

A. Purpose:

To train employees (new or those where re-training is indicated) in the Standard Operating Procedures of the Computer Crimes Electronic Evidence Unit (CCEEU).

B. Responsibility:

Operations Manager of ID: to assure all training is preformed using the guidelines set forth in this document. The Manager may perform parts of the training or assign a designee as the trainer.

Forensic Science Examiner 3 or 2: to assist the unit Manager in coordinating the employee training and to maintain training documents. To evaluate trainees to assure that training goals are accomplished.

Trainer: to adhere to the training guidelines set forth in this SOP. To train the trainee in a manner consistent with the standard operating procedures for the CCEEU.

Trainee: (new employee or any employee undergoing re-training): to adhere to the guidance of the CCEEU SOPs.

C. Definitions/Abbreviations:

Refer to SOP-CC-26 - Definitions and Abbreviations.

D. Procedure:

New Employees (or Newly Assigned Employees):

The following training outline will be followed for all persons newly assigned to the CCEEU. The amount of time necessary to achieve proficiency in any area may be affected by the previous experience and training of the individual examiner; the goal is to complete the tasks in six (6) months. The time period may be extended depending on individual's progress and other circumstances.

The examiners may be authorized in various categories of casework as they successfully complete a method of testing.

1. Introduction: The first section of this training manual are common to all of the DSS. The trainee is responsible for learning and familiarizing themselves with the general concepts of these chapters before beginning training in the Digital Forensic Unit (DFU).

a. Goals:

- i. Upon completion the examiner will be familiar with the DSS operation, LIMS system and individual responsibilities.

- b. Tasks: Refer to GL-14 General Training for additional guidance.
 - i. Orientation to the DSS facility and personnel and review of Table of Organization.
 - ii. Instruction of the organization structure, code of ethics and chain of command.
 - iii. Security and confidentiality requirements.
 - iv. Alarm code and scan cards will be requested via QMS workflow.
 - v. Introduction to the quality control and quality assurance, including required documentation and the use of the QMS.
 - vi. Safety procedures - incident reports, fire and emergency procedures will be reviewed in QMS training.
 - vii. GL2.2 and GL14.1 will be completed and returned to the Quality Manager for signature. The signed forms will be uploaded to the QMS.
- c. Readings:
 - i. General Laboratory SOPs and Unit SOPs.
- d. Assessment:
 - (a) Completion is indicated by the completion of General Laboratory form GL-14:1, GL-2.2 and GL-14.4 (contract employees only)

2. Evidence Handling

- a. Goals:
 - i. To handle evidence in a manner appropriate for the DSS and to preserve evidence which may be analyzed by other sections / units within DSS.
 - ii. To learn the operation of the LIMS system, item assignment, and the maintenance of chain of evidence for submissions and items.
 - iii. To demonstrate proficiency in the basic tasks necessary to complete evidence transfer functions and create a chain of evidence.
 - iv. Three mock cases with evidence will be provided for employee to perform transfers.
 - v. LIMS Administrator will initiate the LIMS QR-01 worksheet.
- b. Reading:
 - i. LIMS GL as assigned in QMS and Unit SOPs

3. Foundational Scientific Knowledge

- a. Goals:
 - i. To assure examiners have both an educational and working knowledge of the fundamental basis of computers and digital media.
- b. Tasks:

- i. Document any coursework and training received prior to or during the training period which has been identified as essential to the well-trained person performing the analyses. All certifications and course information will be added to training binder and also uploaded to the QMS.
 - ii. List and upload to QMS any prior experience or professional organization memberships and certifications held by the trainee that are recognized in the field of computers and digital media forensics.
 - iii. Completion of assigned trainings to include online classes, training webinars, readings and external trainings. Trainings are divided between cell phone analysis, data analysis and then other types of digital evidence examination.
4. Cell Phone Analysis
- i. Unit SOPs for cellphone analysis will be reviewed.
 - ii. Trainings for understanding of cell phone data and its analysis will be assigned.
 - iii. Trainings will include the use of primary software used for cell phone analysis to include: Cellebrite, Greykey, Magnet Axiom and other tools if necessary.
 - iv. During the portion of the training, the trainee will review the State and Federal statutory language for child sexual abuse material (CSAM). Trainee will be introduced to Cybertips and how the National Missing and Exploited Children (NCMEC) distributes tips and reviews recovered evidence using the Child Recognition and Identification System (CRIS) form.
 - v. Trainee will be introduced to methods to categorize images and videos as CSAM, Age Indeterminate (or similar title) CGI/Anime and non-pertinent.
 - vi. Trainee will review Proficiency Test Non-consensus binder prior to competency test.
- b. Assessment:
- i. Refer to QR CC-47 for practice analysis and competency cases to be assigned.
 - ii. Assessments will include keyword search, GPS locations and the use of a secondary tool to verify GPS locations. Practice cases will include report writing as part of the exercise.
 - iii. Completion of a competency case to include a proficiency case involving the analysis of data from a cell phone.
5. Other Technical Knowledge
- a. Goals:
 - i. To demonstrate specific knowledge related to the field of digital evidence. Detail required should correspond to the types of analysis and the level of independent work required, corresponding to the applicable job description.
 - b. Tasks:
 - i. To provide instruction and show proficiency in the following areas:

Approved by Director: Dr. Guy Vallaro

- (a) Data analysis
 - (b) Data recovery
 - (c) Data restoration
 - (d) Imaging/Acquisition
 - (e) Cell phone data recovery
 - (f) Hard drive sterilization
 - (g) Removable media sterilization
- ii. Other training may be included after assessment for data analysis that can include Chip Off processing, vehicle infotainment acquisition and analysis, cloud analyzer.
- c. Required reading
 - i. Review of SOPs, validations studies both internal and external and performance checks for the various procedures.
 - ii. Review of Proficiency Test Non-Consensus results.
- d. Assessment:
 - i. Documentation of successful completion of each task by written and /or oral examination will be made on QR CC-47 "In-House Training and Qualification Record".
 - ii. Documentation of practice cases that include the application of imaging/acquisition, data recovery, data restoration, use of Griffeye/Magnet Axiom, sterilization of hard drives and removable media. Cases will include report writing as part of the exercises.
 - iii. Completion of a competency case involving the analysis of data from a hard drive.
 - iv. Documentation of the readiness for casework by the unit Supervisor in the form of an approval memo.
- 6. Legal Issues
 - a. Goals:
 - i. To become familiar with the legal requirements for testimony in Connecticut.
 - b. Tasks:
 - i. The Examiner will receive instruction on the requirements and testimony related to:
 - (a) Qualifications
 - (b) Technical testimony
 - (c) Courtroom dress and demeanor
 - (d) Ethical responsibilities of expert witnesses
 - (e) Laboratory courtroom monitoring procedures and reports
 - (f) Presentation of evidence
 - (g) Pertinent rules of the courtroom
 - c. Required reading:
 - i. Transcripts or sample testimony
 - ii. State admissibility requirements (*State v. Porter*)
 - iii. Admissibility, in general -*Frye*, *Daubert*, etc.

Approved by Director: Dr. Guy Vallaro

- d. Assessment:
 - i. Oral or written questions by the section supervisor or designee.
 - ii. Moot court - each examiner who is new to the Laboratory shall demonstrate expertise by Moot court. Documentation of the Moot court should contain an evaluation in memo form of the examiner's responses and demeanor.
 - iii. Feedback is provided to the analyst and is documented on the records
- 7. Assessment method, in general:
 - a. A checklist (QR CC-47 "In-House Training and Qualification Record") for each of the above, listing the specific skills, knowledge or ability demonstrated for a particular requirement. This would be signed off by for each step by the Supervisor / Technical Lead conducting the training and the examiner. At the end of the training program a memo would be written that all training is complete, as outlined in the Quality Manual.
- 8. Re-Training:
 - a. Re-training may be indicated due to numerous issues such as:
 - i. Failing a proficiency test
 - ii. Unsatisfactory analysis of case materials as determined by the unit Supervisor or unit Technical Lead.
 - iii. An extended leave from the unit.
 - iv. Other
 - b. The extent of the re-training will be dependent on the specific circumstance. The unit Technical Lead with the unit Supervisor will develop a written re-training plan prior to implementation of the training. The Deputy Director or Division Quality Manager may be consulted to assure the plan is comprehensive.
 - i. In general the training plan will include:
 - (a) Goals of training.
 - (b) The individual(s) performing the training.
 - (c) The steps of the training (tasks to be performed, reference materials to be reviewed, if applicable, specific topics to be covered).
 - (d) Timeline for completion.
 - (e) Method of assessment of the training (acceptable methods of assessment include a written test, oral examination documented by the unit Supervisor / Technical Lead, or a competency test).
 - c. Completion of the re-training will be indicated by:
 - i. The successful completion of the assigned tasks.
 - ii. The successful completion of the competency test.
 - iii. Documented review of the training materials by the unit Supervisor / Technical Lead.

*Approved by Director: Dr. Guy Vallaro***9. Training/Re-Training Completion Approval**

- a. Upon completion of the training exercise(s), the examiner's training records will be provided to the Quality Manager for review. Upon completion of GL-14.3 (Review of Training Records), the supervisor may move forward with assigning the examiner a competency test.
- b. The examiner will be issued a competency test which will include reporting writing. This may be followed up with an oral or written test which the examiner must pass with a grade of 80% or better.
- c. At the end of the training/re-training program, a memo/email shall be written to the Deputy Director stating that the examiner has successfully completed their training and has been administered a competency case that evaluated their analytical skills and their ability to clearly communicate their findings in a report.
- d. The Deputy Director may review the training files or simply endorse this memo/email and generate a request to the QMS requesting that this examiner be authorized to perform casework in that discipline.
- e. A Qualtrax workflow will be initiated for the authorization of the examiner. The workflow may include the following in which the analyst is being authorized:
 - i. Handle evidence,
 - ii. Perform examination and/or analytical methods,
 - iii. Utilize all applicable equipment in methods described in SOPs,
 - iv. Report, review and authorization of results,
 - v. Perform administrative reviews,
 - vi. Perform Validations in the Discipline,
 - vii. Development of new methods,
 - viii. Modification of methods,
 - ix. Verification of methods

10. Technical Review Approval:

- a. The examiner will perform casework and after gaining experience in conducting analysis and reporting findings in a variety of evidence type/conclusions in the discipline, their experience will be evaluated for the ability to conduct technical reviews. This evaluation period may include technical review ghosting with an experienced examiner. Once the examiner has completed the evaluation period, a memo/email shall be written to the Deputy Director stating that the examiner has successfully completed their evaluation period and has been deemed competent to conduct technical reviews in that discipline.
- b. The Deputy Director, after review, may endorse this memo/email and generate a request to the QMS requesting that this examiner be authorized to perform technical reviews based upon the examiner's casework experience in that discipline.

Approved by Director: Dr. Guy Vallaro

- c. A Qualtrax workflow will be initiated for the authorization of the analyst in the following:
perform technical reviews of cases and testimony and/or perform administrative reviews.

11. References:

- a. All associated reference materials relating to the training process are maintained in the CCEEU library, archived on the main CCEEU server (currently the iso folder) and online.
- b. QR CC-47 "In-House Training and Qualification Record"