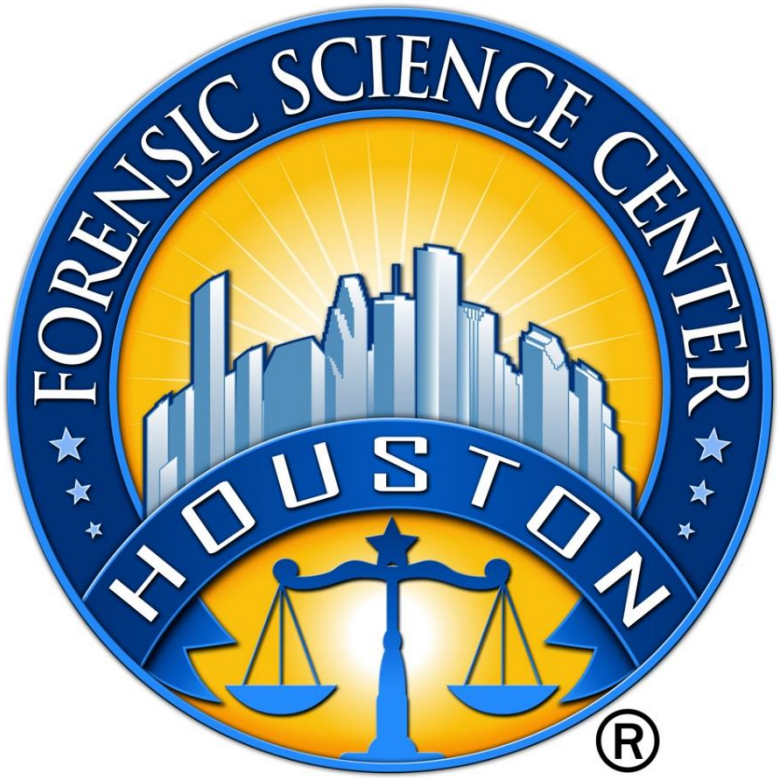

DIGITAL FORENSICS
TRAINING PROGRAM MANUAL

Crime Scene/Digital and Multimedia Division

Table of Contents

1. Scope

Education and training form the cornerstone for achieving excellence in the delivery of highly reliable and repeatable digital forensic services. The management of the Houston Forensic Science Center (HFSC) is committed to excellence by initiating, supporting, and adhering to this training program intended to develop Digital Forensic Laboratory (DFL) staff technical skills through a set of relevant and comprehensive training activities.

This training manual and the overall training program is applicable to management and technical staff of the Digital Forensics Laboratory. The training program includes basic HFSC orientation training, training and development of digital forensic skills, competency and proficiency testing, continuing education, and advanced technical skills training and certification. This program defines requirements for the career development of examiners from the basic levels of technical services to the professional development of expert level competencies.

2. Training Objectives

The objectives of this training program include:

- Establishing the required technical knowledge, skills, and abilities for each category of examiner to develop a level of competency.
- Identifying core training requirements that provide a foundation to develop required competencies.
- Identifying continuing education requirements to remain proficient and current with rapidly evolving technologies.
- Defining annual proficiency testing requirements.
- Identifying opportunities for advanced external certifications to perform more complex technical tasks.

3. The Training Program

3.1 Management Responsibilities under the DFL Training Program

3.1.2 Digital Forensic Laboratory Supervisor

The Digital Forensic Laboratory Supervisor is responsible for assessing the competency of technical examiners, recommends to the Forensic Analysis Division Director and Quality Director the authorization of examiners to perform specific technical services based upon each individual examiner's demonstrated knowledge, skills, and abilities. The HFSC maintains records of the examiner's training, mentoring records, competency examination results, software certifications, authorization memo specifying forensic equipment and software authorized to use, continuing education, and proficiency test results.

The section supervisor is responsible for assessing the training needs for examiners assigned to the DFL based upon the technical services offered. The supervisor balances the workloads of forensic services technical examiners to ensure that adequate training and mentoring are provided for the professional development, and that examiners successfully complete competency testing and annual proficiency testing demonstrating a baseline understanding for applying quality and technical policies and procedures when performing technical services. The supervisor is

responsible for assessing the competency of forensic services technical examiners, and recommending when new technicians and Examiners (trainees) have developed the necessary knowledge, skills and abilities to be authorized to perform independent technical services. The supervisor is responsible for assessing the professional development of each individual to determine his/her potential ability to perform more advanced technical services, serve as a mentor to less experienced examiners, or be responsible for laboratory programs (i.e., technical processes, etc.).

3.1.3 Mentors

Mentors are qualified examiners who are assigned by management to provide direct day-to-day training and guidance to less experienced examiners or trainees. The mentor's primary goal is to guide and train examiners in performing their technical and administrative responsibilities.

Mentors strive to facilitate professional and technical development of the examiner they are assigned to train and mentor. They work closely with the section's supervisor to ensure that the training program is effective and relevant, offering suggestions for improvement as a result of their mentoring experience.

The development of each examiner's knowledge, skills, and abilities under the guidance of their mentor are documented in a Training and Mentoring Guide which serves as an official record of the progress for each examiner undergoing basic or higher level technical training and development. The mentor is responsible for verifying the mentored examiner's skills and abilities to perform specific administrative and technical tasks as documented in this record.

3.2 Casework Authorization

The Training and Mentoring Guide, competency examination results, mentored casework report(s) and results, and other supporting documentation is reviewed and approved by the Section Supervisor and Quality Director before independent casework begins.

Letters of authorization are issued upon approval of the successful completion of training and a competency exam. This letter specifies the technical services the examiner is authorized to perform and is signed by the Section Supervisor and the Quality Director. New letters are issued as the examiner develops new competencies.

Clause: Because the HFSC DFL has been operational for many years, those working in the laboratory will undergo a review of their education, training, certifications, and technical experience against the knowledge, skills, and abilities defined in this manual. Examiners fulfilling the competence requirements will be issued a Letter of Authorization delineating the areas in which they are qualified and authorized to perform analysis.

3.3 Examiners

Examiners include examiner trainees, examiners, and experts assigned to the DFL. The general requirements and procedures for DFL examiners can be found in the DFL SOP or on the City of Houston or HFSC websites. However, since the Digital Forensic discipline is quite new, often the traditional job descriptions do not map the actual work performed by examiners. This Training Manual section describes the knowledge, skills, and abilities, as well as technical responsibilities of examiners.

Examiners are required to participate in ethics training which will be offered at least annually. Examiners should receive training on such topics as presenting evidence during court and testimony, understanding the rule of law, criminal and civil procedure, and data spoliation considerations as it relates to their responsibilities in forensic science, digital evidence, and eDiscovery, if applicable.

The training program has been developed under the premise that examiners begin at the most basic level for technical training and professional development. Training may be modified for newly hired experienced examiners. Regardless of the experience level, all trainee examiners are evaluated and deemed competent to perform technical services upon successful completion of a competency test.

The training program is organized into the following three major categories for training, establishing and retaining competency, and professional development:

- Examiner Trainees
- Forensic Examiners
- Expert Examiners

3.3.1 Examiner Trainees

Examiner Trainees, regardless of their previous training and /or experience, are new examiners to the HFSC**.** Trainees must complete the required training for their position and demonstrate knowledge, skills, and abilities prior to being authorized to perform independent technical services.

3.3.1.1 Demonstrate Technical Knowledge

- Understand the technical processes and general forensic methodologies and tools to preserve and collect electronically stored information from digital devices and networks.
- Understand the technical processes and procedures to preserve and collect data from physical devices such as hard drives, laptops, and desktop computers using approved hardware and software. Understand the requirements for uniquely identifying, documenting, and controlling digital evidence in addition to requirements for sealing and storing physical evidence.
- Understand the most common data structures and server architecture to facilitate basic collection of electronically stored information.
- Understand common Windows file structure, Microsoft Office applications, and concepts for data storage on internal and external devices, the characteristics of electronic stored information (i.e., logical and physical data on a hard drive) vs. Redundant Array of Independent Disks (RAID) storage (i.e., server logical data), and the methods to identify and analyze computer activity (e.g., forensic artifacts, metadata, timelines, etc.).

3.3.1.2 Demonstrate Technical Skills and Abilities

- Remove hard drives from laptops or desktops for data collection and preservation. Use write protection devices, imaging hardware (e.g., Logicube) and forensic software to collect and preserve data from physical devices. Use verification (hash) tools from within forensic products to verify physical or digital data (i.e., network) recovered or collected. Use hardware and software to forensically wipe devices of data. Use other tools to collect and recover relevant data requested by the customer while maintaining the integrity of the data.
- Uniquely identify, document, seal and securely store physical evidence/devices. Uniquely identify, document, and secure digital data.
- Should a forensic image be archived on the forensic SAN, uniquely store the files within an "images" folder inside the master uniquely-identifiable case folder. Can HASH the contents of the contents of the "images" subfolder and store that value in the main case folder.
- Recover and collect electronically stored physical and logical level data from devices and/or networked computers which may include the machine BIOS, Windows Registry, active files and folders, deleted files and folders, Pagefile data, unallocated data recovery, data carving, social network artifacts and transactions, email and email attachments, link file analysis, file metadata extraction, temporary file activity, and browser history and activity. Use forensic analysis tools to filter and sort data based upon file types, dates, special characters (e.g., credit card number) text searches, and password recovery and/or cracking.
- Document in sufficient detail technical processes and procedures in LIMS. Draft a report that meets the HFSC standards for reporting.

3.3.1.3 Demonstrate Non-Technical Knowledge

- Understand the legal requirements for data preservation, criminal procedure, presentation of findings of collected data in court, during affidavits, or during depositions, as well as the concept and consequences of data spoliation.
- Understand the requirements for sensitivity of the nature of their work, privacy of parties, and confidentiality of the data recovered.
- Understand the quality management system requirements for administration, operations, and technical specifications for documenting processes and procedures in the HFSC Quality Manual.

3.3.1.4 Demonstrate Non-Technical Skills and Abilities

- Follow legal requirements for data preservation. Present findings and evidence in court, affidavits, or during depositions as well as describe the technical processes and procedures for data collection and preservation. Avoid any action which would result in spoliation of original physical or digital data.
- Maintain a high degree of personal and professional ethical behavior. Protect the confidentiality of technical services and recovered data.
- If needed, establish and maintain communications with the customer throughout the services, and

when practical, receive feedback on the product provided to the customer.

- Embody ethical standards in technical services, interaction with stakeholders, and maintain a high degree of professional responsibility.
- Follow the HFSC Quality Manual requirements for laboratory operations, technical specifications for documentation in the LIMS, and participate in continuous quality improvement activities such as internal audits, offering suggestions for process improvements, corrective actions and/or preventive actions.

3.3.1.5 Technical Training Requirements

Trainees must successfully complete the following vendor or in-house technical training courses to be qualified as a Forensic Examiner:

- EnCase Computer Forensics I and II or equivalent; and/or item 2
- AccessData Bootcamp and AccessData Advanced Forensics or equivalent; and
- One of the following – USSS BCERT, SANS 401, SANS 408, IACIS BCFE, NW3C Basic Data Recovery and Acquisition (BDRA) CyberCop 101, or other DFL Supervisor approved equivalent courses offered that is designed to provide knowledge and skills necessary to respond to an electronic crime scene, to safely and methodically collect, and preserve items of evidentiary value that may be used in court proceedings.

3.3.1.6 Mentorship Requirements

Trainees must successfully complete a period of performance under the training and guidance of a mentor. The mentor guides the development of knowledge, skills, and abilities and will assist with applying the technical and quality policies and procedures in practice. Specific mentoring activities and experiences are documented on the Training and Mentoring Guide by the trainee and verified by the mentor. At the conclusion of the training period, the Section Supervisor reviews the Training and Mentoring Guide to verify that the required mentoring activities have been completed.

3.3.1.7 Competency Test Requirement

Upon successful completion of technical training and after having performed technical examinations under the guidance of a mentor, the Section Supervisor can administer a competency test to the trainee. The competency test includes a practical application of technical skills and the quality management system requirements (i.e., required level of detail for forensic reporting, and using approved technical methods), and, if deemed necessary, an oral examination of the trainees' ability to define technical processes and terms logically and professionally.

If the trainee is unsuccessful in completing the competency test, a remediation plan is developed by the mentor and approved both by the Section Supervisor and the Quality Director. The remediation plan will focus upon the trainee's deficiency(s) identified during testing.

3.3.2 Forensic Examiner

Forensic Examiners (FE) perform basic, intermediate, and advanced data imaging, file recovery and analysis, and data wiping services. They may also conduct mobile phone data extraction. This category of Examiners may be involved with assigning technical services, performing technical and administrative reviews, and be responsible for administrative or technical processes (i.e., evidence management, equipment management, technical procedure updates or new procedure test and validation). This is delineated in their letter of authorization.

3.3.2.1 Demonstrate Technical Knowledge

- Understand complex data structures and storage devices to the extent necessary to recover Electronically Stored Information (ESI) for mainstream requests.
- Understand technical processes and procedures to preserve and collect electronically stored information using standard and non-standard methods.
- Understand requirements for complex forensic service requests and develop effective organization skills for data collection and recovery from multiple sources and/or multiple subjects in the same request.
- Understand the value of data stored in the Windows Registry, temporary files, and transactional data that facilitate development of timelines and identify user activity. Understand the nature of password protected files and encryption, and methods to recover or defeat passwords encryption.
- Understand the requirements and methods for network forensics, UNIX forensics, and/or MAC forensics.
- Understand the nature of volatile data and methods to capture volatile data.
- Understand the requirements for updating technical procedures, and/or test and validation of new procedures to remain relevant with best computer forensic industry practices.

3.3.2.2 Demonstrate Technical Skills and Abilities

- Use their knowledge, training, and experience to address requests to locate and access electronically stored information from complex data systems.
- Use standard and non-standard methods to collect, preserve, and maintain the integrity of electronically stored information.
- Use their experience to collect data from multiple data sources in more complex work.
- Apply knowledge of a Windows Operating System to recover and analyze forensic artifacts from the Windows Registry, temporary files, and transactional data which may be used to develop timelines and identify user activity.
- Recognize password-protected and encrypted files. Use forensic methodologies or technical tools to defeat encryption when possible, recover or decode passwords, and/or by-pass passwords to access the data being protected.
- Perform one or more of the following technical processes:

- For cell phone examiners, use mobile device extraction software and hardware to retrieve data from mobile devices.
- Conduct forensic examinations on MAC equipment.
- Conduct advanced hard drive recovery.
- Restore a hard drive from a forensic image using standard forensic methodologies.

- Use methods to capture volatile data stored in memory on computers and laptops if received in a powered-on state.
- Recognize the need for tested and validated methodologies in computer forensics for the average investigation.
- Understand that computer forensics is a fast-paced, evolving field where experimental methods are often required to address the needs of the customer. Static approaches are often ill-suited to keeping pace with technology in many cases. Examiners must be able to overcome obstacles and adapt with new and reproducible approaches in order to successfully complete an assignment. Examiners must be able to articulate and document the approach utilized in the case record when mainstream software or hardware is not able to extract the required data.
- Understand how to document validation studies and performance verification tests on hardware and software categorized as a forensic tool.

3.3.2.3 Demonstrate Non-Technical Skills and Abilities

- Recognize the skill levels and abilities of colleagues to ensure that only those qualified and authorized are performing specific technical tasks. Understand the requirements and required skills for examiners to be deemed competent to conduct certain types of technical services.
- If authorized, effectively perform technical and administrative reviews of technical services offering suggestions for improvement or correction of deficiencies. Evaluate and review the technical notes and reports to be issued to customers to ensure they meet the sectional and Quality Manual requirements.

3.3.2.4 Continuing Education Training

To maintain some outside certifications, continuing education is required. Examiners are also encouraged to participate in continuing education training to maintain proficiency. Continuing education, certifications not completed under their trainee training, and advanced training may include:

- EnCase Advanced or equivalent;
- AccessData Advanced Decryption or equivalent;
- AccessData Windows Registry or equivalent;
- USSS, Celebrite or other comparable mobile device data extraction training or equivalent;
- SANS or IASIS training courses on digital forensics

- Forensic training provided at CEIC and/or HTCIA conferences, webinars, symposiums, or attending related university courses.

3.3.2.5 Mentorship Requirements

Less experienced examiners or examiners learning new technologies may be required to complete a period of performance under the training and guidance of a more experienced mentor who will guide the application of technical procedures.
On a case-by-case basis, examiners may be qualified and selected to train and mentor trainees or less experienced examiners in specific administrative or technical tasks.

3.3.2.6 Casework Authorization Requirements

For newly hired experienced examiners, they must successfully complete technical training, courtroom testimony training, data collection and evidence preservation training, anddemonstrate a competent level of knowledge, skills, and abilities to perform technical and non-technical responsibilities. For current Forensic Examiners, a review of their education, training, certifications, and technical experience is completed. The examiner must possess or have received one of the following external certifications and/or degrees to be deemed competent to perform computer casework:

- EnCase Certified Examiner (EnCE) certificate
- Access Data Certified Examiner (ACE) certificate
- Master's Degree in Computer Forensics

The examiner must possess or have received one of the following external certifications and/or degrees to be deemed competent to perform mobile device/ cell phone casework using that manufacturer's forensic product or software:

- Certification from Micro Systemation for XRY ;
- Mobile Phone Examiner (MPE) Certification from AccessData Corporation;
- Both Cellebrite CCLO and CCPA Certifications, or a Cellebrite CCME Certification

Examiner's fulfilling the competency requirements will be issued a Letter of Authorization delineating the areas in which they are qualified and authorized to perform analysis.

3.3.3 Expert Forensic Examiner

In addition to mastering the knowledge, skills, and abilities of Forensic Examiners, Expert Examiners, also referred to as Technical Experts (TE), will have a minimum of 3 years of computer forensic experience and be able to demonstrate the following:

3.3.3.1 Demonstrate Knowledge

- Understand the need and requirements for training specialists in the current, improved or new

methods to support requests.

- Understand the requirements for test and validation of new methods.
- Understand the technical methodologies used by the team to the expert level.
- Understand troubleshooting methodologies for forensic software, hardware, hard drive recovery, and alternative methods for performing services when standard attempts to collect data fail.
- Understand the need for accurate and unbiased technical reporting of results.

3.3.3.2 Demonstrate Skills and Abilities

- Implement training programs in methodologies and provides technical and quality training and mentorship to less experienced examiners.
- Perform verification tests and validations of new forensic software, hardware and methods. Use their knowledge, training, and experience to address requests for collection of data from more complex data stores which may include using non-standard methods for analysis and/or collection.
- Serve as a technical advisor to the HFSC and customers, if appropriate.
- Implement troubleshooting methodologies when forensic software or hardware fail, or when attempts to collect data from data stores are unable to be accomplished using standard methods.
- Review and analyze reports for accuracy, unbiased findings and conclusions, and ensures they meet the sections and Quality Manual standards. Train and mentor less-experienced technical expert examiners with reviewing reports.
- Monitor HFSC LIMS transactions, file content, and evidence movement to ensure that their specific LIMS file and evidence integrity is maintained.

3.3.3.3 Demonstrate Non-Technical Knowledge

In addition to the requirements for examiners, TEs are expected to understand the rapidly evolving digital forensics and data recovery industry in terms of technical challenges that it presents for the DFL or HFSC and the legal issues that must be considered when providing services.

3.3.3.4 Demonstrate Non-Technical Skills and Abilities

TEs provide HFSC management with recommendations for technical and operational improvements that increase the efficiency and effectiveness of the laboratory and service to the customer that meets technical challenges and ensures reliable and defensible results are provided to the customer.

3.3.3.5 Technical Training Requirements (Continuing Education)

To maintain competency, Technical experts are encouraged to participate in continuing education training. Continuing education training may include:

- Advanced coursework in data collection and collection methodologies;

- Advanced coursework in digital forensics; and/or
- Other forensic training at conferences, symposiums, webinars or attending related university courses.

It is desirable that TEs earn computer forensic certification from a reputable organization.

3.3.3.6 Serve as Mentors

TEs serve as trainers and mentors guiding professional development and practical application of technical and quality management system knowledge, skills, and abilities to less experienced forensic Examiners and trainees.

3.3.3.7 Casework Authorization Requirements

For newly hired experienced TEs, they must successfully complete technical training, courtroom testimony training, and demonstrate a competent level of knowledge, skills, and abilities to perform technical and non-technical responsibilities. For current Forensic Examiners, a review of their education, certifications, and technical experience is evaluated to determine if they are qualified to be a Technical Expert. Technical Experts must fulfill the Forensic Examiner competence requirements. Examiner's fulfilling the competence requirements will be issued a Letter of Authorization delineating the areas in which they are qualified and authorized to perform analysis.

3.4 Other Training Opportunities

3.4.1 In-House Developed Training

On occasion, due to financial constraints, unique training topics, or lack of relevant vendor-based training, it may be necessary for the laboratory to develop training in-house. The requirements to earn continuing education credits include:

- The trainer will develop course materials and training objectives which shall be peer reviewed by the DFL Section Supervisor.
- The trainer will document criteria for students to successfully complete training (e.g., written test or practical exercise) and develop the criteria tools.

3.4.2 Professional Organization Conferences, Seminars, and Symposiums

The following is a list of some recognized professional organizations that offer educational programs as part of their conference, seminar, or symposium activities:

- High Technology Crime Investigation Association (HTCIA) Annual Conference
- Computer and Enterprise Investigations Conference (CEIC)
- SANS FIRE (Forensics, Investigations, Response & Education) Conference
- Paraben Forensic Information Conference (PFIC)
- International Association for Computer Information Systems (IACIS)

3.4.3 Web-Based Training

Several organizations offer web-based training which may be relevant to the technical services offered by the DFL section. A limited number may be offered for free. Those not charging a fee are often sponsored by and oriented to a vendor, but still offer information which may be of value by increasing knowledge of the vendor's tools and capabilities. Some organizations include:

- Guidance Software
- AccessData
- National White Collar Crime Organization (NW3C)

4. Management Training Requirements

4.1 Technical Supervisor

In addition to the required general HFSC training, it is recommended that the DFL Section Supervisor participate and remain current on digital forensic technology challenges, advancements and developments, and related legal issues by continuing education training. The continuing education training may be met by attending classes, symposiums, webinars, conferences, or attending related university courses.

5. DFL Proficiency Test Program

Generally, the forensic community defines Computer Forensics as a subcategory of testing for the Digital and Multimedia Forensic Discipline. The HFSC has further divided the Digital Forensics discipline into two subcategories of testing: cell phone and computer forensics. Technical examiners are proficiency tested in at least one Digital Forensic sub discipline (i.e., computer forensics, cell phone forensics) in which they have been deemed competent. During the accreditation cycle, examiners who are authorized to conduct examinations in multiple sub- disciplines (e.g., computers and cell phones) must take at least one proficiency test in each authorized category of casework. Proficiency tests will be performed using laboratory approved hardware, software, and methodologies.

6. Professional Organizations and Memberships

HFSC examiners are encouraged to participate in local, regional, national, and international professional organizations relating to forensic science and information technology. Such groups provide a source of relevant technical and forensic science laboratory references and information that can enhance professional development. Recognized organizations include:

- HTCIA
- IACIS