Department of Forensic Science

DIGITAL & MULTIMEDIA EVIDENCE SECTION TRAINING MANUAL

TABLE OF CONTENTS

1 Introduction

1.1 Purpose and Scope
1.2 Coordination of the Program
1.3 Training Period
1.4 Training Goals
1.5 Instructions to the Trainee
1.6 Instructions to Training Coordinators
1.7 Mock Trials
1.8 Guidelines for the Competency Examination
1.9 Assessment/Training of Experienced Personnel
1.10 Transition from Trainee to Examiner

2 Orientation

2.1 Minimum Requirements

3 Computer and Mobile Device Analysis

Part I: Computer / Digital Storage Device Analysis

3.1 Objectives
3.2 Methods of Instruction
3.3 Lectures and Discussions
3.4 Required Reading
3.5 Study Questions
3.6 Practical Exercises
3.7 Evaluation

Part II: Mobile Device Analysis

3.8 Objectives
3.9 Methods of Instruction
3.10 Lectures and Discussions
3.11 Required Reading
3.12 Study Questions
3.13 Practical Exercises
3.14 Evaluation

4 Video Analysis

4.1 Objectives
4.2 Methods of Instruction
4.3 Lectures and Discussions
4.4 Required Reading
4.5 Study Questions
4.6 Practical Exercises
4.7 Evaluation

5 Report Writing and Testimony

5.1 Objectives
5.2 Methods of Instruction
5.3 Required Reading
5.4 Assignments
5.5 Evaluation

1 INTRODUCTION

1.1 Purpose and Scope

1.1.1 The purpose of this manual is to provide a uniform coordination of the training of forensic scientists in the Digital & Multimedia Evidence (DME) Section. This work is intended to be used in a formal training program that will establish a minimum standard of professional competency in the computer and mobile device analysis and video analysis sub-disciplines of digital and multimedia evidence.

1.1.2 Certain inherent qualities of the analysis of digital evidence prohibit the establishment of a rigid set of standard training procedures to cover each and every type of digital evidence; therefore, enough latitude has been given to allow for independent thought and individual freedom in selecting appropriate courses of action. The available options will be addressed within the established protocols for the specific sub-discipline. Upon completion of these courses, the trainee will be thoroughly familiar with the options available to handle most items of evidence that will be encountered.

1.1.3 The sequence in which the tasks are presented in the outline should not necessarily be considered as a mandatory order of instruction.

1.2 Coordination of the Program

1.2.1 The training program will be coordinated by the Training Coordinator (TC). The TC will be an experienced examiner designated by the Section Supervisor in consultation with the Program Manager (PM).

1.2.2 The TC will be responsible for the overall training, but may delegate certain duties and blocks of instruction to other qualified examiners.

1.3 Training Period

1.3.1 The training of a new examiner, depending on their assigned sub-disciplines, will be broken into two phases: computer and mobile device analysis and video analysis.

1.3.2 The length of the training period will be left to the determination of the Section Supervisor with approval of the PM, and will vary depending on the trainee's experience and education. For an unqualified trainee, it is anticipated that full-time training for the video analysis module can be completed within 12 months and training for the computer and mobile device analysis can be completed within 18 months. Training for each sub-discipline is to include successful completion of the competency examination. The qualifications of the trainee will be evaluated and modifications will be made to the training program, as appropriate, with approval by the PM.

1.4 Training Goals

Upon completion of the training program, the trainee shall have gained the following:

- The basic knowledge of the sub-discipline;
- The knowledge of the principles and practices of the sub-discipline;
- The knowledge of the theory and applications of the variety of equipment and specialized techniques used to acquire and analyze digital and multimedia evidence within a specific sub-discipline;
- The ability to perform accurate, forensic acquisition and analysis independently and proficiently;
- The ability to skillfully present and defend analytical findings in courts of record.

1.5 Instructions to the Trainee

1.5.1 The trainee is expected to maintain a training file of information compiled on the specific sub-discipline in which they are training. This file is to be reviewed by the TC upon completion of an assigned training module.

1.5.2 The written answers to the study questions listed in each section shall be maintained in the training file and can be used as reference material once the trainee is qualified as an examiner; therefore, references are to be listed for each answer whenever possible.

1.5.3 References listed as "Required Reading" are required for an adequate understanding of the subject matter. Document in the training file the date the reading was completed.

1.5.4 Under the direct supervision of a qualified examiner, the trainee will assist with casework throughout the training period. This will familiarize the trainee with different forms of case evidence, packaging requirements, analytical techniques, and note-taking. Document in the training file the case number and date of the activities.

1.5.5 The trainee shall provide a monthly written progress report to the TC. This report shall include a weekly log of training activities and completed assignments.

1.6 Instructions to Training Coordinators

1.6.1 The intent of this manual is to provide a guide that will ensure every examiner receives training in certain basic principles and fundamentals necessary to complete acquisition and analyses of digital and multimedia evidence.

1.6.2 The TC is responsible for maintaining the Department's training program documentation during the training period. The TC shall document on the Digital & Multimedia Evidence Training Module Documentation Form (DFS Document 242-F200), with dates and initials, the successful completion of each required training module. If any module is not completed for any reason, it must be explained in the training file and approved by the PM.

1.6.3 Modules may be skipped for previously trained and qualified examiners who have demonstrated to the Section Supervisor and/or TC a comprehensive knowledge of the section's subject matter with the approval of the PM.

1.6.3.1 The Section Supervisor and/or TC will submit a written recommendation to the PM outlining the sections which may be omitted or modified, and the justification for doing so.

1.6.3.2 A copy of the approved recommendation will be placed in the training file.

1.6.4 If the trainee cannot meet the expected criteria during the period allowed for training, the PM and/or Director of Technical Services should be consulted to determine the appropriate course of action.

1.6.5 The TC shall submit a monthly written progress report of the trainee to the PM and the Laboratory Director, in accordance with Quality Manual (QM).

1.7 Mock Trials

1.7.1 The TC is responsible for ensuring that the trainee is thoroughly prepared for legal questioning. This can be done by a combination of practice mock trials, prearranged as well as impromptu question and answer sessions and observation of courtroom testimony given by experienced examiners.

1.7.1.1 Documentation, to include dates, initials and brief description of content, shall be included in the training file.

1.7.2 The scheduling of practice mock trials is to be done by the TC. These are to be conducted throughout the training period.

1.8 Guidelines for the Competency Examination

1.8.1 Practical Test

The practical test is a mock case, intended to simulate an average case in difficulty and complexity. There should be clear expected outcomes that have been validated by a qualified examiner. The test shall be approved by the PM prior to being presented to the trainee.

1.8.2 Technical Final

The technical final examination will be given by the Section Supervisor and TC in the presence of the PM and other Department management (as needed) to ascertain the technical knowledge of the individual. This examination will be limited to hours (2) hours. After the examination, the TC, PM and relevant management with input from other attendees, will assess the individual's performance. The performance of the individual will be determined to be either satisfactory or unsatisfactory. The trainee must clearly demonstrate sufficient technical knowledge to perform examinations unaided and to draw correct conclusions. If the performance is deemed to be unsatisfactory, the TC, Section Supervisor, PM, and Laboratory Director will determine the appropriate action. After satisfactory completion of the technical oral examination, the individual will be subjected to a final mock trial.

1.8.3 Mock Trial

A mock trial will follow the successful completion of the technical oral examination. Section 19 of the QM outlines the roles and responsibilities of the participants as well as evaluation and grading guidelines.

1.8.4 After successful completion of the technical oral examination and the final mock trial, the TC, Section Supervisor and the Physical Evidence Program Manager will document, initial and date the technical and mock trial sections on the appropriate page of the sub-discipline's Digital & Multimedia Evidence Training Module Documentation Form (DFS Document 242-F200).

1.8.5 Satisfactory performance on the entire competency examination must be achieved before the individual is qualified to perform the duties of an examiner.

1.8.6 When the trainee has satisfactorily completed all training requirements, a memorandum will be issued by the PM to the Department Director recommending that the trainee be qualified to perform the duties of an examiner in the specific sub-discipline(s) within the section.

1.9 Assessment/Training of Experienced Personnel

1.9.1 The PM, Section Supervisor and the TC will interview the employee in detail upon reporting to the Section. The focus will be on past training, experience, education, published articles and other credentials to establish the employee’s knowledge, skills and abilities.

1.9.2 An Individual Training Plan (ITP) will be prepared by the TC documenting how previous training/experience meets the requirements of this training manual.

1.9.3 The ITP shall contain documentation of topics requiring training to ensure the employee possesses the same body of knowledge as an individual who completed the entire training process.

1.9.4 The employee shall complete a competency examination, consisting of a practical test, technical oral interview and mock trial, prior to being qualified to perform casework.

1.10 Transition from Trainee to Examiner

1.10.1 After the new examiner has successfully completed this training, there follows a period of adjustment. The job of the TC is to ensure that this transition from training to casework takes place as smoothly as possible.

1.10.2 Casework will be monitored by the TC for at least six (6) months.

1.10.3 The supervisor, TC or designee will accompany and monitor the newly qualified examiner to court for the first three (3) testimonies.

1.10.4 The new examiner will be required to evaluate the training program 4-6 months after qualification, by completing a Training Program Evaluation form (DFS Document 100-F121) in accordance with QM. The TC, the examiner's supervisor and the PM will review the completed evaluation form and use the information to improve the training of future examiners.

2 ORIENTATION

2.1 Minimum Requirements

2.1.1 Assessment and development of individual training plan for experienced personnel

2.1.2 An introduction to operating facilities and personnel

2.1.3 An introduction to the technical capabilities of all regional laboratories, to include definitions of the regional boundaries and areas of overlap

2.1.4 The outline of the training program and the expectations of both the TC and the trainee will be discussed

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

2.1.6 The duties of a DME forensic examiner will be clarified

2.1.7 Overview of DME section layout and capabilities

2.1.8 Coverage of the following documentation:

- Organization of the Department of Forensic Science
- DFS Quality Manual (DFS Document 100-D100) and forms
- Administrative policies and forms
  - DFS Code of Ethics
- Regional Operating Procedures (ROPs)
- DFS Safety Manual
- DME Evidence Handling & Laboratory Capabilities Guide
- DME Section Procedures Manual
- DME Section Training Manual

2.1.9 Introduction to DME section equipment, networks, storage locations, and logs

2.1.10 Introduction to the Digital & Multimedia Section (DME) Reference Library

2.1.11 Introduction to the laboratory information management system (LIMS)

3 COMPUTER AND MOBILE DEVICE ANALYSIS

Forensic computer and mobile device analysis includes the scientific examination of electronically stored information originating from a variety of devices.

Part I: Computer / Digital Storage Device Analyis

3.1 Objectives

To provide the trainee with the knowledge, skills and abilities to understand, explain and perform:

- The stages of a digital forensics examination
- The internal and external components of a typical computer system
- The boot and shutdown processes
- The characteristics of hard-disk drives, solid-state drives, flash memory cards and optical discs
- How digital storage devices store and represent data
- Media partitioning and formatting
- File systems, operating systems, file slack, free (unallocated) space and previously-existing data
- The function of data obfuscation, encryption and passwords
- The data acquisition and verification process
- Mapping and parsing derivative evidence datasets
- Recovering previously-existing data
- File types and metadata typically encountered during analysis
- Identifying and authenticating responsive data
- Producing examination results and evidence sources
- The operation and maintenance of examination equipment

3.2 Methods of Instruction

- Lectures and Discussions
- Required Reading
- Practical Exercises
- Study Questions

3.3 Lectures and Discussions

The following lectures and discussions will provide the trainee with an overview of computer analysis concepts.

3.3.1 Digital Forensics

This lecture and discussion will address the history, evolution and current state of digital forensics, as well as the stages of a digital forensics examination.

3.3.2 Computer Systems

This lecture and discussion will address the internal and external components of a typical computer system, as well as the Basic Input/Output System (BIOS) and Unified Extensible Firmware Interface (UEFI) interfaces and their respective boot sequences.

3.3.3 Digital Storage Devices and Data

This lecture and discussion will address the most common digital storage device form factors and interfaces, the fundamentals of magnetic, solid-state and optical data storage, and how data can be represented using the binary, decimal and hexadecimal numeral systems, as well as the American Standard Code for Information Interchange (ASCII) and Unicode character encoding systems.

3.3.4 File Systems and Operating Systems

This lecture and discussion will address disk partitioning schemes and high-level formatting, the most commonly encountered file systems and operating systems, drive letter assignment and volume labels, and what happens when a file is deleted within different file systems.

3.3.5 Security Measures

This lecture and discussion will address the fundamentals of password-protection, encryption and data obfuscation, as well as the available methods for identifying and countering these security measures.

3.3.6 Evidence Handling

This lecture and discussion will address how to safely package, store and handle evidence items containing electronically stored information.

3.3.7 Data Acquisition and Verification

This lecture and discussion will address some of the different methods for acquiring and verifying derivative evidence; including the available equipment and when it should be utilized.

3.3.8 Data Processing and Recovery

This lecture and discussion will address some of the different automated and manual methods for mapping and parsing both existing and previously-existing data from the contents of derivative evidence datasets, as well as advanced techniques for recovering previously-existing data; including the available equipment and when it should be utilized.

3.3.9 Metadata

This lecture and discussion will address the different forms of metadata, its importance and methods to parse the information.

3.3.10 Analysis Techniques

The lecture and discussion will address the methods used to identify and authenticate responsive data, including the available equipment and when it should be utilized, as well as filtering, searching, deduplicating and reviewing techniques. Measures for analyzing compressed, compound, embedded, database and other complex structured and unstructured data, as well as targeted data components, such as user-generated vs. system files, electronic communications, file activity, web-browser history, hardware and software configuration settings, and system logs will also be addressed.

3.3.11 Data Production

This lecture will discuss the different formats in which evidence sources and examination results can be produced, stored and transferred.

Additional or substitute lectures and discussions may be assigned, as necessary, by the TC or Section Supervisor with approval of the PM.

3.4 Required Reading

The following reading materials, or their equivalent, will provide the trainee with the knowledge, skills and abilities to understand computer analysis concepts.

3.4.1 Virginia Department of Forensic Science. *Digital & Multimedia Evidence Section Procedures Manual*.

3.4.2 The operating manuals and help files associated with currently utilized equipment.

3.4.3 Scientific Working Group on Digital Evidence (SWGDE). *https://www.swgde.org/documents*.

3.4.4 Carrier, Brian. *File System Forensic Analysis*. Second Edition. Upper Saddle River, NJ: Addison-Wesley, 2011.

3.4.5 Association of Chief Police Officers. *ACPO Good Practice Guide for Digital Evidence*. Version 5. 2012.

3.4.6 National Institute of Justice (NIJ), US Department of Justice, Office of Justice Programs. *Electronic Crime Scene Investigation: A Guide for First Responders*. Second Edition. 2008.

3.4.7 Barbara, John J., ed. *Handbook of Digital and Multimedia Forensic Evidence*. Totowa, NJ: Humana Press, 2008.

3.4.8 U.S. Department of Homeland Security, United States Secret Service. *Best Practices For Seizing Electronic Evidence: A Pocket Guide for First Responders*. Version 3. 2007.

Additional or substitute literature may be assigned, as necessary, by the TC or Section Supervisor with the approval of the PM.

3.5 Study Questions

The following study questions will provide the trainee with the knowledge, skills and abilities to effectively explain computer analysis concepts.

3.5.1 Explain what digital forensics is and what the stages of a digital forensics examination are.

3.5.2 Explain what information in the BIOS, UEFI or other system firmware interfaces should be documented.

3.5.3 Explain the differences between magnetic, solid-state and optical storage devices.

3.5.4 Explain the binary numeral system and some of the different ways binary data can be represented.

3.5.5 Explain what a byte unit of digital information is and how it, and its multiples, can represent a dataset's size and a storage devices capacity.

3.5.6 Explain what an operating system and file system are, which ones are typically encountered during analysis and what types of systems or devices they can be found on.

3.5.7 Explain what happens when a file is deleted in the File Allocation Table (FAT), New Technology File System (NTFS), Hierarchical File System Plus (HFS+), and fourth Extended File System (Ext4) file systems and the options for recovering previously-existing data from each file system.

3.5.8 Explain the purpose of password-protection, encryption and data obfuscation, and some of the ways they can be countered.

3.5.9 Explain how to safely handle evidence items containing electronically stored information so as to minimize the potential for data loss.

3.5.10 Explain what volatile and non-volatile flash memory are and why they can be problematic in digital forensics.

3.5.11 Explain what write-blocking is and its importance.

3.5.12 Explain the function of a boot disk.

3.5.13 Explain what derivative evidence is and give examples of different types and formats.

3.5.14 Explain what a hash value is and give examples of how it is utilized.

3.5.15 Explain the process of acquiring, restoring and verifying a forensic image of a source storage device and its importance.

3.5.16 Explain what generally occurs when a dataset is processed by analysis equipment.

3.5.17 Explain what metadata is and give examples of where it can be found.

3.5.18 Explain what proprietary data and data encoding are and give examples of their use and methods for decoding.

3.5.19 Explain the difference between user-generated (non-system) data and system data and methods for differentiating between them.

3.5.20 Explain what data deduplication is, its importance and examples of how it can be used.

3.5.21 Explain the challenges of analyzing complex structured (e.g., compressed, compound, embedded, database, etc. files) and unstructured data.

3.5.22 Explain what the Microsoft Windows Registry is, where it's stored, how it's structured, how to extract elements from it, and provide examples of elements that are typically analyzed.

3.5.23 Explain what the "cloud" is.

3.5.24 Explain data authentication and its purpose.

3.5.25 Define the following terms and acronyms:

- Electronically-Stored Information (ESI)
- Unique Identifier (UID)
- Boot
- Power-On Self-Test (POST)
- Peripheral
- Clock drift
- PATA, SATA, USB, and Firewire
- Hot-Swappable
- Formatting
- Master Boot Record (MBR), Volume Boot Record (VBR), and GUID Partition Table (GPT)
- Physical Drive, Logical Drive, Partition, Volume, Session, and Track
- Hexadecimal
- Sector and Cluster
- File Slack and Free (Unallocated) Space
- Storage Media, Source Media and Target Media
- Logical Acquisition and Physical Acquisition
- Image Restoration (Clone)
- Virtual Boot and Virtual Machine
- File Format, Native File Format and Proprietary File Format
- Driver
- Archive File
- Backup File
- Compound File
- Database
- Embedded Data
- Log File
- Configuration Settings
- Internet Protocol (IP) Address
- Compression

- Malware
- Area of Interest (AoI)
- Electronic Communication
- Web-Browser History
- Import and Export

Additional or substitute questions may be assigned, as necessary, by the TC or Section Supervisor with the approval of the PM.

3.6 Practical Exercises

The following exercises will provide the trainee with the knowledge, skills and abilities to perform a thorough computer analysis.

3.6.1 Binary, Decimal, Hexadecimal, ASCII, and Unicode Conversions

3.6.2 Prepare a storage device for use

3.6.3 Verify, alter and re-verify a file

3.6.4 Acquire and verify derivative evidence from a computer system, hard-disk drive, USB flash memory device, and optical disc

3.6.5 Verify and process acquired derivative evidence

3.6.6 Identify partition or session information

3.6.7 Identify metadata

3.6.8 Identify file types

3.6.9 Extract elements from the Microsoft Windows Registry

3.6.10 Recover previously-existing data

3.6.11 Identify data responsive to criteria

3.6.12 Prepare analytical notes and examination results for verification review

3.6.13 Generate evidence sources and examination results media

3.6.14 Generate a printed copy of analytical notes

3.6.15 Prepare a Certificate of Analysis (CoA)

Additional or substitute exercises may be assigned, as necessary, by the TC or Section Supervisor with the approval of the PM.

3.7 Evaluation

3.7.1 Review of completed assignments.

3.7.2 A presentation on a topic assigned by the TC.

Part II: Mobile Device Analysis

3.8 Objectives

To provide the trainee with the knowledge, skills and abilities to understand, explain and perform:

- The internal and external components of a typical mobile telephone
- The purpose and function of Universal Integrated Circuit Cards (UICC) and removable flash memory cards
- File systems, operating systems and previously-existing data
- Device security measures
- Radio frequency shielding of mobile devices and its importance
- The acquisition of logical and physical data
- Advanced data acquisition and processing methods
- SQLite database analysis
- The limitations of automated data acquisition and processing methods
- The operation and maintenance of examination equipment

3.9 Methods of Instruction

- Lectures and Discussions
- Required Reading
- Study Questions
- Practical Exercises

3.10 Lectures and Discussions

The following lectures and discussions will provide the trainee with an overview of mobile device analysis concepts.

3.10.1 Mobile Phones

This lecture and discussion will address the internal and external components of a typical mobile phone, the Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS) and code division multiple access (CDMA) communication technologies, as well as the Android and iOS boot processes.

3.10.2 File Systems and Operating Systems

This lecture and discussion will address the different file systems and operating systems that are typically encountered on mobile phones.

3.10.3 Security Measures

This lecture and discussion will address the fundamentals of password-protection, encryption and data obfuscation, as well as the available methods for identifying and countering these security measures.

3.10.4 Evidence Handling

This lecture and discussion will address how to safely package, store and handle mobile device evidence items containing electronically stored information.

3.10.5 Data Acquisition and Verification

This lecture and discussion will address some of the different methods for acquiring and verifying derivative evidence from mobile devices; including the available equipment and when it should be utilized.

3.10.6 Data Processing and Recovery

This lecture and discussion will address some of the different automated and manual methods for mapping and parsing both existing and previously-existing data from the contents of mobile devices, as well as advanced techniques for recovering previously-existing data; including the available equipment and when it should be utilized.

3.10.7 Analysis Techniques

The lecture and discussion will address the methods used to identify and authenticate responsive data; including the available equipment and when it should be utilized, as well as filtering, searching, deduplicating, and reviewing techniques. Measures for the automated and manual analysis of SQLite databases, encoded data, and other complex structured and unstructured data; as well as targeted data components, such as user-generated vs. system files, electronic communication records, file activity, web-browser history, device and application configuration settings, and system logs will also be addressed.

3.11 Required Reading

The following reading materials, or their equivalent, will provide the trainee with the knowledge, skills and abilities to understand mobile device analysis concepts.

3.11.1 Virginia Department of Forensic Science. *Digital & Multimedia Evidence Section Procedures Manual*.

3.11.2 The operating manuals and help files associated with currently utilized equipment.

3.11.3 Scientific Working Group on Digital Evidence (SWGDE). *https://www.swgde.org/documents*.

3.11.4 Bommisetty, Satish, Rohit Tamma, and Mahalik, Heather. *Practical Mobile Forensics* -. S.l.: Packt Limited, 2014.

3.11.5 Cellebrite Inc. *What Happens When You Press that Button? Explaining Cellebrite UFED Data Extraction Processes.* Version 05/29/2014.

Additional or substitute literature may be assigned, as necessary, by the TC or Section Supervisor with the approval of the PM.

3.12 Study Questions

The following study questions will provide the trainee with the knowledge, skills and abilities to effectively explain mobile device analysis concepts.

3.12.1 Explain what mobile device analysis is and what the stages of a mobile device examination are.

3.12.2 Explain the types of information that can be extracted from mobile phones.

3.12.3 Explain what the GSM, UMTS and CDMA communication technologies are.

3.12.4 Explain what the function of a UICC is for a GSM-compatible, UMTS-compatible and CDMA-compatible mobile phone, and the type of information that can be extracted from it.

3.12.5 Explain the purpose of a mobile device's removable flash memory card.

3.12.6 Explain what operating systems and file systems are typically encountered during analysis and what types of devices they can be found on.

3.12.7 Explain what security measures are typically encountered on a mobile phone and some of the ways they can be countered.

3.12.8 Explain shielding and its importance, as well as some of the effective methods of shielding.

3.12.9 Explain what a logical and physical acquisition is?

3.12.10 Explain how user-generated data is typically stored on a mobile phone.

3.12.11 Explain what an SQLite database is and the importance of its associated, when applicable, Write-Ahead Log (WAL).

3.12.12 Explain how previously-existing data might be recovered from a mobile phone.

3.12.13 Define the following terms and acronyms:

- GPS
- IMEI and MSISDN
- ESN, MEID, MIN, and MDN
- SIM, USIM and CSIM
- PIN and PUK
- ICCID, Ki, and LAI
- IMSI, MCC and MNC
- Airplane Mode
- Remote Destruction of Data
- JTAG
- ISP
- Chip-Off
- Scroll Capture
- SMS and MMS

Additional or substitute questions may be assigned, as necessary, by the TC or Section Supervisor with the approval of the PM.

3.13 Practical Exercises

The following exercises will provide the trainee with the knowledge, skills and abilities to perform a thorough mobile device analysis.

3.13.1 Removal of onboard storage and proper use of shielding

3.13.2 Acquire and verify derivative evidence from a mobile phone, UICC, and flash memory card

3.13.3 Verify and process acquired derivative evidence

3.13.4 Identify device information

3.13.5 Extract existing and previously-existing records from SQLite databases

3.13.6 Decode encoded timestamp values

3.13.7 Identify data responsive to criteria

3.13.8 Prepare analytical notes and examination results for verification review

3.13.9 Generate evidence sources and examination results media

3.13.10 Generate a printed copy of analytical notes

3.13.11 Prepare a Certificate of Analysis (CoA)

Additional or substitute exercises may be assigned, as necessary, by the TC or Section Supervisor with the approval of the PM.

3.14 Evaluation

3.14.1 Review of completed assignments.

3.14.2 A presentation on a topic assigned by the TC.

4 VIDEO ANALYSIS

Video analysis includes the scientific examination of analog or digital video recordings and images.

4.1 Objectives

To provide the trainee with the knowledge, skills and abilities to understand, explain and perform:

- The stages of a video/image examination
- The internal and external components of a typical digital/network video recorder (D/NVR) and digital camera
- How video recordings and digital images are produced
- The characteristics of hard-disk drives, solid-state drives, flash memory cards, and optical discs
- How digital storage devices store and represent data
- Media partitioning and formatting
- File systems and operating systems
- D/NVR security system characteristics
- Countering video recording and/or playback problems
- The data acquisition and verification process
- Working with derivative evidence datasets
- Recording formats typically encountered during analysis
- Identifying and authenticating responsive data
- Clarification techniques (e.g., sharpening, brightness, contrast, levels, de-interlacing, de-multiplexing, frame averaging, etc.)
- Producing examination results and evidence sources
- The operation and maintenance of examination equipment

4.2 Methods of Instruction

- Lectures and Discussions
- Required Reading
- Study Questions
- Practical Exercises

4.3 Lectures and Discussions

The following lectures and discussions will provide the trainee with an overview of video and image analysis concepts.

4.3.1 Video and Image Analysis

This lecture and discussion will address the history, evolution and current state of video and image analysis, as well as the stages of a video/image examination.

4.3.2 Digital/Network Video Recorders and Digital Cameras

This lecture and discussion will address the internal and external components of a typical digital video recorder and digital camera, analog and digital recording technology, and how video recordings and images are produced.

4.3.3 Digital Storage Devices and Data

This lecture and discussion will address the most common digital storage device form factors and interfaces, the fundamentals of magnetic, solid-state and optical data storage, and how data can be represented using the binary, decimal and hexadecimal numeral systems, as well as the American Standard Code for Information Interchange (ASCII) and Unicode character encoding systems.

4.3.4 File Systems and Operating Systems

This lecture and discussion will address disk partitioning schemes and high-level formatting, as well as the characteristics of non-proprietary and proprietary file systems and operating systems.

4.3.5 Evidence Handling

This lecture and discussion will address how to safely package, store and handle evidence items containing analog and digital information.

4.3.6 D/NVR Security Systems

This lecture and discussion will address the characteristics of the commonly encountered digital/network video recorders; including the available methods for identifying and countering security measures.

4.3.7 Reconstruction of Media

This lecture and discussion will address the methods for repairing damaged analog media.

4.3.8 Data Acquisition and Verification

This lecture and discussion will address some of the different methods for acquiring and verifying derivative evidence; including the available equipment and when it should be utilized, as well as the image restoration process and techniques for countering video playback issues.

4.3.9 Data Processing and Recovery

This lecture and discussion will address some of the different automated and manual methods for mapping and parsing both existing and previously-existing data from the contents of derivative evidence datasets, as well as advanced techniques for recovering complex structured data; including the available equipment and when it should be utilized.

4.3.10 Video and Image Formats

This session will include discussions on the variety of video and image formats and the advantages and disadvantages of each.

4.3.11 Analysis Techniques

The lecture and discussion will address the methods used to identify, authenticate and clarify responsive data. Measures for analyzing compressed video, maintaining proper aspect ratio and countering clarification limiters will also be addressed.

4.3.12 Data Production

This lecture will discuss the different formats in which evidence sources and examination results can be produced, stored and transferred.

Additional or substitute lectures and discussions may be assigned, as necessary, by the TC or Section Supervisor with approval of the PM.

4.4 Required Reading

The following reading materials, or their equivalent, will provide the trainee with the knowledge, skills and abilities to understand video and image analysis concepts.

4.4.1 Virginia Department of Forensic Science. *Digital & Multimedia Evidence Section Procedures Manual*.

4.4.2 The operating manuals and help files associated with currently utilized equipment.

4.4.3 Scientific Working Group on Digital Evidence (SWGDE). *https://www.swgde.org/documents*.

4.4.4 Technical Support Working Group (TSWG). *Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems*. Version 1.0. 2006.

4.4.5 U.S. Department of Homeland Security, United States Secret Service. *Best Practices For Seizing Electronic Evidence: A Pocket Guide for First Responders*. Version 3. 2007.

4.4.6 Association of Chief Police Officers. *ACPO Good Practice Guide for Digital Evidence*. Version 5. 2012.

4.4.7 National Institute of Justice (NIJ), US Department of Justice, Office of Justice Programs. *Electronic Crime Scene Investigation: A Guide for First Responders*. Second Edition. 2008.

4.4.8 Blitzer, Herbert L., and Jack Jacobia. *Forensic Digital Imaging and Photography*. San Diego: Academic, 2007.

4.4.9 Damjanovski, Vlado. *CCTV: Networking and Digital Technology*. N.p.: Butterworth-Heinemann, 2005.

4.4.10 Reis, George. Photoshop for Forensics Professionals: A Complete Digital Imaging Course for Investigators. N.p.: Wiley, 2007.

Additional or substitute literature may be assigned, as necessary, by the TC or Section Supervisor with the approval of the PM.

4.5 Study Questions

The following study questions will provide the trainee with the knowledge, skills and abilities to effectively explain video and image analysis concepts.

4.5.1 Explain what video and image analysis are and what the stages of a video/image examination are.

4.5.2 Explain the following common limiting factors in video/image analysis:

- Poor media quality
- Camera placement
- Focal length
- Lighting
- Quad recordings
- Electrical interference
- Multiplexing
- Time-lapse recordings
- Compression

4.5.3 Explain what information in a recorder's interface should be documented.

4.5.4 Explain the differences between analog and digital video.

4.5.5 Explain how digital video recordings and digital images are produced.

4.5.6 Explain the differences between magnetic, solid-state and optical storage devices.

4.5.7 Explain the binary numeral system and some of the different ways binary data can be represented.

4.5.8 Explain what a byte unit of digital information is and how it, and its multiples, can represent a dataset's size and a storage devices capacity.

4.5.9 Explain what an operating system and file system are, which ones are typically encountered during analysis and what types of systems or devices they can be found on.

4.5.10 Explain how to safely handle evidence items containing analog and digital information so as to minimize the potential for data loss.

4.5.11 Explain what volatile and non-volatile flash memory are and why they can be problematic in digital forensics.

4.5.12 Explain what write-blocking is and its importance.

4.5.13 Explain what derivative evidence is and give examples of different types and formats.

4.5.14 Explain what a hash value is and give examples of how it is utilized.

4.5.15 Explain the process of acquiring, restoring and verifying a forensic image of a source storage device and its importance.

4.5.16 Explain the difference between single frame video capture and video stream capture.

4.5.17 Explain the following most common playback issues:

- Format
- Proprietary player
- Aspect ratio

4.5.18 Name the most common analog and digital video formats and explain their differences.

4.5.19 Name three types of digital video signal formats and explain their differences.

4.5.20 Explain what interpolation is.

4.5.21 Name two types of compression methods and explain the differences between them.

4.5.22 Explain what pixel dimension, aspect ratio and resolution are and how they are related.

4.5.23 Explain what clarification is and the following common clarification techniques:

- Interlace/de-interlace
- Brightness/Contrast
- Sharpening
- Levels

4.5.24 Explain what metadata is and give examples of where it can be found.

4.5.25 Explain the following terms and acronyms:

- Unique Identifier (UID)
- Boot
- Power-On Self-Test (POST)
- CCD and CMOS
- Peripheral
- Clock drift
- PATA, SATA and USB
- Formatting
- Physical Drive, Logical Drive, Partition, Volume, Session, and Track
- Hexadecimal

- Sector and Cluster
- File Slack and Free (Unallocated) Space
- Storage Media, Source Media and Target Media
- Reconstruction
- Logical Acquisition and Physical Acquisition
- Image Restoration (Clone)
- Overwrite
- NTSC and PAL
- CRT
- Horizontal Blanking
- ITU 601
- Progressive Scan
- Component/Composite Video Signal
- VGA, DVI, HDMI, and DisplayPort
- Capture and Capture Device
- Tracking
- Time Base Correction
- Time-Lapse Recording
- Syncing
- Digitize
- File Format, Native File Format and Proprietary File Format
- Format Conversion
- Encoding
- H.264
- Embedded Data
- Compression, Lossless/Lossy Compression and Spatial/Temporal Compression
- CMYK/RGB/Gray Scale Image
- Additive/Primary Color
- Halftone
- Hue
- Gamma
- Luminance and Chrominance
- 4:2:0 and 4:2:2
- Dots Per Inch (DPI) and Pixels Per Inch (PPI)
- Pixel
- Re-sizing
- Field
- Frame
- GOP
- Predictive Frame, Bi-directional Frame, and Intraframe
- Frame Averaging
- Artifact
- Noise
- Blooming
- Pixelization
- Anti-Aliasing
- Clipping
- Area of Interest (AoI)
- Primary Image
- Original Copy and Working Copy
- Filter
- History Log
- Import and Export

Additional or substitute questions may be assigned, as necessary, by the TC or Section Supervisor with the approval of the PM.

4.6 Practical Exercises

The following exercises will provide the trainee with the knowledge, skills and abilities to perform a thorough video/image analysis.

4.6.1 Binary, Decimal, Hexadecimal, ASCII, and Unicode Conversions

4.6.2 Prepare a storage device for use

4.6.3 Verify, alter and re-verify a file

4.6.4 Demonstrate the effect of camera placement, focal length, lighting, and compression on the quality of a digital image

4.6.5 Reconstruct damaged analog media

4.6.6 Capture an analog video recording into a digital format

4.6.7 Acquire and verify derivative evidence from a DVR, hard-disk drive, USB flash memory device, and optical disc

4.6.8 Import derivative evidence into analysis equipment

4.6.9 Identify areas of interest

4.6.10 Clarify areas of interest

4.6.11 Prepare analytical notes and examination results for verification review

4.6.12 Generate evidence sources and examination results media

4.6.13 Generate a printed copy of analytical notes

4.6.14 Prepare a Certificate of Analysis (CoA)

4.7 Evaluation

4.7.1 Review of completed assignments.

4.7.2 A presentation on a topic assigned by the TC.

5 REPORT WRITING AND TESTIMONY

5.1 Objectives

5.1.1 To familiarize the trainee with DME report formats and phraseology.

5.1.2 To familiarize the trainee with the functions of a courtroom criminal proceeding.

5.1.3 To have the trainee prepare a current *curriculum vitae* and convey *voir dire* questioning during testimony.

5.1.4 To familiarize the trainee with proper methods of presenting expert testimony during direct examination.

5.1.5 To familiarize the trainee with the proper methods of defending analytical results during cross-examination.

5.2 Methods of Instruction

- Required Reading
- Assignments

5.3 Required Reading

5.3.1 Ball, Craig. *Becoming a Better Witness on Digital Forensics*. March 2014.

5.3.2 Ball, Craig. *Cross-examination of the Computer Forensics Expert*. May 2004.

5.3.3 National Commission on Forensic Science (NCFS). *Recommendations to the Attorney General Regarding Use of the Term "Reasonable Scientific Certainty"*. March 2016.

5.4 Assignments

5.4.1 Review the DFS Quality Manual and become thoroughly familiar with the guidelines regarding evidence handling, records and case files and reporting test results. Discuss these guidelines with the TC.

5.4.2 Review copies of recent case files generated by at least two examiners for the purpose of familiarization with report formats and phraseology.

5.4.2.1 The trainee shall document the review of at least five case files using the appropriate Technical Review Form. Case files should be generated by multiple examiners, if possible. The potential findings of the reviews shall be discussed with the TC. Technical Review forms generated in this capacity shall be marked as Training and retained in their Training File. The case files shall be technically reviewed by an authorized examiner pursuant to QM 17 prior to release.

5.4.2.2 Complete an ASCLD/LAB-International Audit Trail Worksheet on at least one case.

5.4.3 Discuss the meaning and/or definition of the following terms or phrases with the TC.

- Expert witness
- *Voir dire*
- *Daubert* standard
- *Spencer* standard
- Reasonable scientific certainty
- Hearsay
- Opinion
- Objection, Sustained and Overruled

5.4.4 Prepare responses to the below list of questions which can be used in court to assist in qualifying you as an expert witness.

5.4.4.1 What is your name?

5.4.4.2 What is your occupation?

5.4.4.3 What is your field of expertise?

5.4.4.4 How long have you been practicing in this field?

5.4.4.5 What is your current place of employment?

5.4.4.6 What is your current position?

5.4.4.7 What are your duties in this position?

5.4.4.8 How long have you been employed in this position?

5.4.4.9 What other positions in this field have you held?

5.4.4.10 What education and training have you had related to this field?

5.4.4.11 Do you hold any certifications related to this field?

5.4.4.12 Have you taught or lectured in this field?

5.4.4.13 Have you written or published any materials related to this field?

5.4.4.14 Are you a member of any professional organizations related to this field?

5.4.4.15 How many times have you testified in court as an expert witness in this field?

5.4.4.16 How many examinations have you conducted?

5.4.5 Review transcripts (as available) of at least one examiner regarding their testimony, in the applicable sub-discipline(s) of DME, and discuss the testimony with the examiner.

5.4.6 Observe (as available) at least one examiner testify and discuss the testimony with the examiner. Coordinate this with the TC.

5.4.7 Confer with other examiners regarding recommendations in regards to courtroom testimony.

5.4.8 Discuss with the TC characteristics of an effective and ineffective expert witness.

5.5 Evaluation

5.5.1 Review of completed assignments.

5.5.2 Provide a presentation to the TC and the PM focused on how the discipline meets the *Daubert* and *Spencer* standards.

5.5.3 Provide a presentation to the TC and the PM focused on how DFS meets, where applicable, the recommendations of the National Academy of Sciences (NAS), *Strengthening Forensic Science in the United States: A Path Forward*, 2009 report.