C39   A Discussion of ASTM E2493-07, a New Standard Guide for the Collection of Non-Volatile Memory Data in Evidentiary Vehicle Electronic Control Units

William Rosenbluth, MSEE, Automotive Systems Analysis, 12015 Canter Lane, Reston, VA 20191*

After attending this presentation, and seeing procedural examples as presented, the attendee will learn several methods for conducting a controlled retrieval of the data in a subject vehicle electronic control unit (ECU). These methods provide an accepted and documented procedure which incorporates a protocol to retrieve EDR data with the highest assurance of not changing or disturbing that data, either by erasure or overwriting.

This presentation will impact the forensic community by providing a new and mutually accepted reference methodology by which crash event data can be retrieved from an evidentiary Electronic Control Unit (ECU). An investigator following such a reference methodology can more effectively face procedural inquiry and challenges common to such activities.

Electronic crash event data retrieval has become an increasingly important aspect of vehicle accident investigation. ASTM E2493-07 describes an acceptable methodology for the examination and interrogation of non-volatile memory data in evidentiary vehicle Electronic Control Units (ECUs) that are identified as having information related to such accident events. This presentation illustrates the methods and considerations implied by that guide by discussing the guide instructions and then illustrating those instructions with selected examples.

The retrieval of electronic crash data is commonly referred to as a *down- load* of information from the subject device, however, that term is not strictly accurate. Strictly speaking, SAE J2190:4.23 identifies that the process of requesting the transfer of data from an on-vehicle ECU to an external ECU (Mode $35) is called an upload request, whereas the process of requesting the transfer of data from an external ECU to an on-vehicle ECU to an (Mode $34) is called a download request. To avoid confusion, the term *data retrieval* is used in ASTM 2493-07 and herein.

ASTM E2493-07 was developed by participants from industry, government and private sectors, and has been approved and published by ASTM, April 2007. That Standard Guide describes acceptable methodologies and protocols for the examination and retrieval of non-volatile memory data in evidentiary vehicle electronic control units (ECUs) that may have been involved in an event or incident. As such, these methodologies and protocols can be considered to be operational benchmarks that are expected to be included in future standard forensic investigation practice.

ASTM E2493-07 presupposes that the data object (ECU and the data therein) is an evidentiary item. However per ASTM E860, as referenced in that guide, investigators dealing with units that are not yet evidentiary, but are reasonably expected to be involved in litigation, are well advised to be cognizant of ASTM E2493-07 as well.

The accepted objective of ASTM 2493-07 is to provide *a forensically neutral* data retrieval process. A *forensically neutral* interrogation is one that will neither add or subtract diagnostic trouble codes (DTCs) or crash data information from any ECU under interrogation, and more specifically, from the data at issue within that ECU. This applies to in-vehicle and benchtop interrogation processes, including ECUs interrogated via direct umbilicals while still mounted in a vehicle. To be *forensically neutral*, benchtop or direct umbilical units must include provisions for actuator electrical loads (squib, solenoid, etc.), sensor electrical loads, MIL electrical loads and expected network communications as seen in situ, so that any ECU under- going such a data retrieval will see only its original or equivalent in situ operating environment.

Certain commonly used commercial interrogating tools are not *forensically neutral* when used in a benchtop or direct umbilical mode to interrogate SRS ECUs (i.e., a direct connection to the SRS ECU). In that mode, certain external fault codes will be added or re-detected. If the data of interest is not changed (e.g., crash data parameters), then a non- forensically-neutral retrieval may be acceptable. However, if certain DTC's are of interest, or ECU sensor performance is at question, then a non- forensically-neutral interrogation may not be acceptable. Forensically neutral data retrievals can be accomplished by correct "load boxes", other test equipment, laboratory breadboards and/or the use of an exemplar vehicle. In general, it is expected that the test conductor will have a proper test fixture, and a proper exemplar component to demonstrate that his/her test bed is *forensically neutral*.

A general protocol for evidentiary electronic data retrieval involves baselining (qualifying) the data retrieval tool using an exemplar ECU, and then, when qualified, using that tool to retrieve data from the subject evidentiary ECU. That general protocol can be shortened when the investi- gator uses a commercial data retrieval tool to perform such a retrieval, however, even with such tools there is jeopardy that careless application of such tools can alter evidentiary data. Examples of *forensically-neutral* and *non-forensically-neutral* data retrievals are shown and discussed.

When a proprietary tool is used for data retrievals, the base lining procedure is very important.

In such a case, the test conductor should perform two test series, with two devices under test (DUT). The first series should involve an exemplar device to provide a baseline verification of the test fixture, and the second series should involve the subject ECU. Examples of data retrieval tools used in *forensically-neutral* and *non-forensically-neutral* data retrievals are shown and explained. The figures show a recent example of a baselined on-vehicle data retrieval.
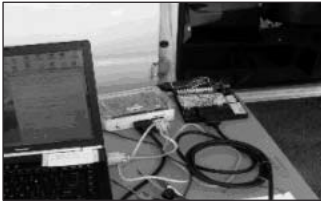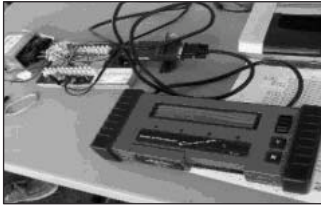
Figures: Sequence of photos for on-vehicle data retrieval using a proprietary retrieval tool. This sequence shows the baselining process, followed by the actual evidentiary data retrieval and translation.

   The last consideration in data retrieval activities is the preservation of electronic data according to new Federal Rules 16, 26, 33, 34, 37, and 45 (1Dec06). With respect to proprietary data retrievals, of special importance is Rule 26(a)(1)(B), identifying that a party must disclose its electronically stored information as well as methods and documents that it may use to sup- port its claims or its defenses. This rule, if applied unilaterally can prove burdensome and crippling. However, if it is anticipated, and then applied in an even handed manner, it can be made livable. An illustration of one method of handling this situation is shown and discussed.

ASTM E2493-07, EDR Data Retrieval, Forensic Neutrality