This report is intended to provide state and local law enforcement with recommended standards for Forensic Data Recovery Education and Training.

Recommended Standards for:

Forensic Data Recovery Education and Training

Great Basin Data Recovery and California Data Recovery

May 2012

Mailing:
4790 Caughlin Pkwy #323
Reno, Nevada 89519

Disclaimer: This is a model policy was designed to provide a guide to writing a policy related to forensic data recovery. This model policy should be reviewed and revised based on your local legal requirements. Implementation of any of this model policy should be done so only after legal review by your agency attorney. Additionally, your policy prior to implementation will need to conform to any national or local laws, labor agreements and existing policy within the agency.

This project was supported by Award No. 2010-MU-MU-K021 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect those of the Department of Justice.

Recommended Standards for Forensic Data Recovery Education and Training

Pre-Training Prerequisites

What an examiner needs to understand prior to electing to receive training in this area.

This is an advanced field of interest and is not an area intended for individuals without a minimum level of training and experience in the field of digital forensics. This minimum level of training should include:

1) Digital evidence handling procedures
2) Standard Operating procedures for Digital Evidence examinations
3) Operating System Analysis
4) Proficient with the concepts of hard drive imaging and the tools to perform imaging.

Forensic Data Recovery Examiner Standards and Training

There are two areas of knowledge and education that each examiner must meet to qualify as understanding Forensic Data Recovery techniques. They are:

Knowledge of Processes: The examiner will have received training designed to provide the examiner with an understanding of Forensic Data Recovery evidence procedures.

Skills and Techniques: The examiner will have received training designed to provide the examiner with the ability to competently use specific tools and along with the procedures to effectively accomplish Forensic Data Recovery.

These two areas are further broken down into learning domains with specific sub-categories of learning within the specific domain.

Knowledge of Processes:

These domains cover the knowledge unique to Forensic Data Recovery (FDR). A qualified FDR examiner should understand the issues related to the domain and the specifics of the sub-category:

Domain and Description	Domain Sub-Category
Evidentiary Issues This domain covers evidence preservation and rules of evidence for court admissibility.	a) Evidence handling (to preserve integrity of evidence) b) Chain of custody
Preparation This domain covers how to prepare for forensic data recovery examinations.	a) Planning for forensic data recovery from a non-functioning hard disk drive
Law & Ethics This domain covers ethical implications of forensic data recovery in relation to the field and roles and duties of expert witnesses, digital forensic laws, and laws governing forensic data recovery procedure.	a) Ethics of forensic data recovery b) Court testimony c) Law related to forensic data recovery d) Role of an expert witness e) Forensic data recovery procedures
Quality Assurance, Control, and Management This domain covers standards and controls, certification, and quality in relation to the field of forensic data recovery.	a) Safety issues · Electrical and fire safety b) "Best Practices" (i.e., technical procedures). c) Standard Operating Procedures (SOP's). d) Demonstration of competency (written or practical exam)
Documentation & Findings This domain covers forensic data recovery report writing and how to provide expert testimony.	a) Diagnosing hard drive failures b) Technical writing and note taking skills c) Documenting the forensic data recovery process d) Completing the forensic data recovery report
Hard Disk Drive Mechanics This domain covers all aspect of how hard disk drives function.	a) PCB Design b) PCB ROM/RAM Basics c) Firmware basics d) Head Assembly mechanics e) Identifying donor drives
Forensic Data Recovery Process This domain covers all aspect of the forensic data recovery process	a) Maintain data integrity a. Preventing data modification is preferred but some changes may become necessary. All modifications to data should be technically and scientifically sound and thoroughly documented. b) General forensic principles and practices

Skills and Techniques:

These domains cover the skills and techniques unique to forensic data recovery. An examiner should understand the issues related to the domain and the specifics of the sub-category:

Domain	Domain Sub-Category
Hardware Tools This domain covers the understanding and use of hardware specific to forensic data recovery.	a) Hardware tools specific to forensic data recovery b) Use of tools for media acquisition c) Clean Environment tools d) Head and Platter replacement tools
Software Tools This domain covers the understanding and use of software specific to forensic data recovery.	a) Software tools specific to forensic data recovery b) Use of tools for media acquisition c) Tools for logical recovery
Basics of soldering This domain covers the techniques of soldering and its use in forensic data recovery.	a) Use of a soldering iron b) Using a hot air rework station c) Removing and replacing wire mount chips d) Removing and replacing Surface Mount chips
Repairing Printed Circuit Boards This domain covers the techniques of repairing printed circuit boards from hard disk drives.	a) Areas of common failure b) Identifying electrical problems c) Removing chips from the PCB d) Using a digital Multimeter to measure chip resistance
Repairing Firmware This domain covers the techniques of firmware repair unique to hard disk drives.	a) Hardware tools specific to firmware recovery b) Use of tools for firmware acquisition c) Drive specific knowledge of firmware repair
Head Assembly replacement This domain covers the techniques for removing and replacing head assemblies.	a) Tools required for replacing head assemblies b) Techniques required for head assembly replacement
Platter removal This domain covers the techniques for removing hard disk drive platters.	a) Tools required platter removal b) Techniques required for platter removal

On the Job Training

Experience is a critical training tool. Examiners who train/intern under a competent practitioner (if available) can gain valuable experience, knowledge and improved skills.

Continuing Education

Continuing education in a new field may be difficult. Examiners should attempt to obtain annual education from training conferences, trade shows, professional organizational

memberships, professional publications, current literature and other specialized courses. This training should address updates and the use of new technologies as it relates Forensic Data Recovery.

Competency Testing

Competency testing can be conducted either at the end of training or in a concurrent format throughout the course of training. At any point that a Digital Forensic examiner learns a new technique, process and/or hardware/software to perform their duties, their competency in that area should be tested.

Proficiency Testing

Proficiency testing is a means to confirm that a trained Digital Forensic examiner is qualified to continue performing the duties of Forensic Data Recovery. Annual discipline specific training and testing should be conducted to confirm the examiners level of proficiency.

Certification

Individual

Certification is the process by which an individual examiner undergoes assessment by a third-party auditor to determine if they meet certain requirements set out a standard for that discipline. Completion of the certification process can earn the examiner a certificate attesting to their understanding and compliance with the standard.

Facility

Third party assessment occurs when a facility is voluntarily audited against a standard or code by an independent, external body. Performance deemed to be in compliance with the standard is acknowledged by the granting a certificate. This certificate can be displayed and its contents communicated to relevant parties such as customers and governmental agencies.