Raleigh/Wake City-County
Bureau of Identification
Crime Laboratory Division

FORENSIC COMPUTER UNIT
TRAINING MANUAL

TABLE OF CONTENTS

Chapter 1: Training Program Overview 3
Chapter 2: TRAINING TASK #1: COMPUTER FORENSICS BASICS 8
Chapter 3: TRAINING TASK #2: IMAGING HARD DRIVES 11
Chapter 4: TRAINING TASK #3: IMAGING REMOVABLE MEDIA 13
Chapter 5: TRAINING TASK #4: IMAGING A MACINTOSH COMPUTER WITHOUT HARD DRIVE REMOVAL 15
Chapter 6: TRAINING TASK #5: PREVIEWING DIGITAL MEDIA 18
Chapter 7: TRAINING TASK #6: ANALYZING DIGITAL MEDIA 20
APPENDIX: FORENSIC COMPUTER UNIT TRAINING OUTLINE 23

Chapter 1: Training Program Overview

1.1 Orientation

1.1.1 Before beginning the training program, an orientation of the new employee will include an introduction to the operating facilities and personnel. This shall be in addition to any new employee orientation conducted by Wake County. A work/study area will be assigned by the Technical Leader or Supervisor. In addition, the following documents will be covered:

- CCBI Laboratory Administrative Procedures
- CCBI Laboratory Safety Manual
- CCBI organizational chart
- CCBI Standard Operating Procedures
- Forensic Computer Unit Technical Procedures Manual
- Forensic Computer Unit Training Manual
- Forensic Science Quality Manual

1.1.2 An introduction to the technical capabilities of area laboratories, to include jurisdictional boundaries and areas of overlap, will be discussed.

1.1.3 The outline of the training program and the expectations of the principal instructor, the Technical Leader and/or Supervisor, and the trainee will be discussed.

1.1.4 An explanation of the operation of local, state, and federal law enforcement agencies and court systems will be provided.

1.1.5 The duties of a forensic examiner will be clarified.

1.1.6 The employee will be introduced to the CCBI records management system.

1.2 Training Program

1.2.1 The goal of this manual is to provide uniform coordination and quality training in all aspects of the Forensic Computer Unit. Training is multi-faceted and ever changing. The chapters of this manual are outlined to allow for changes in technologies and processing techniques that are current for the training period. The sequence in which the modules are presented in the outline should not necessarily be considered as a mandatory order of instruction. Exposure to case examinations, legal aspects, and testimony will be continuous throughout the training period.

1.2.2 Proper and safe work practices shall be observed at all times.

1.2.3 The training program will be coordinated by the assigned principal instructor. Trainees go through ~~two~~ three phases of training, Phase I, ~~and~~ Phase II, and Phase III. The length of the training period is a highly variable matter and will be left to the determination of the principal instructor, with approval of the Technical Leader. Certain individuals may require less time than others, depending on experience, education, or learning ability. However, Phase I and Phase II training may require ten (10) to twelve (12)

months, ~~which is to include successful completion of a mock trial,~~ and Phase III training requires a minimum of six (6) months. Please refer to Chapter 22 of the CCBI Crime Laboratory Administrative Procedures Manual for further additional details on the training program requirements.

1.2.4 The principal instructor is responsible for the overall training, which will incorporate all of the listed topics, but may delegate certain duties and blocks of instruction to other examiners in the Forensic Computer Unit. The principal instructor is responsible for assuring that the appropriate documentation is completed in a timely fashion as training progresses.

1.2.5 The various Training Tasks will be assessed on a pass/fail basis. Periodic performance evaluations of the trainee will be prepared by the principal instructor and the results provided to the Forensic Quality Manager.

1.2.6 The trainee is expected to keep a notebook of information compiled during the training program. This notebook will contain at least the following, in addition to other relevant material:

- Notes generated during training tasks
- Copies of written examinations, presentations, and research papers prepared during training
- Documentation of the completion of the suggested reading list for each training task
- Written answers to any study questions provided by the principal instructor
- A copy of the monthly log of activities described in 1.2.7 below

The written answers to the study questions will be used as reference material once the trainee is qualified as a forensic examiner. Therefore, references are to be listed for each response whenever possible.

1.2.7 As designated by the principal instructor, the trainee may assist with casework during ~~the training~~ Phase II, only under the direct supervision of a qualified forensic examiner. The trainee will maintain a monthly log of activities and provide it to the principal instructor at the end of each month.

1.2.8 Phase I training includes all of the training topics fundamental to the discipline, practical exercises and examinations to demonstrate the ability to perform work in the discipline, oral and/or written examinations to assess knowledge of individual training topics, and a final comprehensive written examination.

In order to complete Phase I training, the trainee must successfully complete a mock court. The mock court should provide as realistic a courtroom experience as possible and will be used to evaluate the trainee's ability to effectively communicate his/her technical knowledge in a courtroom setting. After the trial, supervision/management will assess the trainee's ~~individual's~~ performance as either satisfactory or unsatisfactory. If the trainee's ~~individual's~~ performance is determined to be unsatisfactory, steps must be taken to effect appropriate action.

1.2.9 Upon successful completion of the mock court, Phase I training is complete. ~~A training certificate will be prepared by the Forensic Quality Manager, signed by the Director, and forwarded to the newly certified examiner. The certificate will document that the examiner is certified in the appropriate~~

~~discipline or category of testing. Notice of certification will be placed in the examiner's permanent training file.~~

1.2.10 In Phase II training, the trainee will perform casework tasks under the direct supervision of the principal instructor. The trainee will document all work according to all applicable CCBI Crime Laboratory policies and procedures. The principal instructor will be responsible for supervising and reviewing all casework performed by the trainee and issuing reports. The trainee may be included as an author of the report with a clear indication that they are a trainee.

1.2.~~10~~11 To complete Phase II training, the trainee must successfully complete a practical competency test; complete a written test report; and complete an oral examination conducted by at least the principal instructor, Technical Leader, and Forensic Quality Manager or Deputy Director. Upon completion of the Phase II training, the trainee will have attained the necessary knowledge, skills, and abilities to independently perform casework. ~~Regardless of how well a new examiner handled their assignments during the training period, there follows a period of adjustment.~~

1.2.12 Phase III training will last for a period of at least six (6) months ~~following certification by CCBI~~. During Phase III Training, 100% of the examiner's casework will be technically reviewed. If no significant technical discrepancies that could affect the reliability of the examiner's conclusion are noted during this time, Phase III training is completed at the end of this six (6) month period.

1.3 Assessment/Training of Experienced Personnel

1.3.1 The responsibility for assessing the degree of qualifications of newly hired personnel who have previously successfully completed a qualifying training program of instruction in digital and multimedia evidence shall lie with the ~~Supervisor of the~~ Forensic Computer Unit Technical Leader or designee with approval from the Forensic Quality Manager. Under the circumstances outlined below, previous training and experience may substitute for the training tasks contained in this manual (e.g. Phase I and Phase II training) but not Phase III training.

1.3.2 The training tasks in this manual may be skipped for a previously trained examiner who has demonstrated to the Technical Leader a comprehensive knowledge of the training task's subject matter, and with the approval of the Forensic Quality Manager.

1.3.3 A previously trained examiner may substitute the entirety of this training manual by providing proof of successful completion of a forensic computer examination course of study. In order to substitute for the entirety of the training specified in this manual, the qualifying course must have been formally structured; must have covered all appropriate facets of the sub discipline in which the trainee is being qualified; and must have been administered by a reputable organization (or individual).

1.3.4 Methods of verifying the completion of prior training will include:

- Completion of sufficient unknown samples to cover the anticipated spectrum of assigned duties and evaluate the individual's ability to perform proper testing methods;

- A written test report to demonstrate the individual's ability to properly convey results and/or conclusions and the significance of those results/conclusions; and
- A written or oral examination to assess the individual's knowledge of the discipline, category of testing, or task being performed.

1.3.5 Newly hired personnel shall not be considered for certification by the Director to begin any actual casework until each has successfully completed at least one (1) competency test and one (1) mock trial and/or written or oral examination.

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
7/14/14	2	Incorporation of revisions to LAPM22

Chapter 2: TRAINING TASK #1: COMPUTER FORENSICS BASICS

2.1 Training Objectives

Familiarize the trainee with the basic principles of imaging hard drives, safety, and the instrumentation and equipment used in the Forensic Computer Unit.

2.2 Training Methods

2.2.1 Lectures

2.2.1.1 Wiping digital media and its function
2.2.1.2 Hashing digital media and its function
2.2.1.3 Imaging of digital media and its purpose
2.2.1.4 Ethical obligations

2.2.2 Required Reading

2.2.2.1 *Best Practices for Seizing Electronic Evidence v3*, United States Secret Service, October 2006
2.2.2.2 *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, U.S. Department of Justice National Institute of Justice, April 2008
2.2.2.3 Scientific Working Group on Digital Evidence, Best Practices for Computer Forensics (current version)
2.2.2.4 Scientific Working Group on Digital Evidence, Best Practices for GPS Devices (current version)
2.2.2.5 Scientific Working Group on Digital Evidence, Best Practices for Mobile Phone Examinations (current version)
2.2.2.6 Scientific Working Group on Digital Evidence, Data Integrity within Computer Forensics
2.2.2.7 Scientific Working Group on Digital Evidence, Position Paper on Standards and Controls
2.2.2.8 Scientific Working Group on Digital Evidence, Recommendations for Validation Testing
2.2.2.9 Scientific Working Group on Digital Evidence, SWGDE-SWGIT Glossary
2.2.2.10 Chapter 1 of *Criminalistics: an Introduction to Forensic Science*, Richard Saferstein

2.2.3 Trainee will successfully complete an ethics course approved by the Forensic Quality Manager.

2.3 Method of Testing

2.3.1 Trainee will demonstrate the necessary safety considerations when handling computer evidence or digital devices and will identify the possibility of evidence or data destruction.

2.3.2 Trainee will identify different types of hard drives and different connection types such as PATA, SATA, mSATA, SCSI, SAS, ZIF, etc.

2.3.3 Trainee will explain the documentation required to complete the chain of custody.

2.3.4 Trainee will explain how a forensic image is obtained and how to verify that the forensic image is accurate and complete.

2.3.5 Trainee will explain the operation of the forensic imaging software programs FTK Imager, EnCase, Helix, LinEn, Paladin, Raptor, SPADA, etc.

2.3.6 Trainee will explain the examiner's ethical obligations related to objectivity, validated scientific principles, reporting inculpatory and exculpatory findings, and issuance of conclusions and opinions.

2.4 Criteria for Successful Completion

2.4.1 Demonstration

The principal instructor will observe the trainee's performance of related techniques from beginning to end, and all notes will be generated by the trainee. These requirements will demonstrate that the trainee complied with all of the required procedures.

2.4.2 Oral/Written Examination

2.4.2.1 Oral review on each technique and procedure utilized in this section.

2.4.2.2 Various techniques and terms to be defined both orally and written.

2.4.2.3 Written papers(s) on related topics to be assigned and approved by the principal instructor, Technical Leader, and/or Supervisor. This will be considered as a technical research paper.

2.5 Estimated Training Time

See Appendix: Forensic Computer Unit Training Outline

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025
7/14/14	2	Incorporation of revisions to LAPM22

Chapter 3: TRAINING TASK #2: IMAGING HARD DRIVES

3.1 Objectives

Familiarize the trainee with process of obtaining a forensic image of a hard drive.

3.2 Training Methods

3.2.1 Lectures

3.2.1.1 Proper removal of media
3.2.1.2 Differences between hardware, firmware, and software write blocking
3.2.1.3 Target drive preparation
3.2.1.4 Hashing digital media and its function
3.2.1.5 Proper method for examining BIOS settings

3.2.2 Required Reading

3.2.2.1 EnCase User's Guide
3.2.2.2 FTK Imager User Guide
3.2.2.3 Tableau User Guides for T4, T8, and T35es

3.3 Method of Testing

Trainee will wipe a hard drive of all data and format it for use as a target drive.

Given a hard drive that has been previously verified to contain no evidence and contains a known MD5 hash value, the trainee will connect the hard drive to a write-blocking device and acquire the hard drive using a minimum of two (2) forensic tools. The trainee will explain the hazards of altering digital evidence storage devices and the possibility of destroying data.

The trainee will correctly attach the hard drive, correctly attach the write blocker, acquire the data, and verify the information using hash algorithms.

Once the hard drive is acquired and the forensic image verified, the trainee will demonstrate the proper way to exit the forensic software and disconnect the hard drive. The trainee will then return the hard drive to its original condition.

The trainee will document the process correctly noting all dates and times, device information, processes used, software and hardware used, and any problems or errors during the forensic imaging process.

3.4 Criteria for Successful Completion

3.4.1 Demonstration

3.4.1.1 Trainee must use all instrumentation and equipment properly and obtain a forensic image without altering the data on the original hard drive.

3.4.1.2 The principal instructor will observe the trainee's performance of related techniques from beginning to end, and all notes will be generated by the trainee. These requirements will demonstrate that the trainee complied with all of the required procedures.

3.4.2 Oral/Written Examination

3.4.2.1 Oral review on each technique and procedure utilized in this section.

3.4.2.2 Various techniques and terms to be defined both orally and written.

3.4.2.3 Written papers(s) on related topics to be assigned and approved by the principal instructor, Technical Leader, and/or Supervisor. This will be considered as a technical research paper.

3.5 Estimated Training Time

See Appendix: Forensic Computer Unit Training Outline

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 4: TRAINING TASK #3: IMAGING REMOVABLE MEDIA

4.1 Objectives

The objectives of this training assignment are to familiarize the trainee with process of obtaining a forensic image of removable media such as USB drives, CDs and DVDs, and flash media.

4.2 Training Methods

4.2.1 Lectures

4.2.1.1 Proper removal of media
4.2.1.2 Proper method for removable media imaging

4.2.2 Required Reading

4.2.2.1 CD/DVD Inspector User Guide
4.2.2.2 EnCase User's Guide
4.2.2.3 FTK Imager User Guide

4.3 Method of Testing:

Trainee will wipe a hard drive of all data and format it for use as a target drive.

Given removable media that has been previously verified to contain no evidence and contains a known MD5 hash value, the trainee will write-block the media and acquire the media using a minimum of two (2) forensic tools. The trainee will explain the hazards of altering digital evidence storage devices and the possibility of destroying data.

The trainee will correctly attach the media, correctly attach the write blocker, acquire the data, and verify the information using hash algorithms.

Once the media is acquired and the forensic image verified, the trainee will demonstrate the proper way to exit the forensic software and disconnect the media. The trainee will then return the media to its original condition.

The trainee will document the process correctly noting all dates and times, media information, processes used, software and hardware used, and any problems or errors during the acquisition.

4.4 Criteria for Successful Completion

4.4.1 Demonstration

4.4.1.1 Trainee must use all instrumentation and equipment properly and obtain a forensic image without altering the data on the original removable media.

4.4.1.2 The principal instructor will observe the trainee's performance of related techniques from beginning to end, and all notes will be generated by the trainee. These requirements will demonstrate that the trainee complied with all of the required procedures.

4.4.2 Oral/Written Examination

4.4.2.1 Oral review on each technique and procedure utilized in this section.

4.4.2.2 Various techniques and terms to be defined both orally and written.

4.4.2.3 Written papers(s) on related topics to be assigned and approved by the principal instructor, Technical Leader, and/or Supervisor. This will be considered as a technical research paper.

4.5 Estimated Training Time

See Appendix: Forensic Computer Unit Training Outline

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 5: TRAINING TASK #4: IMAGING A MACINTOSH COMPUTER WITHOUT HARD DRIVE REMOVAL

5.1 Objectives

To familiarize the trainee with process of obtaining a forensic image of a hard drive that cannot be removed from a Macintosh computer. The trainee will identify the issues with imaging a Macintosh computer without removing the digital media, how to ensure there is no Windows partition on the media, options if a Windows partition is located, and when hardware or software write blockers are needed.

5.2 Training Methods

5.2.1 Lectures

5.2.1.1 File system differences between Macintosh and Windows computers
5.2.1.2 Relevance of Power PC-based versus Intel-based Macintosh operating systems
5.2.1.3 Dangers of dual boot partitions and disk arbitration
5.2.1.4 Target disk mode
5.2.1.5 fstab configuration file
5.2.1.6 Proper use of forensically sound Linux boot CDs

5.2.2 Required Reading

5.2.2.1 EnCase User's Guide
5.2.2.2 FTK Imager User's Guide
5.2.2.3 *Acquisition*, The Apple Examiner, URL: www.appleexaminer.com/MacsAndOS/Img_Pwds/Acquisition/acquisition.html
5.2.2.4 *How To: Forensically Sound Mac Acquisition in Target Mode*, SANS Computer Forensics and Incident Response, February 2011, URL: http://computer-forensics.sans.org/blog/2011/02/02/forensically-sound-mac-acquisition-target-mode

5.3 Method of Testing:

Trainee will wipe a hard drive of all data and format it for use as a target drive.

Given a Macintosh computer that contains a hard drive that has been previously verified to contain no evidence and contains a known MD5 hash value, the trainee will obtain a forensic image of the Macintosh hard drive without removing it from the computer. The trainee will use two methods: a forensically sound Linux boot disc and Target Disk Mode. The trainee will explain the hazards of altering digital evidence storage devices and the possibility of destroying data.

The trainee will correctly communicate with the Macintosh hard drive, obtain a forensic image of the data, and verify the information using hash algorithms.

Once the hard drive is acquired and the forensic image verified, the trainee will demonstrate the proper way to exit the forensic software and disconnect the Macintosh computer. The trainee will then return the Macintosh computer to its original condition.

The trainee will document the process correctly noting all dates and times, media information, processes used, software and hardware used, and any problems or errors during the acquisition.

5.4 Criteria for Successful Completion

5.4.1 Demonstration

5.4.1.1 Trainee must use all instrumentation and equipment properly and obtain a forensic image without altering the data on the original hard drive.

5.4.1.2 The principal instructor will observe the trainee's performance of related techniques from beginning to end, and all notes will be generated by the trainee. These requirements will demonstrate that the trainee complied with all of the required procedures.

5.4.2 Oral/Written Examination

5.4.2.1 Oral review on each technique and procedure utilized in this section.

5.4.2.2 Various techniques and terms to be defined both orally and written.

5.4.2.3 Written papers(s) on related topics to be assigned and approved by the principal instructor, Technical Leader, and/or Supervisor. This will be considered as a technical research paper.

5.5 Estimated Training Time

See Appendix: Forensic Computer Unit Training Outline.

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 6: TRAINING TASK #5: PREVIEWING DIGITAL MEDIA

6.1 Objectives

Familiarize the trainee with the process of forensically previewing digital media.

6.2 Training Methods

6.2.1 Lectures

6.2.1.1 Proper use of forensically sound Linux boot CDs
6.2.1.2 Proper use of crossover cable
6.2.1.3 Proper use of write blockers
6.2.1.4 Disk configuration overlays and hidden disk areas

6.2.2 Required Reading

6.2.2.1 EnCase User's Manual
6.2.2.2 Scientific Working Group on Digital Evidence, Capture of Live Systems
6.2.2.3 *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, U.S. Department of Justice National Institute of Justice, April 2004

6.3 Method of Testing:

Trainee will wipe a hard drive of all data and format it for use as a target drive.

Given a hard drive that has been previously verified to contain no evidence and contains a known MD5 hash value, the trainee will write-block thee hard drive and preview the digital data using at least two (2) methods: a forensically sound Linux boot disc and hard drive removal. The trainee will explain the hazards of altering digital evidence storage devices and the possibility of destroying data.

The trainee will correctly communicate with the hard drive, preview the data, and determine if further analysis is warranted for information that may be deleted or hidden. The trainee will review the data structures, images, documents, and other files to triage digital evidence.

Once the hard drive has been previewed, the trainee will demonstrate the proper method to exit the preview platform and disconnect the hard drive. The trainee will then return the hard drive to its original condition.

The trainee will document the process correctly noting all dates and times, device information, processes used, software and hardware used, and any problems or errors during the preview.

6.4 Criteria for Successful Completion

6.4.1 Demonstration

6.4.1.1 Trainee must use all instrumentation and equipment properly and conduct the forensic preview without altering the data on the original hard drive.

6.4.1.2 The principal instructor will observe the trainee's performance of related techniques from beginning to end, and all notes will be generated by the trainee. These requirements will demonstrate that the trainee complied with all of the required procedures.

6.4.2 Oral/Written Examination

6.4.2.1 Oral review on each technique and procedure utilized in this section.

6.4.2.2 Various techniques and terms to be defined both orally and written.

6.4.2.3 Written papers(s) on related topics to be assigned and approved by the principal instructor, Technical Leader, and/or Supervisor. This will be considered as a technical research paper.

6.5 Estimated Training Time

See Appendix: Forensic Computer Unit Training Outline.

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

Chapter 7: TRAINING TASK #6: ANALYZING DIGITAL MEDIA

7.1 Objectives

Familiarize the trainee the trainee with process of analysis of digital media.

7.2 Training Methods

7.2.1 Lectures

7.2.1.1 Identifying disk configuration overlays and hidden disk areas
7.2.1.2 Accessing deleted, overwritten, or compressed files and folders
7.2.1.3 Addressing passwords and encryption
7.2.1.4 Proper methods for data carving
7.2.1.5 Relevance of the Windows Registry
7.2.1.6 Proper methods for suspect image restoration

7.2.2 Required Reading

7.2.2.1 EnCase User's Manual
7.2.2.2 *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, U.S. Department of Justice National Institute of Justice, April 2004, URL: www.ncjrs.gov/pdffiles1/nij/199408.pdf

7.3 Method of Testing:

Trainee will wipe a hard drive of all data and format it for use as a target drive.

Given a known forensic image of a hard drive that has been previously verified with a known MD5 hash value and that contains no actual evidence, the trainee will load the forensic image into a forensic analysis platform such as Encase and analyze the data for items of contraband and or evidence.

The trainee will correctly load the known forensic image into the forensic program and verify the MD5 hash value of the loaded forensic image. The trainee will then utilize the forensic software and recover any deleted folders, verify file signatures, and obtain hash values for all files. The trainee should review the data structures and pay attention to large file sizes and possibly hidden data reporting with incorrect file extensions.

Once the image has been thoroughly examined and all items of contraband or evidence located, the trainee will demonstrate the proper way to bookmark and report on the findings. Once the bookmarks are created, the trainee will export the bookmarks and exit the program without losing any recovered data.

The trainee will document the process correctly noting all dates and times, device information, processes used, software and hardware used, and any problems or errors during the preview.

7.4 Criteria for Successful Completion

7.4.1 Demonstration

7.4.1.1 Trainee must use all instrumentation and equipment properly and recover all data items of evidentiary interest.

7.4.1.2 The principal instructor will observe the trainee's performance of related techniques from beginning to end, and all notes will be generated by the trainee. These requirements will demonstrate that the trainee complied with all of the required procedures.

7.4.2 Oral/Written Examination

7.4.2.1 Oral review on each technique and procedure utilized in this section.

7.4.2.2 Various techniques and terms to be defined both orally and written.

7.4.2.3 Written papers(s) on related topics to be assigned and approved by the principal instructor, Technical Leader, and/or Supervisor. This will be considered as a technical research paper.

7.5 Estimated Training Time

See Appendix: Forensic Computer Unit Training Outline

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025

APPENDIX: FORENSIC COMPUTER UNIT TRAINING OUTLINE

CCBI Crime Laboratory Division Forensic Computer Unit		
Forensic Computer Unit Training Outline		
Training Areas	CCBI Standard Operating Procedures	
	CCBI Crime Laboratory Administrative Procedures	
	CCBI Crime Laboratory Forensic Science Quality Manual	
	Computerized records management systems	
	Chain of custody	
	Evidence handling procedures	
	Digital evidence acquisition	
	Digital evidence analysis	
	Digital evidence reporting	
	Courtroom testimony	
In-House Training		
		Anticipated completion timeline from hire date:
CCBI Standard Operating Procedures; Crime Laboratory Administrative Procedures and Quality Manual	Read all current SOPs and Administrative Orders and ISO documentation	2-3 weeks
Computerized records management systems	Obtain logon information and training on computerized records management systems	3 weeks
Chain of custody and evidence handling procedures	Read SOPs, Forensic Science Quality Manual, and Evidence Submission Guide; receive individualized training with unit supervisor or designee on proper evidence handling procedures.	3 weeks
Digital evidence acquisition	Read all applicable material on digital evidence acquisition using Windows, Linux, and Mac OS. Utilize write protection equipment such as software and hardware write blockers.	4-8 weeks
Digital evidence analysis	Properly analyze digital evidence using various proven and tested forensic tools.	8-40 weeks
Digital evidence reporting	Properly report on located digital evidence using proper terminology, hash analysis, and location on original digital evidence.	8-40 weeks
Courtroom testimony	Review evidence and participate in moot court. Complete a CV that includes training and certifications.	40-52 weeks

Outside Training		
National White Collar Crime Center	1. Cybercop 101-Basic Data Recovery and Acquisition 2. Cybercop 201-Intermediate Data Recovery and Analysis 3. Cybercop 305-Windows NT File System 4. Cybercop 310-Windows NT Operating System 5. Cybercop 225-Macintosh Triage and Imaging	1-52 weeks
EnCase	1. EnCase Basic 2. Encase Intermediate	26-104 weeks
IACIS	1. Basic Computer Forensic Examiner	52-104 weeks

Revision History		
Effective Date	**Version Number**	**Reason**
January 1, 2013	1	New Policy to comply with ISO 17025