North Carolina Department of Secretary of State Digital Forensic Analyst Training Manual

Issued: Jan 15, 2013
Revision: 1

Table of Contents

End of Table of Contents

Issued by: Quality Manager Auth: SPruett 5/23/2018
All printed copies are uncontrolled

Digital Forensic Laboratory
Analyst Training Program

The Digital Forensic Laboratory Analyst Trainee training program (DFLATP) is designed to be modular. This means that units do not have to be completed in sequential order. However, all elements within a unit shall be completed before starting Phase II of the Digital Forensic Analyst Training Program (DFLATP). The trainee will be given an initial evaluation to gauge their pre-existing knowledge and experience in the domain of Phase I training objectives.

Phase I Training

Several external training courses will be required of a Phase I to successfully complete the ATP training program. The courses described below are not required to be taken in the order they are listed, nor within specific training units. These courses, or proof of completing equivalent curriculum and/or work experience either during or before the training program, are required in Phase I training in ATP:

"Basic Data Recovery and Analysis" – The National White Collar Crime Center
Regional or International conferences focusing on issues in computer forensics
"Encase Intermediate" – Guidance Software
"Encase Advanced" – Guidance Software
Courses from the "Advanced Data Recovery and Analysis" series – The National White Collar Crime Center

Unit 1: Laboratory Familiarization

1. Objectives
1.1 To familiarize the trainee with all aspects of the laboratory environment.
1.2 To inform the trainee of security issues and access privileges.
1.3 To inform the trainee of important issues pertaining to administration and management of the laboratory and the department.

2. Topics
2.1. Security Access
Discuss with the trainee all aspects pertaining to security access to the particular building in which the trainee will be working.
Arrange to have appropriate security access privileges obtained for trainee including the issuance of security access badge, key, etc.
Demonstrate the proper use of the access badge, key, etc.
Assign the trainee to read and be familiar with department policies concerning security access issues.
2.2. Facilities
Take the trainee on a complete tour of the facilities, including the location of restrooms, refreshments, break rooms, exercise areas, etc.
2.3. Chain of Command
2.4. Personnel Issues
Complete Departmental In-Processing Procedures.
2.5. Familiarize Trainee with Department's Digital Forensic Lab Quality Manual (DFLQM) and Digital Forensic Laboratory Administrative Procedures Manual (DFLAPM).
2.6. Introduce Department Laboratory Information Management System (LIMS) Network.
Establishing Account
Demonstrate Access Capabilities
Security Issues with LIMS
2.7. Enroll Trainee into Department's New Member Orientation Program
2.8. Overview of other laboratory disciplines
2.9. Ethics
3. Method of Testing
Trainees will be presented with a review upon completion of the above listed topics.
Trainees will be asked to demonstrate their understanding of this material through oral questioning exercises at the end of the unit.

4. Training Methods
Tours of the necessary Departmental Laboratory facilities and Departmental offices will be conducted by qualified NC Department of Secretary of State Personnel.

Additional guidance will be provided by Training Committee Members to introduce the trainee to the proper personnel and Departmental resources.

5. Required Reading

Introductory Departmental Literature, and Departmental and Building policies presented in the DFLQM, DFLAPM, and Standard Operating Procedures (DFLSOP)

Ethics in the Forensic Sciences: Value Based Decision Making presented by Midwest Forensics Resource Center - Dan Gunnell (DVD)

or

Barnett, Peter D.; Ethics in Forensic Science: Professional Standards for the Practice of Criminalistics, CRC Press, 2001

1. Est. Training Time: Two Weeks

Unit 2 Evidence Handling Procedures

1. Objectives

. To familiarize the trainee with all aspects of evidence handling within the laboratory environment.
. To insure the competency of the trainee in evidence handling procedures.
. To prepare the trainee for a diverse set of challenges in encountering crime scenes and identifying the optimal solution(s) to secure computer data in such scenarios.

2. Topics

2.1. Laboratory Evidence

2.2. NCSOS Laboratory Case Intakes

. Case Tracking Form (CTF) Required Information
. Web Prelog requirements

2.3. Case Transfer Procedures

. Shipping, Transport & Courier Resources
. Multi-Section Analyses
. 2.4. Case Dispositions

Return Policies

2.5. Evidence

. Interpreting the Scope of Search Warrants pertaining to Seizing Automated Equipment
. Approaching Consent Searches
. Properly Sealing and Documenting Computer Evidence Discovered at Crime Scenes
. Handling, Marking, Sealing, Storage and Retention
. Tracking in LIMS
. Auditing

3. Method of Testing

. Trainees will be asked to show their mastery of this material through properly demonstrating how to: utilizing a mock search warrant and consent search scenarios, complete an actual case intake and evidence transfer (under supervision from qualified personnel), properly utilize the Digital Forensic Laboratory Evidence Section, and perform an evidence audit of the Digital Forensic Lab.

4. Training Methods

. Individualized demonstrations in the laboratory
. Additional guidance will be provided by qualified personnel to familiarize the trainee with departmental evidence handling procedures.

5. Required Reading
A mastery of DFLSOP, Evidence Submission and DFLQM procedures for case file and evidence handling
“The Handbook of Computer Crime Investigation” by Eoghan Casey
“Incident Response” by Mandia & Prosise Chapters 1 – 5
“Digital Evidence and Computer Crime” by Eoghan Casey Chapters 1 - 4
Review Federal Guidelines on Search and Seizure

1. Est. Training Time: Four Weeks

Unit 3 Case File Handling

1. Objectives

To instruct the trainee on proper methods of organizing the contents of individual case files.
To familiarize the trainee with the Laboratory's case file organization and retention schedule.
To familiarize the trainee with Evidence Examination Policy.
To demonstrate the functionality of LIMS and obtain access privileges.
To instruct on case file note-taking requirements and policies.
To instruct the trainee on the court structure and analytical testimony.

2. Topics

2.1. Case Folder
2.1.1. Contents
2.1.2. Organization
2.1.3. Files Room
. Organization
. Retention Schedule
. 2.2. Laboratory Information Management System (LIMS)
. 2.2.1. Managing the User Account
. 2.2.2. Mastering Required Steps in LIMS for Evidence and Workload Tracking
. Submission Assignments
. Submission Management
. Submission Dispositions
. 2.3. Note Taking and Tracking of Analytical Procedures
. Rationale behind Best Practices
. 2.4. The Courtroom
. Structure of the Court System
. Courtroom Demeanor and Testimony

3. Method of Testing

. Trainees will be asked to locate several case files from the Digital Forensic Lab records room and provide information to the instructor that is documented in the case file.
. Trainees will be presented with a hypothetical caseload, with individual submissions and types of investigations. They will then develop a priority list of which submissions to analyze first, and at what level to cease further analytical efforts.
. Trainees will be quizzed on the court structure and will field questions from mock courtroom scenarios.

4. Training Methods

. Hands on analyses of case folders, analytical processes and proper tracking of procedures in analyzing evidence submissions.

. Trainees will be guided through common LIMS screens and procedures by training committee members.
. Trainees will visit the local state and federal court systems (if available) and observe trials, including some which involve expert forensic testimony.

5. Required Reading:A mastery of DFLSOP, DFLQM and DFLAPM procedures for case file and evidence handling State of North Carolina Judicial System Overview
6. Est. Training Time: Four Weeks

Unit 4 Assigned Resources

1. Objectives

To disclose to the trainee what equipment and resources will be assigned.
To instruct the trainee on the proper handling of assigned resources.

2. Topics

2.1. Hardware
2.2. Software
. Licensing
. 2.3. Media
. 2.4. Quality Control Procedures
. 2.5. Accountability
. 2.6. Purchasing Requests

1. Method of Testing Oral Review and Questioning

4. Training Methods

Assist with developing a list of the hardware and software required for a model laboratory.
Assist with Developing a Digital Forensic Lab Equipment Replacement Schedule.
Review and Apply Regular Hardware QA Procedures.

1. Required Reading Relevant NC SOS DFLQM, DFLAPM and QA Documentation

1. Est. Training Time Three Weeks

Unit 5 Personal Computer Hardware

1. Objectives

To provide the trainee with an in-depth knowledge of computer hardware, networking and peripheral components, and their proper operation.

2. Topics

2.1. Computer Hardware

2.1.1. The trainee should attend (4 day minimum) courses on the following topics:

. Computer Hardware, Troubleshooting and/or Repair
. Networking Technologies
. Forensic Data Recovery Platforms and Procedures

. 2.2. Peripherals

. The instructor should demonstrate to the trainee each of the peripheral drives and components that are currently in use in the Laboratory.

3. Method of Testing

External courses will have proficiency tests at end of curriculum to test the student's mastery of the material.

Trainee will demonstrate their understanding of configuring and utilizing section hardware during supervised analytical exercises and bench analyses within the Laboratory.

4. Training Methods

Attend external training courses as prescribed in assessment memorandum developed for Trainee

Study material in assigned readings

Assist with bench analyses within the Laboratory

5. Required Reading

5.1. How Computers Work – Ron White

5.2. Selected readings from:

. New Inside the PC – Peter Norton
. The Computer Glossary – Alan Freedman
. "Hacking Exposed: Network Security" by Stuart McClure, *et al*.

1. Est. Training Time Seven weeks

Unit 6 Personal Computer Software

1. Objectives

To provide the trainee with an in-depth knowledge of current operating systems, end user applications and related utility programs.

2. Topics

2.1. Operating Systems

. The trainee must attend at least one support course for the predominant operating system currently in use in the section. The trainee will be required to demonstrate competency in this assigned operating system.

. 2.2. Applications

. The trainee must become familiar with several applications and demonstrate competency in these applications during this training phase. Typical applications include word processing, spreadsheets, databases, graphics, communications, etc. The purpose is to expose the trainee to as many applications as possible within time and funding constraints.

. 2.3. Utility Programs

. The trainee will understand and demonstrate competency in all currently utilized utility programs in the section. The trainee will read and understand pertinent portions of the user's guide for each utility in an effort to become proficient in the operation of each program.

. 3. Method of Testing

. 3.1. External Courses

. Trainee will demonstrate their understanding of configuring and applying section software during supervised analytical exercises and bench analyses within the Digital Forensic Lab

4. Training Methods

Attend external training courses as prescribed in trainee assessment.
Assist with bench analytical exercises and bench analyses within the Laboratory.

5. Required Reading

Software Documentation for Operating Systems, End User Programs and Utility Applications

6. Est. Training Time Seven weeks

Unit 7 Examination Procedures

The trainee will process multiple types of devices, media, and file allocation systems using different software and analytical procedures. The trainee will learn how to logically integrate the techniques, software, and hardware from Units 5 and 6. Additionally, the trainee will process the same device using different techniques and software to compare and contrast results from each tool and technique. The trainee's level of competency will be monitored on a regular basis by their training committee.

1. Est. Training Time Seven weeks

Assessment of trainee for graduating to Phase II of the Training Program

Phase II

Unit 8 Supervised Casework and Reporting

Phase II, also known as "Supervised Casework", should consist of taking on a wide variety of casework spanning multiple types of devices, media, file allocation systems, software and analytical procedures. A written report shall be completed to properly convey results and/or conclusions. The trainee's level of competency will be determined on a regular basis by their trainer.

1. Est. Training Time Twelve weeks

Unit 9 Courtroom Testimony and Demeanor

1. Objectives

. To instruct the trainee so they may demonstrate appropriate courtroom appearance, demeanor and ability to render testimony.

. To discuss important considerations of courtroom testimony.

. 2. Method of Testing

. Summative questioning and an internal moot court.

3. Training Methods

. Lecture, independent study, demonstration and simulation.

. 4. Required Reading

. "A Guide to Forensic Testimony" by Smith and Bace

. State of North Carolina Judicial System Overview

. 5. Est. Training Time Two Days supplemented by discussion and training exercises during other Units

Unit 10 Mock Trial

Training Monitor

Analyst Trainee: Primary Trainer:

Unit 1: Laboratory Familiarization
Date Completed: _____ Evaluator: _____

Unit 2: Evidence Handling Procedures
Date Completed: _____ Evaluator: _____

Unit 3: Case File Handling
Date Completed: _____ Evaluator: _____

Unit 4: Assigned Resources
Date Completed: _____ Evaluator: _____

Unit 5: Personal Computer Hardware
Date Completed: _____ Evaluator: _____

Unit 6: Personal Computer Software
Date Completed: _____ Evaluator: _____

Unit 7: Examination Procedures
Date Completed: _____ Evaluator: _____

Unit 8: Supervised Casework
Date Completed: _____ Evaluator: _____

Unit 9: Courtroom Testimony and Demeanor
Date Completed: _____ Evaluator: _____

Unit 10: Moot Court
Date Completed: _____ Evaluator: _____