Training Program for the Examination of Digital Media

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

2.0 Scope

2.1 This program is designed in a series of blocks. Each block is composed of several assigned tasks. When the trainee has completed a block to the satisfaction of the Training Coordinator, the Training Coordinator and the trainee shall initial the line next to that task on the training checklist. Upon successful completion of each block of instruction, the Training Coordinator shall write a memorandum to the Forensic Scientist Manager. The signed memorandum shall be placed in the trainee's training folder, and a copy of the memorandum shall be provided to the trainee, documenting the completion of the instruction. Blocks of instruction may be worked concurrently.

2.2 This training program includes training for all types of digital media (e.g. mobile devices, SD card, computers) encountered by the Laboratory. The training program may be completed for one or more types of media and then cross train in the remaining media types at a later date.

2.3 Should a new forensic scientist with previous experience provide training records, the Technical Leader, Training Coordinator, and supervisor shall discuss the possibility of employing an abbreviated training plan. If an abbreviated training plan is to be used, the Training Officer shall write a memorandum detailing the abbreviated training plan. The memorandum shall be provided to the Forensic Scientist Manager for final approval. The signed memorandum shall be placed in the trainee's training folder.

2.4 Additional sources of education in the field of computer forensics shall be considered for Forensic Scientist trainees. Additional training shall be determined based on scheduling, availability, and Laboratory funding.

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 The trainee shall read all laboratory procedures. A list of required laboratory policies and procedures shall be provided to the trainee. Once the trainee has read each laboratory policy/procedure, the trainee shall initial next to each listed policy/procedure.

3.1.2 Review the SDS for acetone.

3.1.3 The trainee shall successfully complete a written examination to demonstrate his/her knowledge of the laboratory policies and procedures.

3.2 Block II - General Computer Knowledge - The object of this block of instruction is the demonstration of the general computer 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 demonstrate knowledge of the internal components of a computer (such as the hard drive, motherboard, and the RAM).

3.2.3 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).

3.2.4 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 to develop a working knowledge of the policies and procedures used in the forensic examination of computer evidence.

3.3.1 The trainee shall review legal considerations for digital forensics examinations.

3.3.2 The trainee shall read all of the computer forensic discipline technical procedures. A list of required discipline specific technical procedures shall be provided to the trainee. Once the trainee has read each technical procedure, the trainee shall initial next to each listed technical procedure. 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.

3.3.3 The trainee shall study and become familiar with the Digital/Multimedia Scientific Committee documents and discipline specific baseline documents which include the Scientific Working Group Digital Evidence (SWGDE) best practices for all things computer forensics related. The trainee shall provide the Training Officer with a list of read SWGDE articles, which shall be placed in the trainee's training folder.

3.3.4 The trainee shall successfully complete a written examination to demonstrate his or her knowledge of the section's computer forensics policies and procedures.

3.4 Block IV – Worksheets and Forensic Advantage (FA)

3.4.1 The trainee shall gain a working knowledge of how to document case observations on the case notes form.

3.4.2 The trainee shall become familiar with the following aspects of FA:

- Creating and Editing FA Generated Worksheets
- Locating and Reviewing the Request for Laboratory Examination (RFLE)
- Using the Case Record Object Repository
- Using the Case Object Repository
- Transferring Evidence
- Creating Evidence
- Generating Lab Reports
- Accessing and Creating Communication Logs

- Scheduling Reviews
- Finalizing Lab Reports
- Creating Discovery Packets and Court Binder

3.4.3 The trainee shall complete a practical case entry in FA.

3.4.4 The use of FA shall be graded as part of each practice case in Block VIII.

3.5 **Block V – Forensic Software Familiarization** - The objective of this block of instruction is to familiarize the trainee with the approved forensic software.

3.5.1 The Training Coordinator shall provide instruction on the use of approved forensic software.

3.5.2 The trainee shall become familiar with each forensic software tool. A list of forensic software tools shall be provided to the trainee. Once the trainee has used the forensic software tool, the trainee shall initial next to each one.

3.5.3 The trainee shall complete an over-the-shoulder assessment using each of the forensic software tools.

3.6 **Block VI – Validation and Authorized Deviations**

3.6.1 The trainee shall perform a validation on a piece of forensic software or hardware. The trainee shall select a previously approved forensic software/hardware to perform the validation.

3.6.2 The trainee shall draft a validation report and memorandum. The validation report and memorandum will be graded based on thoroughness, steps taken, adherence to technical procedures, and the results.

3.6.3 The trainee shall select a current technical procedure and draft a Deviation Request Form (DRF) requesting at least one change. The DRF will be graded based on thoroughness and adherence to Laboratory procedures.

3.7 **Block VII - 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 qualified Forensic Scientist.

3.7.1 The trainee shall assist in preparing computer evidence for examination under the direct supervision of a qualified Forensic Scientist.

3.7.2 The trainee shall gain a working knowledge of the verification procedures used within the unit. The trainee shall demonstrate proficiency in verifying equipment used during analysis.

3.7.3 The trainee shall become proficient in preparing media for an examination.

3.7.4 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).

3.7.5 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.

3.8 Block VIII – Practice Cases

3.8.1 The trainee shall complete a minimum of three practice cases. If applicable, each practice case will increase in complexity.

3.8.2 The trainee shall present each practice case to all qualified examiners, in a round-table setting, describing how the examination was conducted (steps taken) and the results of the examination.

3.8.3 Upon successful completion of each of the practice test, the Training Coordinator and trainee shall initial the training checklist.

3.8.4 The trainee shall observe another forensic scientist providing court testimony. If no scientist is providing court testimony, it is permissible for the trainee to view previous testimony from an online source (example: WRAL). The trainee shall document the name of the forensic scientist observed and date of testimony.

3.9 Block IX - 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.

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

3.9.2 The 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.

3.9.3 The trainee shall complete an oral review board on the examination of digital media.

3.9.4 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 the oral review board for a Forensic Scientist who is already authorized in another digital evidence discipline.

Revision History		
Effective Date	Version Number	Reason
09/21/2020	1	Original Document – Created from Computer Forensics Forensic Scientist Training Program