Computer Forensics Forensic Scientist Training Program

1.0 Purpose - The purpose of this training program is to outline the steps necessary to become qualified to perform computer forensic cases.

2.0 Scope

2.1 The Computer Forensics Forensic Scientist Training Program is designed in a series of blocks. Each block is composed of several assigned tasks. When the Trainee has completed a task to the satisfaction of the Supervising Forensic Scientist, the Supervising Forensic Scientist shall initial the line next to that task. Upon successful completion of each block of instruction, the Supervising Forensic Scientist shall initial beside the task and write a memo to the Forensic Scientist Manager, Trainee, and the Trainee's training file documenting the completion of the instruction. Blocks of instruction may be worked concurrently.

2.2 Additional sources of education in the field of computer forensics shall be considered for Forensic Scientist Trainees and qualified Forensic Scientists as scheduling, availability, and Laboratory resources allow. Additional training may include but is not limited to the following:

2.2.1 Computer Forensic Training Courses by the National White Collar Crime Center.

2.2.2 Computer Forensic Training Courses by the American Academy of Applied Forensics

2.2.3 Computer Forensic Training Courses by the Federal Law Enforcement Training Center.

2.2.4 Investigation of Computer Crime – SEARCH.

2.2.5 A+ Certification

2.2.6 Computer Forensics Bootcamp Courses for Certification

2.2.7 Vendor specific training courses such as Guidance Software, AccessData, Magnet Forensics, Cellebrite, MicroSystemation, etc.

3.0 Training Procedure

3.1 Block I - General Laboratory Procedures

The objective of this block of instruction is to familiarize the trainee with the general practices and procedures used at the State Crime Laboratory.

3.1.1 See of the Laboratory Procedure for Personnel Training (4.2) for this requirement.

3.2 Block II - General Computer Knowledge

The object of this block of instruction is the demonstration of the knowledge needed for casework.

3.2.1 The Trainee shall be able to explain the differences between file structures such as FAT16, FAT32, and NTFS.

3.2.2 The Trainee shall have a working knowledge of Microsoft DOS. The Trainee shall be able to boot a computer into DOS, view directories in DOS, and execute programs in DOS.

3.2.3 The Trainee shall demonstrate knowledge of the various computer operating systems (e.g., DOS, Windows, Mac OS, and Linux).

3.2.4 The Trainee shall demonstrate knowledge of the internal components of a computer (such as the hard drive, motherboard, and the RAM).

3.2.5 The Trainee shall demonstrate knowledge of various types of storage media (e.g., hard drives, floppy disks, CDs, CD-Rs, CD-RWs, DVDs, Zip disks, and flash memory cards).

3.2.6 The Trainee shall successfully complete a written examination to demonstrate his or her general computer knowledge.

3.3 Block III - Policies and Procedures of Computer Forensics

The objective of this block of instruction is a working knowledge of the policies and procedures used in the forensic examination of computer evidence.

3.3.1 The Trainee shall find articles on computer forensics and create a personal library.

3.3.2 The Trainee shall study the computer forensics technical procedures. The Trainee shall understand the procedures and the consequences to the evidence if the procedures are not followed in a case.

3.3.3 The Trainee shall study additional reading (e.g., equipment guides, manuals, articles, and books) as assigned by the Supervising Forensic Scientist and demonstrate an understanding of the materials.

3.3.4 The Trainee shall attend approved training session(s) on the use of computer forensics software.

3.3.5 The Trainee shall successfully complete a written examination to demonstrate his or her knowledge of the computer forensics policies and procedures.

3.4 Block IV - Forensic Acquisition

The objective of this block of instruction is to allow the Trainee to begin working with computer forensics evidence under the supervision of a trained Forensic Scientist.

3.4.1 The Trainee shall assist in preparing computer evidence for examination under the direct supervision of a trained Forensic Scientist.

3.4.2 The Trainee shall have a working knowledge of the verification procedures used within the unit. The Trainee shall be proficient in verifying equipment used during analysis.

3.4.3 The Trainee shall become proficient in preparing media for an examination.

3.4.4 The Trainee shall become proficient in acquiring and extracting various types of digital media (e.g., hard drives, flash memory cards, CDs, and mobile devices).

3.4.5 The Trainee shall successfully complete a written examination to demonstrate his or her knowledge of acquiring and extracting digital evidence as written in the computer forensics technical procedures.

3.5 Block V - Competency Tests

The objective of this block of instruction is to ensure that the Trainee has developed the skills necessary to be certified as a Forensic Scientist.

3.5.1 The Trainee shall be required to pass a written examination to demonstrate the knowledge of computer forensics needed in everyday casework.

3.5.2 Each Trainee shall be required to pass a final practical examination that consists of conducting a computer forensic examination on digital evidence which has been prepared for this examination. The Trainee shall find all pertinent information which exists on the media.

3.5.3 The Trainee shall meet with the Deputy Assistant Director/Quality Manager to discuss accreditation.

3.5.4 The Trainee shall participate in a moot court that is based on the work done in the practical examination. The Forensic Scientist Manager may substitute an oral review board for a Forensic Scientist who already testifies in another discipline.

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
10/31/2013	2	Added issuing authority to header
11/07/2016	3	2.2 – edited statement for clarity 2.2.1 to 2.2.10 – updated additional course list 3.2.3 – edited statement to remove specific versions 3.2.5 – added "-" to CD references 3.2.6 – edited for grammar 3.4 – edited title from Imaging to Acquisition 3.4.4 – updated to include new technology and extracting mobile devices 3.4.5 – updated to include extracting for mobile devices 3.5.2 – changed piece of storage media to digital evidence 3.6 to 3.61 – removed block