**Protocols for the Recovery, Maintenance and Presentation of Motor Vehicle Event Data Recorder Evidence (12/05)**

By James O. Harris, Harris Technical Services, Traffic Accident Reconstructionists
With contributions by William C. Wilson, Investigative Mechanics, LLC
Edited by Joseph E. Badger

## Purpose

The recovery and presentation of electronic data to a court requires procedures that assure the information presented is an accurate record of the data stored on the computer chip and that the data was not deliberately altered or lost due to mishandling. This protocol has been devised to provide a means of being reasonably certain that data held as being obtained a motor vehicle Event Data Recorder (EDR) is an accurate representation, that data access and recovery was authorized and that recovered data is afforded protection from an inadvertent release of an individual's private information.

These procedures also provide that documentation must be such that in the absence of the originator another competent person can evaluate what was done and interpret the data.

## Definitions

The following terms are defined in Digital Evidence, Standards and Principles[2].

Original Digital Evidence: Physical items and the data objects associated with such items at the time of acquisition or seizure.

Duplicate Digital Evidence: An accurate digital reproduction of all data objects contained on an original physical item.

Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

## Preparatory Activities

The acquisition of digital evidence begins when information and/or physical items are collected or stored for examination. The term "evidence" implies that the collector of evidence is recognized by the courts.

In every instance, the authority to remove an EDR module, or access the data contained in a module, should be determined before any efforts begin. For a criminal investigation, a search warrant or the vehicle owner's consent may be required absent a determination by legal counsel that a search authorization is not necessary given the circumstances[3].

For a private sector crash reconstruction, permission should be obtained from an appropriate individual or authority, i.e., the owner of the vehicle or the attorney for the vehicle owner. This is consistent with the procedures of the National Highway Traffic Safety Administration[4] (NHTSA):

> "It is NHTSA's position that the owner of the subject vehicle owns the data from the EDR. In order to gain access to the data, NHTSA must obtain a release for the data from the owner of the vehicle."

In the last 25 years, all fifty states and the federal government have enacted criminal laws that prohibit unauthorized access to computers[5]. For example, Florida State Statutes[6] provides the following:

> 815.03 Definitions. -- As used in this chapter, unless the context clearly indicates otherwise:
>
> (1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.
>
> (2) "Computer" means an internally programmed, automatic device that performs data processing.
>
> (7) "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files.
>
> (8) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, in storage media or stored in the memory of the computer, or in transit or presented on a display device.
>
> 815.06 Offenses against computer users. --
>
> (1) Whoever willfully, knowingly, and without authorization:
>
> (a) Accesses or causes to be accessed any computer, computer system, or computer network;
>
> commits an offense against computer users.

By 2005, California, North Dakota and Arkansas had enacted laws regarding access to data stored on EDRs. Several other states had pending legislation. The technician should be familiar with any applicable state and local laws before proceeding to retrieve a module, accessing or releasing an EDR data file.

Before attempting to access the EDR, inspect and photograph the vehicle. This will record the condition of the vehicle as found. Note those details that will be pertinent to data interpretation such as wheel and tire size, air bags deployed or not, anti-lock or standard brakes, drive wheels, transmission type, cruise control, etc.

The ignition to the vehicle should not be engaged during the inspection as this could result in an ignition cycle being recorded in the EDR that is not related to the accident or data recovery effort. Once the EDR module is exposed, it should be photographed in place.

Methodologies

There are four field methods to retrieve data from a module. Laboratory methods, which may involve removing computer chips from the module, are not addressed in this document.

1. Through the On Board Diagnostic connection (OBD II).
2. Direct connection to the module while it remains in the vehicle.
3. Direct connection to the module outside of the vehicle (bench download).
4. Removal of the module from the accident vehicle and connecting it to the wiring harness of an exemplar vehicle with the download through the OBD II connection.

For any data recovery, a source of reliable power is required. If there is any question as to the voltage levels at the module interface, the use of an outside power source is recommended. Voltage levels can be monitored using a voltage meter.

On some models of EDR, each time the module is energized or the vehicle's ignition is activated, an ignition cycle is recorded. To avoid the inadvertent recording of an ignition cycle, first connect all required data cables between the CDR Tool, computer and the EDR module or OBD II port. Have the computer ready to commence data recovery when the last power connection, the one to the CDR Tool or vehicle electrical system, is completed.

Some computer operating systems add a date and time stamp to the file that indicates the date and time a file was created, saved, modified or last accessed. The time and date is obtained from the computer operating system clock. This clock should be checked for reasonable accuracy before the download is accomplished.

Access through the OBD II is often the easiest method requiring no direct access to the module. With this method, the data is routed through the vehicle's wiring system. Even with safeguards in the data recovery software and hardware, there is a possibility of data loss or degradation due to failures within a damaged vehicle's signaling systems.

With the OBD II method, the module is not removed from the vehicle. Access through the OBD II is recommended when feasible. If the OBD II download file is incomplete, or contains suspected errors, then a download should be attempted by direct connection to the EDR module.

Insure the ignition is in the off position before connecting the CDR Tool; cutting or disconnecting any EDR cables. Disabling the vehicle's electrical system, by disconnecting or cutting the battery cables, may be desirable to prevent energizing of the EDR module and the inadvertent creation or overwriting of files at a later date.

In some vehicles, energizing an EDR module while it is not connected to an intact vehicle electronics system can result in the alteration of diagnostic trouble codes that existed at the time of the accident. In instances where these trouble codes may be at issue, the codes can be first read using a vehicle manufacturer approved scan tool and software. This information can then be compared to or used in conjunction with the data obtained directly from the EDR module using the CDR Tool.

Downloading the EDR with a direct connection while the module is still secured to the vehicle prevents handling of the module beyond the minimum necessary to complete the download. If removal of the EDR is required to perform the download, the data retrieval should be accomplished as soon as practical once the module has been removed.

Electrostatic charges can damage electronic components. The technician should be grounded when handling the module, or the module insulated, to prevent a possible static discharge. To reduce the possibility of a static charge altering or erasing data within the module during handling, plastic tape can be placed over the module connection port

The removal of the EDR module should be with the least destructive means to the remainder of the vehicle. Insure there is no power to the module before attempting to disconnect any cables or removing securing bolts. Disconnection of the data cable should be at the module connection. If the connection will not release, cut the vehicle data cable several inches beyond the module connection. The data cable consists of a number of individual wires. The outer sheath of the cable bundle should be cut and peeled away from the wires and each wire within the sheath cut individually to avoid a cross-connection.

Avoid handling the module while it is energized as this can result in the inadvertent creation or alteration of a data file. Non-deployment files, that are not associated with a deployment or deployment level event, can be overwritten or erased by the EDR program.

The module must be maintained on a stable surface while energized.

Utilizing an exemplar vehicle as an OBD II platform for an EDR module that was removed from an accident vehicle presents unique hazards to the data integrity. This method should only be used with the technical assistance of the vehicle manufacturer.

In all methods, once all downloads have been completed, the power supply to the CDR Tool should be removed first. The EDR module should be left on a stable surface, or undisturbed if in the vehicle, for ten minutes to allow any residual capacitor power that may have built up during the period the unit was energized to fully dissipate.

Securing Recovered Data

Recovery and handling actions are based upon the fundamental procedures contained in the U.S. Dept. of Justice guide for searching and seizing digital evidence[7].

The initial download must be saved to a removable computer data disk[8]. This disk is marked with the vehicle identification number (VIN) or reference case file number. Any number of additional disks of this download can be prepared at the same time without creating additional ignition cycles. The first disk, a reference disk, should be marked as above and the storage media set to prevent any accidental overwriting or alteration of the data if possible.

As a minimum, two disks of the first data access should be saved. The reference disk is secured to prevent access to the disk without leaving readily visible evidence, such as a tamper-resistant evidence container. This may be the same container used to store the module following the download. The outside of the container is marked with pertinent data to identify the contents. Subsequent disks can be used for routine uses such as to create reports and exhibits. Storing the file on the internal drive of the computer used to complete the download may substitute for a second data disk.

The reference disk is not to be accessed except under conditions that require comparison of the data currently in the module to the data preserved on the reference disk.

Upon termination of all data recovery efforts the EDR module is sealed in a tamper-resistant evidence container. The module may be marked with the VIN using a felt-tip marker or the serial numbers on the module noted. The outside of the container should be marked to identify the contents.

As a courtesy to others, leave a card with contact information for the responsible person or organization for the removal of the module in the same place as the module was located.

The U.S. Dept. of Justice has published Proposed Standards for the Exchange of Digital Evidence[9]. Standards and Criteria 1.6:

> "All activity relating to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony."

If evidence conatiners must be opened, the actions must be documented with the names of all persons that gained access to the module, the reason for access and activity details. Following an interim access, the module and reference disk in the original evidence container should be placed in new containers.

The EDR programs utilize a checksum (CRC) process to assure data integrity. The design and construction of the EDR modules makes the deliberate alteration of deployment and deployment level files unlikely but the possibility cannot be entirely dismissed. From a NHTSA report[10] on EDRs:

> "When 150 msec. have elapsed from algorithm enable, the data stored in RAM [Random Access Memory] are transferred to the EEPROM [Electrically Erasable Programmable Read Only Memory]. It requires about 0.7 sec. to permanently record all information. Once a deployment record is written the data are frozen in EEPROM and cannot be erased, altered, or cleared by service or crash investigation personnel."

A sealed evidence container, containing the module and reference disk with appropriate records, is evidence of the integrity of the data.

The release of data obtained from an EDR presents of number of privacy concerns. EDR data is generally considered the property of the vehicle owner[11]. EDR data should be considered confidential with releases only to those determined to have a valid requirement and legal authority to obtain the information.

It is acceptable to release the data, for further technical analysis, by removing the last six digits of the VIN so the vehicle can only be identified by year, make and model. A public release of the data file should be with the same portion of the VIN removed only after all proceedings have concluded and the material is no longer evidentiary in nature. Vehicle photos that accompany the data file should have the VIN and license plate obscured.

Data Recovery Records

A detailed record of the data recovery effort must be completed. This information includes the date, time and location of the data recovery, the name of the person responsible for the effort, VIN, CDR Tool software version number and serial number and the EDR module serial number when available. Include the CDR Tool data cable designation and computer operating system. Notations should include the method of download and power source, i.e. vehicle battery, exterior 12V power pack, 12V power from another vehicle, 110V line current, OBD II or direct module connection.

A record of the ignition cycles at investigation, if available, should be included in the field notes. Since the ignition cycles at investigation increase by one each time the module is powered, energize the unit the minimum number of times necessary. Keep a record as to the number of ignition cycles during the data recovery effort. Note the reason(s) for more than one and note the number of ignition cycles when the module is powered down immediately prior to storage. Some EDR models do not report ignition cycles at investigation.

Data Presentation

Federal Rule of Evidence 702, and it's variations adopted by most states, defines the admissibility of expert testimony in the following manner:

> "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise" (Melton, Petrila, Poythress, & Slobogin, 1997, p.16)

Since 1923, Frye vs. U.S., 293 F. 1013, D.C. Ct. App. 1923, has served as the standard for determining whether an expert's testimony would assist the trier of fact. Frye requires that expert testimony be supported by scientific principles or evidence generally accepted by the relevant scientific or professional community. Frye rulings traditionally rely on peer review, particularly the availability of peer-reviewed articles, to assess general acceptance.

The U.S. Supreme Court's opinions in Daubert vs. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 113 S.Ct. 2876; 1993, as enhanced by the subsequent decision in Kumho Tire Company, Ltd., vs. Patrick Carmichael, 526 U.S. 137; 1999, requires that all expert testimony meet general tests of reliability and relevancy.

Surviving a Daubert or Frye hearing does not prevent further challenges to the validity of the data presented on other grounds, such as chain of custody issues.

The rules of evidence vary among jurisdictions. In some cases, if the original data is available, it will be accepted as superior to any copy. Since a file retrieved from a computer disk is necessarily a copy or duplicate of the original digital data, still contained within the module, a live,

direct download and presentation in court may be necessary. The reference disk may also be considered to be an equally valid presentation of the data contained within the module as long as the integrity of the reference disk can be confirmed.

A court's agreement to the introduction of EDR evidence is not binding on the jury for consideration. In deliberation, the jury may accept or disregard, in whole or in part, any expert witness testimony. EDR data recovery and interpretation is within the province of an expert witness. A jury's disregard of expert testimony is generally insufficient to overturn a verdict on appeal

The CDR Tool data computer display and report print-out is a low resolution computer generated image. As with any digital image, it can be altered. With a scanner and graphics editing program, an EDR data print-out or screen display could have the data charts, tables and text changed. Absent an original data source, it would be difficult or impossible to detect such alterations. With the original EDR module or reference disk, in a condition known to be same as when the module was recovered and data first acquired for subsequent comparison, an altered image can be readily identified.

When creating trial exhibits from the EDR data record, care must used so as not to alter the relevant information. Changing the background, foreground or text colors to improve contrast are effective and acceptable as long as the data is not altered.

For the presentation of the data at trial or other proceeding, the original module, in the sealed evidence container, should be available.

For a live demonstration, before opening the sealed evidence container, all other required equipment should be set-up and operational. The opening of the sealed evidence container is to be observed by all interested parties. Standard procedures and safeguards for a bench download should be followed.

The EDR should be connected to the computer with no external data disks available. Remove all other EDR files from the computer's internal drives. Note the ignition cycles at the time of the demonstration and compare this with the data recorded at the time of the original download, if reported. This is further evidence that the EDR had not been accessed since the original data recovery effort.

Once the demonstration is completed, save the download conducted for the court to a separate data disk marked appropriately. This disk may be needed in the event of an appeal where this would be the only record of the evidence shown to the jury.

Once the proceedings are over, the disposal of the EDR and data disks are dictated by the circumstances. In some cases, trial evidence must be retained by the court for extended periods.

Summary

These procedures do not provide any assurance that the data contained in the EDR is relevant to the crash event at issue. This falls to the interpretation of the information and comparison of the data to the physical evidence.

It is not possible to have standard procedures that can provide for every conceivable situation. This protocol provides guidance; it is not a replacement for good judgment, compensatory measures or alternative procedures where appropriate. Local evidence handling procedures must be accomodated. Each recovery of EDR evidence must be undertaken on a case-by-case basis with due consideration for the existing circumstances.

As EDR technology advances and the rules of evidence may change, these procedures may not be applicable in whole or in part.

This protocol is advisory in nature, providing a process for a verifiable chain of custody and access control over the original data source and the release of EDR data records. It provides safeguards to minimize the alteration, corruption or loss of data. These procedures can help to insure that the portrayal is an accurate representation of the data contained in the EDR.

Notes -

1. “EDR” refers to a vehicle component that stores crash data in an electronic form as defined by the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) in IEEE P1616 Motor Vehicle Event Data Recorders (MVEDR).

An Event Data Recorder is a sub-component. In GM vehicles, it is part of the Sensing and Diagnostic Module (SDM). This module is generally labeled as the “Air Bag Sensor”. In Ford vehicles, it is a part of the Restraint Control Module (RCM).

2. Digital Evidence, Standards and Principles, Scientific Working Group on Digital Evidence (SWGDE), Oct. 1999, Forensic Science Communications, U.S. Dept. of Justice, Federal Bureau of Investigation, Apr. 2000.

3. It is the policy of Harris Technical Services that EDR data and modules will only be retrieved when the following conditions are met:

a. With a court’s authorization, such as a search warrant or order or

b. With the consent of the legal representative of the current vehicle or property owner and

c. After we have determined such consent or order is in compliance with all applicable local, state and federal laws and

d. Where the authorization or consent specifically includes the physical retrieval of the module and access to the data within the module.

4. Event Data Recorders Summary of Findings, NHTSA EDR Working Group, 8.3.1 Position of the National Highway Traffic Safety Administration.

5. Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Satutes, O. R. Kerr, George Washington University Law School, Public Law and Legal Theory Working Paper No. 065, May 2003.

a. 18USC§1030 - Fraud and related activity in connection with computers.

6. Florida State Statutes, Title XLVI, Crimes, Chapter 815, Computer Related Crimes, 2002.

7. U.S. Dept. of Justice, Criminal Division, Office of Professional Development and Training, Federal Guidelines for Searching and Seizing Computers, Jul. 1994, Bureau of National Affairs, Criminal Justice Reporter, Vol. 56, No. 12, Dec. 21, 1994.

8. “Computer data disk” refers to any removable computer data storage medium to which digital data can be written.

9. Proposed Standards for the Exchange of Digital Evidence, Forensic Science Communications, U.S. Dept. of Justice, Federal Bureau of Investigation, Apr. 2000.

10. Recording Automotive Crash Event Data, A. Chidester, NHTSA, J. Hinch, NHTSA, T. C. Mercer, General Motors Corp. and K. S. Schultz, General Motors Corp., International Symposium on Transportation Recorders, 1999, Arlington, VA.

11. Event Data Recorders Summary of Findings, NHTSA EDR Working Group, 8.0, Privacy and Legal Issues.

Chief Supply, Corp., Eugene, Oregon
Phone: 541-342-4624/800-624-4338
Internet: www.chiefsupply.com
Tamper resistant evidence bag, 9” x 12”, clear plastic, #BD3001-1
Tamper resistant evidence bag, 6” x 8”, clear plastic, #BD3002
Tamper resistant evidence tape, #0440

CDR Tool is a registered trademark of Vetronix Corp.
GM is a registered trademark of General Motors Corp.
Ford is a registered trademark of Ford Motor Co.

© 2003 Harris Technical Services, Traffic Accident Reconstructionists. This document may be copied and distributed as long as the material and credits are not altered.

As the recommended procedures may be changed due to advances in technology and the law, please contact Harris Technical Services or visit our web site for the most current version.

Harris Technical Services
Traffic Accident Reconstructionists
2338 S.W. Scodella Terrace
Port St. Lucie, FL 34953
Phone: 800-486-2142
Phone: 772-336-2279
Fax: 772-785-6095
Internet: www.harristechnical.com