehicle or may be a single integrated ECU that has dual functionality. General guidelines for working with vehicles associated with an investigation include:

- Handle evidence according to agency policy and maintain a chain of custody.
- Preserve the state of the ECUs prior to the physical processing of a vehicle as described in section 4.1.
- If physical forensic processing of a vehicle (DNA, latent prints, etc.) is required, 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.
- Biological contaminants and physical destruction provide unique challenges to the recovery of data. Use universal precautions to protect the health and safety of the examiner.
- Infotainment and/or telematics systems may have active external connections (e.g cellular, WiFi, or Bluetooth). Isolate the vehicle from connecting to external networks when possible; e.g., disconnect antennas or cellular modems, remove SIM cards, etc..

4.3 Equipment Preparation

"Equipment" in this section refers to the non-evidentiary hardware and software the examiner utilizes to conduct data extraction and analysis of the evidence. Equipment and software applications should be validated[1] to ensure proper performance.

Removing the system from the vehicle to acquire the data in a lab environment may require the following:

- Vehicle network simulator to replicate vehicle network traffic to fully power on the system.
- Adjustable DC power supply with metered variable output - Used to power the evidence
- Appropriate cables and adapters

4.4 Data Acquisition

Infotainment and telematics systems can contain a variety of storage media, including removable SD cards, onboard flash memory, and hard drives. Review the manufacturer's documentation to identify relevant features, functions, and possible data storage locations.

Data may be acquired from vehicle systems either "in car" or "on the bench". The methods used depend on the tools available to extract the data and the level of analysis required by the investigation. Higher levels require a more comprehensive examination, additional skills, and may not be applicable or possible for every device or situation. The following represents the potential levels of acquisition that may apply[2]:

1. **Manual** – A process that involves the manual operation of the system to display and document data present in the device's internal memory.
2. **Logical** – A process that extracts a portion of the device's memory.
3. **File System** - A process that provides access to the file system.
4. **Physical (Non-Invasive)** – A process that provides physical acquisition of a device's data without requiring opening the case of the device.
5. **Physical (Invasive)** – A process that provides physical acquisition of a device's data requiring disassembly of the device providing access to the circuit board. (e.g., JTAG)
6. **Chip-Off** – A process that involves the removal and reading of a memory chip to conduct analysis.
7. **MicroRead** – A process that involves the use of a high-power microscope to provide a physical view of memory cells.

[1] The validation process is discussed in the document titled "*SWGDE Recommended Guidelines for Validation Testing*."

[2] See the discussion of the Mobile Forensics Pyramid in the document *SWGDE Best Practices for Mobile Phone Forensics*

Handle and image media associated with the infotainment or telematics system in a forensically sound manner.

4.5 Data Analysis

Analysis of data can be conducted using a variety of validated tools. Data of importance may include but is not limited to:

Vehicle/System Information

- Serial Number
- Part Number
- VIN Number(s)
- Build Number

Installed Application Data

- Weather
- Traffic
- Facebook
- Twitter

Connected Devices

- Phones
- Media Players
- USB Drives
- SD Cards
- Wireless Access Points Logs

Navigation Data

- Tracklogs and Trackpoints
- Saved Locations
- Previous Destinations
- Active and Inactive Routes

Device Information

- Device IDs
- Calls
- Contacts
- SMS
- Audio
- Video
- Images
- WiFi Access Point Information

Events

- Doors Opening/Closing
- Lights On/Off
- Bluetooth Connections
- Wifi Connections
- USB Connections
- System Reboots
- GPS Time Syncs
- Odometer Readings
- Gear Indications

5. Reference Sites and Publications

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

- **GPSForensics.org** – http://www.GPSForensics.org
- **CAN Bus Information** - http://en.wikipedia.org/wiki/CAN_bus

- **Automotive Buses -** http://www.interfacebus.com/Design_Connector_Automotive.html
- **SAE Standards: J1850 and J1939**
- **ISO Standards: 11992 and 9141**

6. Proposed Definitions for the SWGDE Glossary

Electronic Control Unit (ECU) – A generic term for any embedded system that controls one or more of the electrical system or subsystems in a motor vehicle.

In-vehicle infotainment (IVI) – An integrated electronic control unit installed in vehicles that delivers content for entertainment and informational purposes.

Telematics – An external wireless connection to and from a vehicle for data and information transfer.

SWGDE Best Practices for Vehicle Infotainment and Telematics Systems

History

Revision	Issue Date	Section	History
V1 Draft	09/13/2012	All	Initial draft for public comment.
V1 Final	02/11/2013	All	Edit/format for publishing as Approved. (Original title: SWGDE Best Practices for Vehicle Navigation and Infotainment System Examinations)
2.0	01/14/2016	Title; All	Technical update preformed 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	02/08/2016	All	Formatting and technical edit performed for release as a Draft for Public Comment.
2.0	06/09/2016	--	SWGDE voted to publish as an Approved document.
2.0	06/23/2016	--	Formatted and posted as an Approved document.