



TABLE OF CONTENTS

Table of Contents	1
Revision History.....	3
01 Overview	4
DM-TM-01-01 Overview of Digital/Multimedia Training Program.....	4
02 Computer/Mobile Forensic Analysis Unit	9
DM-TM-02-01 Legal Authorization	9
DM-TM-02-02 Components	11
DM-TM-02-03 Configuration / Installation	13
DM-TM-02-04 Digital Media	15
DM-TM-02-05 Partitions and Partition Schemes.....	17
DM-TM-02-06 File Systems	19
DM-TM-02-07 Disc Operating System (DOS).....	21
DM-TM-02-08 Windows® Operating Systems	23
DM-TM-02-09 Non- Windows® Operating Systems	25
DM-TM-02-10 Software and File Identification.....	27
DM-TM-02-11 Basic Network Topology	29
DM-TM-02-12 Web-Based Artifacts	30
DM-TM-02-13 Wiping.....	32
DM-TM-02-14 Performance Verification/Validation.....	34
DM-TM-02-15 Case Documentation	36
DM-TM-02-16 Forensic Acquisition.....	37
DM-TM-02-17 Forensic Analysis.....	40
DM-TM-02-18 Mobile Devices	43
DM-TM-02-19 Mobile Device Analysis.....	46
DM-TM-02-20 Reporting	48
DM-TM-02-21 Case Review.....	50
03 Forensic Audio/Video/Image Analysis Unit	52
DM-TM-03-01 Forensic Image Analysis.....	52
DM-TM-03-02 Forensic Video Analysis	54
DM-TM-03-03 Forensic Audio Analysis	56
04 Internal Department Photographic Support Unit	58
DM-TM-04-01 Suspect Lineup Enhancements	58
DM-TM-04-02 Photographic Overlays	60



DM-TM-04-03 Digital Displays for Court	62
05 Forms	64
Training Forms	64
Digital/Multimedia Computer Cases	64
External Training Courses.....	64
Digital/Multimedia Computer Forensics/Mobile Forensics Training Checklist.....	64
Digital/Multimedia Audio/Video/Image and Photography Training Checklist	64



REVISION HISTORY

Effective Date	Brief Description of Change(s)
10/03/2019	Original Issue Previous revision history for individual chapters included in archived documents



01 OVERVIEW

DM-TM-01-01 OVERVIEW OF DIGITAL/MULTIMEDIA TRAINING PROGRAM

1 Introduction

Individuals employed by the Texas Department of Public Safety as computer/mobile forensic examiners, audio/video examiners, and photographers must meet specific qualifications before being qualified to perform independently. The qualifications consist of educational requirements and forensic experience requirements. Independent casework examinations must not be undertaken until extensive instruction from a qualified examiner or specialist has been completed and the examiner has been authorized. A trainee must successfully complete competency tests before beginning casework responsibilities.

2 Purpose

For personnel meeting the minimum DPS educational employment requirements for the position, the DM training manual is designed to provide the trainee with sufficient background, laboratory skills, education, competency, and supervised hands-on experience to adequately perform independent work with minimal supervision. The Texas DPS training time is approximately one year for Computer/Mobile Forensic Analysis, nine months for Forensic Audio/Video/Image Analysis and three months for Internal Department Photographic Support and Photography. Trainees having prior experience in digital and/or multimedia analysis procedures may be evaluated with documented approval of the SQM to modify the training time and program according to their skills and knowledge.

3 Program Format

The training program is divided into units, each consisting of a set of modules. The modules may consist of: lectures, discussions, observation of demonstrations by the trainer; supervised performance, independent exercises, written exercises, and/or written exams. Once training is completed, final competency demonstrations and/or qualifying examinations must be successfully completed by the trainee before they can proceed to supervised casework. The final competency assessment will be completed at each module or unit level, as applicable.

The training program is identified as containing a set of required modules.

- A. **General Laboratory Training: Fundamentals Unit** will introduce the trainee to general laboratory practices, forensic science, quality assurance, general laboratory safety, and evidence handling.

This unit is not a prerequisite for discipline technical units.

This unit must be completed before supervised work.

- B. **General Laboratory Training: Forensic Legal Unit** will introduce the trainee to basic court testimony and case law.

This unit is not a prerequisite for discipline technical units.

This unit must be completed before supervised work.

- C. **Computer/Mobile Forensic Analysis Unit** will introduce the trainee to analysis of digital and computer/mobile forensic evidence (computer hardware, computer software, basic networks, network applications, mobile forensics, analysis using various software applications), documentation, legal issues, case evaluation and report writing.

This unit must be completed by Computer/Mobile Forensic trainees.



- D. **Forensic Audio/Video/Image Analysis Unit** will introduce the trainee to the analysis of analog and digital video, audio, and image evidence, as well as documentation, legal issues, case evaluation and report writing.

This unit must be completed by Forensic Audio/Video/Image Analysis trainees.

The following DM training manual modules must also be completed by the Audio/Video/Image Analysis trainee:

1. DM-TM-02-01 Legal Authorization
2. DM-TM-02-02 Components
3. DM-TM-02-04 Digital Media
4. DM-TM-02-05 Partitions and Partition Schemes
5. DM-TM-02-06 File Systems
6. DM-TM-02-13 Wiping
7. DM-TM-02-14 Performance Verification/Validation
8. DM-TM-02-15 Case Documentation
9. DM-TM-02-16 Forensic Acquisition
10. DM-TM-02-20 Reporting
11. DM-TM-02-21 Case Review

- E. **Internal Department Photographic Support Unit** will introduce the trainee to the processing of digital images not resulting from an audio/video/image laboratory case submission.

This unit must be completed by Forensic Audio/Video/Image Analysis trainees .

- F. **Photography Unit** found in the Crime Scene Response Training Manual will introduce the trainee to photography equipment and fundamentals of photography.

This unit must be completed by Forensic Audio/Video/Image Analysis trainees.

- G. **Crime Scene Response Training Program** will introduce the trainee to the tasks and responsibilities of the laboratory while participating in a crime scene response.

This unit must be completed by those on the Crime Scene Response Team.

Note: Trainees will not work on actual evidence, but instead copies of evidence. Trainees will not touch the original evidence and will not be involved in the data acquisition process until appropriate work authorization.

4 Safety

Safety precautions outlined in the Texas DPS Safety Manual will be followed at all times during the training program. Any specific safety considerations for the discipline (such as specific reagent SDS or potential physical hazards encountered photographing a crime scene) will be designated in each of the modules.

5 Responsibilities

- A. Meetings between the trainee, the trainer, and/or supervisor should be held periodically in order to evaluate the trainee's progress, plan future study and practical assignments, and address any deficiencies which may require additional training.



- B. The trainee will be required to keep a training notebook. The training program covers information that requires the trainee to keep up with reading assignments on a self-study basis. The trainee is responsible for informing his/her trainer or supervisor when problems arise at any time during the training period.

6 Unit Assessment

Training assessment will be undertaken as separate modules of training and the conclusion of the unit is accomplished when:

- A. All practical examinations are correctly analyzed;
- B. The training notebook is approved by the Trainer;
- C. The training notebook, other training records documenting completion of training requirements, and trainee's credentials are reviewed; and
- D. The laboratory supervisor and trainer(s) recommend that the examiner be approved for supervised casework.

6.2 Computer/Mobile Forensic Competency Requirements

- A. The Computer/Mobile Forensic Unit trainee will successfully complete:
 - 1. A comprehensive written exam,
 - 2. A report writing competency. Final competency exam will include a formal mock report, including a "For Officer Report" digital report.
 - 3. Competency test(s) to sufficiently cover the anticipated spectrum of assigned duties and evaluate the individual's ability to perform proper testing methods, to include:
 - a) *Acquisition of mock evidence*
 - b) *Analysis of mock evidence*
 - c) *Examination performed on at least one of each of the following electronic media*
 - i. *hard drive*
 - ii. *mobile device*
 - d) *Case review*
- B. The Computer/Mobile Forensic Unit trainee will successfully complete a mock trial exercise.

6.3 Additional Computer/Mobile Forensic Unit Requirements

It is recommended that the following training classes (or trainer-approved equivalent) be completed prior to completion of the analysis unit;

- 1. *"DF310: Advanced Digital Forensic Analysis: Windows", National White Collar Crime Center*
- 2. *"DF320: Advanced Digital Forensic Analysis: macOS", National White Collar Crime Center*
- 3. *"Access Data FTK Boot Camp" Access Data*



6.4 Computer/Mobile Forensic Supervised Casework Requirements

A minimum of three supervised cases will be completed; one computer forensic case and two mobile forensic cases.

6.5 Forensic Audio/Video/Image Analysis Competency Requirements

- A. Forensic Audio Video/Image Analysis Unit trainee will successfully complete:
1. A comprehensive written exam
 2. A report writing competency. Final competency exam will include a formal mock report, including a “For Officer Report” digital report.
 3. Competency test(s) to sufficiently cover the anticipated spectrum of assigned duties and evaluate the individual’s ability to perform proper testing methods, to include:
 - a) *Acquisition of mock evidence*
 - b) *Analysis of mock evidence*
 - c) *Video enhancement*
 - d) *Image enhancement*
 - e) *Audio enhancement*
 - f) *Case review*
- B. The Forensic Audio Video/Image Analysis Unit trainee will successfully complete a mock trial exercise.

6.6 Additional Forensic Audio/Video/Image Analysis Unit Requirements

External Training Courses

- B. The following training classes (or trainer-approved equivalent) must be completed within the first year of training:
1. *Level 1, Forensic Video Analysis and The Law, LEVA (Law Enforcement and Emergency Services Video Association)*
 2. *Level 2, Digital Multimedia Evidence Processing, LEVA (Law Enforcement and Emergency Services Video Association)*
- C. It is recommended that the following training class (or trainer-approved equivalent) be completed prior to completion of the analysis unit: *Introduction to Forensic Audio Analysis, Resolution Video*

6.7 Audio/Video/Image Analysis Supervised Casework Requirements

A minimum of five supervised cases will be completed; two video cases, two audio cases, and one image case.

6.8 Internal Department Photographic Support Competency Requirements

The Image Analysis Unit trainee will successfully complete a final comprehensive competency test to sufficiently cover the anticipated spectrum of assigned duties and evaluate the individual’s ability to perform proper processing methods.



6.9 Internal Department Photographic Support Supervised Request Requirements

A minimum of three supervised requests will be completed. If no requests are submitted within a reasonable time frame, mock requests may be provided by the trainer at the trainer's discretion.

6.10 Photography Unit Competency Requirements

The photography unit training can be found in the Crime Scene Response training modules.

- A. The following modules must be successfully completed by the photography unit trainee:
 - 1. CSR-TM-02-01: Introduction to Photography Equipment
 - 2. CSR-TM-02-02: Basic Photography
- B. Photography Unit trainee will successfully complete:
 - 1. Practical exercises as described in the training module
 - 2. A comprehensive written exam

Supervised casework is not required for the Photography Unit training.

7 Evaluation of Training Program

The trainee will complete the Laboratory Training Program Evaluation Form (LAB-304) upon completion of the training program.



02 COMPUTER/MOBILE FORENSIC ANALYSIS UNIT

DM-TM-02-01 LEGAL AUTHORIZATION

Duration 2 days

Purpose Familiarize the trainee with legal aspects of analyzing digital/multimedia evidence

Prerequisite None

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will understand the legal authorization necessary to conduct DM analysis in the laboratory.

Sufficient legal authorization is required prior to examination of digital media evidence in order to preserve admissibility as evidence in court and limit personal and laboratory liability.

1.2 Practical

Following completion of the training, the trainee will be able to:

- A. Examine submitted documents and determine if sufficient legal authorization is present.
- B. Assist in answering questions from submitting officers concerning legal authorization.

2 Training Outline

2.1 Lesson Plan

Trainee will be required to read articles describing legal authorization for analysis.

2.2 Required Readings

- A. Casey, Eoghan. 2000. Digital Evidence and Computer Crime. Academic Press, Pages 15-23
- B. Dept. of Justice Website, www.cybercrime.gov. "Searching and Seizing Computers and Related Electronic Evidence Issues" 2002. Chapters 2 and 5
- C. NW3C STOP Course Material – Reference Materials: 4th Amendment Issues, Consent to Search Computer, Consent to Search Form #3, Consent to Search Form #2, Uniform Consent Form
- D. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. "SWGDE Comments on Forced Minimization Requirements for the Seizure of Digital Evidence" 2016.

3 Practice

3.1 Independent Exercises

The trainee will be required to review case documentation as practiced by a qualified examiner on at least 5 cases.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None



4.2 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.

4.3 Dependent Modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-02-02 COMPONENTS

Duration 3 days

Purpose The trainee will become familiar with various computer hardware components

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will become familiar with various computer hardware components.

Personal computers are comprised of numerous individual components which perform a variety of different functions. The presence or absence of certain components could be significant to forensic acquisition and analysis.

1.2 Practical

Following the completion of training, the trainee will be able to:

- A. Identify various hardware components.
- B. Identify the various functions of computer hardware.

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing computer hardware components.

2.2 Required Readings

- A. White, Ron. 2008. How Computers Work. Que Corporation, Parts 1-5, and 7.
- B. Carrier, Brian, 2005. File System Forensic Analysis. Addison Wesley, Pages 29 – 44.
- C. NW3C BDRA Course Material: Hard Drive Configuration – Hard Drive Connections & Physical Characteristics

3 Practice

3.1 Basic or Special Skills

The ability to identify various hardware components and their functions

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Various loose hardware components
- Forensic workstations with installed components

3.4 Observed Performance

Under guidance from the trainer or an experienced examiner, the trainee will be required to observe individual computer hardware components both installed and uninstalled.



4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.

4.3 Dependent Modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-02-03 CONFIGURATION / INSTALLATION

Duration 1 week

Purpose The trainee will become familiar with the steps of the initial boot process. The trainee will become familiar with the installation of various hardware components to create a bootable computer.

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with the steps of the initial boot process and with the installation of various hardware components to create a bootable computer.

During a forensic analysis, it is sometimes necessary to boot the evidence computer. In order to be able to explain and control the boot process, it is necessary to have an understanding of the initial boot process. A hands-on approach is invaluable to gain knowledge of the boot process.

1.2 Practical

Following the completion of training the trainee will be able to:

- A. Discuss the initial boot process of a computer.
- B. Install hardware components in order to create a bootable computer.
- C. Troubleshoot problems in the boot process and attempt to correct them.

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing the boot process.

2.2 Required Readings

- A. EnCase On-Demand Computer Forensics I Guide pg. 89-90.
- B. Carrier, Brian. 2005. File System Forensic Analysis pg. 27-28.
- C. NW3C STOP Course Material: BIOS/UEFI Changing the Boot Order/Sequence
- D. NW3C BDRA Course Material (2016): Boot Process – The Boot Up Process
- E. Manuals associated with hardware components to be used in bootable computer

3 Practice

3.1 Basic or Special Skills

The ability to identify the boot sequence of events, the ability to install hardware components and troubleshoot any boot problems.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.



3.3 Supervised Performance

Under guidance from the trainer or an experienced examiner, the trainee will be required to install computer hardware components to create a bootable computer.

3.4 Equipment

- Forensic Workstation
- Hardware components required to create a bootable workstation
- Toolkit

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.

4.3 Dependent modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-02-04 DIGITAL MEDIA

Duration 1 week

Purpose The trainee will become familiar with various types of digital media and the mechanics of data storage

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of the training, the trainee will be familiar with various types of digital media and the mechanics of data storage.

Digital data can be stored using a variety of different types of media such as hard disk drives, USBs, SD cards, or optical discs such as CDs and DVDs. The physical construction of each type of media varies widely; but the data is stored on each type using similar structure from the bit level to the sector level. A good understanding of how data is stored on the different media types is necessary for both analysis and evidence handling.

1.2 Practical

Following completion of the training, the trainee will be able to:

- A. Discuss the basic digital data storage conventions from the bit level to the sector level.
- B. Identify various types of digital media including but not limited to: hard drives (including Solid State Drives), DVDs/CDs, floppy disks, USB devices, and digital media cards (SD cards).
- C. Discuss the physical structure of various types of digital media.

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing the data storage conventions and digital media types.

2.2 Required Readings

NW3C BDRA (2016) Training Material - Bits and Bytes

3 Practice

3.1 Basic or Special Skills

- A. The ability to perform HEX/ binary/ ASCII conversions.
- B. The ability to identify various digital media types and hardware structure.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Various types of digital media
- Toolkit



3.4 Observed Performance

The trainee will be required to observe various digital media types and to take apart the more common types to observe the underlying construction.

3.5 Independent Exercises

The computer/mobile forensics trainee will be required to perform calculations based on the data storage conventions including but not limited to:

- A. Total # of sectors/bytes on digital media
- B. Binary / HEX/ ASCII conversions

NOTE: The audio/video/image analysis trainee will not be required to complete the depicted exercises.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

4.2 None

4.3 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.

4.4 Dependent Modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further modules.



DM-TM-02-05 PARTITIONS AND PARTITION SCHEMES

Duration 1 week

Purpose The trainee will become familiar with digital media partitions and master boot records

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with digital media partitions, master boot records, and other similar indices.

On many types of digital media, the media is divided into one or several partitions or similar indices. While forensic software allows for automatic parsing of the indices, a solid grasp of their structure is necessary in the case of troubleshooting media or in order to fully explain the forensic process in court.

1.2 Practical

Following completion of the training, the trainee will be able to:

- A. Recognize different types of partitions and the structure of other similar indices
- B. Use tool(s) to construct different types of partitions
- C. Reconstruct an overwritten master boot record

2 Training Outline

2.1 Lesson Plan

The trainee will review articles describing the partitions and the master boot record.

2.2 Required Readings

- A. Carrier, Brian, 2005. File System Forensic Analysis. Addison Wesley, Chapters 4-5.
- B. NW3C BDRA (2016) Course Material – MBR Partitioning, Alternate Partitioning

3 Practice

3.1 Basic or Special Skills

- A. The ability to identify different components of a master boot record and different types of partitions.
- B. The ability to view and manipulate the master boot record and different types of partitions.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic Workstation
- Software
- Digital media



3.4 Supervised Performance

- A. Under guidance from the trainer or an experienced examiner, the computer/mobile forensics trainee will be required to use a hex editor to view and manipulate a master boot record. The trainee will be required to rebuild an overwritten master boot record.
- B. Under guidance from the trainer or an experienced examiner, the computer/mobile forensics trainee will be required to use different software programs to create and delete various types of partitions.

NOTE: The audio/video/image analysis trainee will not be required to complete the depicted performance exercises.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.

4.3 Dependent modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-02-06 FILE SYSTEMS

Duration 1 week

Purpose The trainee will become familiar with various file systems

Prerequisite None

1 Objectives

1.1 Theoretical

Following training, the trainee will be familiar with various file systems.

- A. File systems are the basic data storage structure on any type of digital media. There are several file systems that can be encountered in a forensic analysis. The location and type of evidentiary artifacts will vary depending on the type of file system.
- B. The trainee should understand the mechanics of various file systems not only for examination of evidentiary media but also for choosing the file system for the forensic media.

1.2 Practical

Following completion of the training, the trainee will be able to:

- A. Discuss the basic mechanics of various types of files systems.
- B. Discuss the differences between different file systems.

2 Training Outline

2.1 Lesson Plan

The trainee will review articles describing various file systems.

2.2 Required Readings

- A. Carrier, Brian, 2005. File System Forensic Analysis. Addison Wesley, Chapters 8-17.
- B. EnCase On-Demand Computer Forensics I Guide – Lesson 7.
- C. NW3C IDRA (2017) Course Material – FAT Formatting, FAT File System (Parts 1 &2), FAT Directory Structure, FAT Recycle Bin, FAT Recovery of Deleted Files, File Headers and Hashing, File Metadata, Search Techniques and Pagefile, NTFS Architecture, NTFS File Structure, NTFS Saving Files, NTFS Recycle Bin, NTFS Deleted Files

3 Practice

3.1 Basic or Special Skills

The ability to identify different file systems and understand the basic mechanics of various file systems.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic Workstation
- Forensic Software



3.4 Supervised Performance

- A. Under guidance from the trainer or an experienced examiner, the computer/mobile forensics trainee will be required to use a hex editor to view various file systems.
- B. Under guidance from the trainer or an experienced examiner, the computer/mobile forensics trainee will be required to use different software programs to create and delete various types of file systems.

NOTE: The audio/video/image analysis trainee will not be required to complete the depicted performance exercises.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.

4.3 Dependent modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-02-07 DISC OPERATING SYSTEM (DOS)

Duration 1 week

Purpose The trainee will become familiar with the Disc Operating System (DOS) and be able to execute basic DOS commands

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with the Disc Operating System (DOS) and be able to execute basic DOS commands.

DOS is an early operating system when compared to most systems in use. It can be used as a building block to understanding more complex operating systems.

1.2 Practical

Following the completion of training, the trainee will be able to:

- A. Identify the necessary DOS system files
- B. Execute basic DOS commands

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing the DOS files and basic DOS commands.

2.2 Required Readings

- A. Microsoft® MS-DOS 6.22 User's Guide, Chapters 2 and 4, 1994, Microsoft® Corporation.
- B. Gookin, Dan. 1996. DOS for Dummies®, Windows 95 Edition.

3 Practice

3.1 Basic or Special Skills

The ability to identify necessary DOS files, execute basic DOS commands.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- DOS boot floppy
- Forensic workstation

3.4 Supervised Performance

Under guidance from the trainer or an experienced examiner, the trainee will execute basic DOS commands.



4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-08 WINDOWS® OPERATING SYSTEMS

Duration 2 weeks

Purpose The trainee will become familiar with the Windows® operating systems

Prerequisite None

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will be familiar with the various Windows® operating systems.

Knowledge of the operating system structure is vital in forensic analysis in order to locate evidentiary data and to interpret the significance of the findings.

1.2 Practical

Following the completion of training, the trainee will be able to:

- A. Discuss the basic Windows® operating structure
- B. Discuss the locations of specific artifacts and their significance

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing Windows® operating systems.

2.2 Required Readings

- A. Carvey, Harlan. Windows® Forensic Analysis. 2009. Syngress Publishing, Inc. Chapter 5.
- B. Carvey, Harlan. Windows® Registry Forensics: Advanced Digital Forensic Analysis of the Windows® Registry. 2011. Syngress Publishing, Inc.
- C. NW3C WinArt (2017) Course Material – All PowerPoints and Reference Material

3 Practice

3.1 Basic or Special Skills

The ability to understand basic Windows artifacts of forensic importance.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation with installation of Windows®
- Forensic Software

3.4 Supervised Performance

Under guidance from the trainer or an experienced examiner, the trainee will explore Windows® operating systems highlighting areas of forensic importance.



4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-09 NON- WINDOWS® OPERATING SYSTEMS

Duration 2 weeks

Purpose The trainee will become familiar with the non-Windows® operating systems

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with certain non-Windows® operating systems.

Knowledge of the operating system structure is vital in forensic analysis in order to locate evidentiary data and to interpret the significance of the findings.

1.2 Practical

Following the completion of training, the trainee will be able to:

- A. Discuss the basic non-Windows® operating structure
- B. Discuss the location of specific artifacts and their significance

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing non-Windows® operating systems.

2.2 Required Readings

- A. Hansen, K.H., Toolan, F., Decoding the APFS file system, Digital Investigation (2017), <http://dx.doi.org/10/1016/j.diin.2017.07.003>
- B. Kubasiak, Ryan R. Morrissey, Sean. Mac OS X, iPod and iPhone Forensic Analysis DVD Toolkit. 2009. Syngress Publishing, Inc. Chapters 1-4 and 8-12.
- C. Linux Bible 8th Edition, 2012, Negus, Christopher. Chapters 9-12.
- D. NW3C MTI (2017) Course Material – Introduction to Macintosh, Live Triage Basics, Performing Live Triage, Macintosh Imaging

3 Practice

3.1 Basic or Special Skills

The ability to understand basic non-Windows® components specifically areas of forensic importance.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation
- Linux and Mac OS image file or installation
- Forensic Software



3.4 Supervised Performance

Under guidance from the trainer or an experienced examiner, the trainee will explore a Linux and Mac operating system highlighting areas of forensic importance.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.

4.3 Dependent Modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-02-10 SOFTWARE AND FILE IDENTIFICATION

Duration 2 days

Purpose The trainee will become familiar with general software and file identification

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of the training, the trainee will be familiar with general software and file identification.

During a forensic computer analysis, it is a common occurrence to locate applications or file types that are unfamiliar to the analyst. It is necessary to identify their function or source in order to determine their probative value.

1.2 Practical

Following the completion of training, the trainee will be able to discuss the process by which an unknown software application or file type can be identified.

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing software and file type identification including file naming systems and file header and footer.

2.2 Required Readings

Module 20 Forensic Analysis Required Readings Notebook – Signature Analysis tab

3 Practice

3.1 Basic or Special Skills

The ability to identify unknown software applications and file types.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation
- Forensic Software

3.4 Supervised Performance

Under guidance from the trainer or an experienced examiner, the trainee will use a hex editor to observe the naming structure and header/footer of known file types. The trainee will use Internet databases to identify various file extensions and software applications.

3.5 Independent Exercises

- A. The trainee will be required to identify unknown file types and software applications and the likelihood they have evidentiary value.
- B. The trainee will be required to find viewers for any files with possible evidentiary value.



4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-11 BASIC NETWORK TOPOLOGY

Duration 5 days

Purpose The trainee will become familiar with basic network topology

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with basic network topology.

A significant portion of forensic computer analysis deals with computers attached to a network, usually the Internet. Having a basic understanding of networking will allow the trainee to locate and identify artifacts of network usage.

1.2 Practical

Following the completion of training, the trainee will be able to discuss basic networking.

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing network topology.

2.2 Required Readings

- A. White, Ron. 2002. How Computers Work. Que Corporation, Chapters 24-28 and 30.
- B. Nelson, Phillips, & Steuart. 2009. Guide to Computer Forensics and Investigations Chapter 11.
- C. USSS/NCFI 2014 (or most recent) Basic Network Intrusion Training Course Notes.
- D. NW3C BNII (2017) Course Materials – All Course Materials and Reference Materials

3 Practice

3.1 Basic or Special Skills

None

3.2 Equipment

None

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-12 WEB-BASED ARTIFACTS

Duration 1 month

Purpose The trainee will become familiar with web-based artifacts such as internet history, email, instant messaging, cloud storage, and peer-to-peer file sharing.

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with web-based artifacts such as internet history, email, instant messaging, cloud storage, and peer-to-peer file sharing.

A significant portion of forensic computer analysis deals with computers attached to the Internet and require analysis of web-based artifacts. Having a basic understanding of the Internet, web browsers, email, cloud computing platforms, peer-to-peer clients and where to search for web-based artifacts will allow the trainee to conduct a more thorough analysis.

1.2 Practical

Following the completion of training, the trainee will be able to

- A. Discuss basic Internet protocols, web servers, and web pages
- B. Recognize and locate web browser artifacts
- C. Discuss email servers and email protocols, and analyze email headers
- D. Discuss instant messaging applications and recognize related artifacts
- E. Discuss cloud based storage and recognize artifacts left behind by cloud storage services
- F. Discuss peer-to-peer file sharing networks and recognize related artifacts

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles or chapters describing web-based artifacts.

2.2 Required Readings

- A. EnCase Internet and E-mail Examinations, 2002, Guidance Software, pp 35-39.
- B. Jones, Robert. Internet Forensics: Using Digital Evidence to Solve Computer Crimes. 2006. O'Reilly Media, Inc. Chapters 2, 3, 5, 6 and 7 and pages 107-109.
- C. Nelson, Phillips, & Steuart. 2009. Guide to Computer Forensics and Investigations. Chapter 12.
- D. Articles and white papers in the Instant Messaging Notebook (Skype Chat, MSN Messenger and Windows Live, Facebook, Yahoo Messenger, and Myspace IM – or readings related to newer Instant Messaging or Chat applications).

3 Practice

3.1 Basic or Special Skills

The ability to locate and identify web-based artifacts.



3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation
- Internet connectivity

3.4 Supervised Performance

Under guidance from the trainer or an experienced examiner, the trainee will examine web-based artifacts including, at a minimum, web pages, web browser artifacts, email, email header, instant messaging artifacts, cloud based storage artifacts, and peer-to-peer file sharing artifacts.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None

4.2 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-13 WIPING

Duration 2 days

Purpose The trainee will become familiar with creating sterile digital media

Prerequisite None

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will be familiar with creating sterile digital media.

In order to prevent cross-contamination when analyzing digital media, it is necessary to use forensic media that has been wiped of all data. This media is then classified as sterile media. This process should be completed prior to each case for each item of forensic media to be used.

1.2 Practical

Following the completion of training, the trainee will be able to create sterile forensic media

2 Training Outline

2.1 Lesson Plan

- A. The trainee will be required to read articles describing the wiping process.
- B. Under the supervision of a trainer or an experienced examiner, the trainee will create sterile digital media using various software applications.
- C. The trainee must demonstrate competency by successful completion of practical examination on wiping.

2.2 Required Readings

- A. Texas DPS DM SOP "DM-03-02 Acquisition of Digital Evidence"
- B. Texas DPS "Forensic Disk Wiping Log"

3 Practice

3.1 Basic or Special Skills

The ability to create sterile digital media.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation
- Various wiping software
- Various digital media

3.4 Supervised Performance

While in training, the wiping of digital media will be performed under observation of the trainer or experienced examiner.



4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Competency

The trainee must demonstrate competency by successful completion of a practical examination on wiping of digital media.

4.2 Written Examination

None

4.3 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-14 PERFORMANCE VERIFICATION/VALIDATION

Duration 2 weeks

Purpose The trainee will become familiar with performance verification/validation of hardware and software applications used in casework.

Prerequisite None

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will be familiar with performance verification/validation of hardware and software applications used in casework.

The results of a forensic analysis are dependent on the hardware and software utilized by the analyst. In order to ensure the hardware and software are reliable, it is necessary to conduct thorough performance verifications and validations.

1.2 Practical

Following the completion of training, the trainee will be able to complete a performance verification and/or validation on hardware and software and properly document the process and results.

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles or chapters describing performance verification/validation.

2.2 Required Readings

- A. Texas DPS DM Equipment Verifications
- B. Texas DPS DM Forensic Software Validations
- C. Crime Laboratory Service Manual, Validations and Performance Verifications Chapter
- D. Daniel, L. & Daniel, L. 2012. Digital Forensics for Legal Professionals. Chapter 5.
- E. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. "SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics" 2018.
- F. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. "SWGDE Recommended Guidelines for Validation Testing" 2014.

3 Practice

3.1 Basic or Special Skills

The ability to conduct a performance verification/validation on hardware and software for use in casework.

3.2 Supervised Performance

Under guidance from the trainer or an experienced examiner, the trainee will be required to conduct a mock performance verification/validation on forensic software and hardware. The trainee will be required to document the process and results.



Note: Performance verification in actual casework encountered while in supervised work will be performed under observation by the trainer or experienced examiner until authorized.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Competency

The trainee must demonstrate competency by successful completion of a performance verification/validation of hardware and software.

4.2 Written Examination

None

4.3 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-15 CASE DOCUMENTATION

Duration 2 days

Purpose The trainee will become familiar with basic documentation during digital media analysis

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with basic documentation during digital/multimedia analysis.

Results from a digital/multimedia analysis must be reproducible. In order to verify results, adequate documentation of the analysis must be completed.

1.2 Practical

Following the completion of training, the trainee will be able to adequately document the analysis performed.

2 Training Outline

2.1 Lesson Plan

The trainee will be required to review notes as produced by a qualified examiner on at least 10 cases

2.2 Required Readings

- A. Texas DPS DM SOP "DM-03-02 Acquisition of Digital Evidence"
- B. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. "SWGDE Best Practices for Computer Forensics" 2014.

3 Practice

3.1 Basic or Special Skills

The ability to take adequate notes during analysis.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

- A. The quality of documentation should improve as the trainee gains experience.
- B. The trainer and experienced examiners share the responsibility to establish high standards for documentation.
- C. Technical and administrative review of the trainee's casework will continuously provide opportunities to point out areas of documentation that can be improved.

4.2 Written Examination

None.

4.3 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-16 FORENSIC ACQUISITION

Duration 3 weeks

Purpose The trainee will become familiar with performing forensic acquisitions of digital media using EnCase®, FTK Imager, Tableau Forensic Duplicator, or other current acquisition tools or methods approved for use in the laboratory.

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with performing forensic acquisitions of digital media using EnCase®, FTK Imager, Tableau Forensic Duplicator or other current acquisition tools or methods approved for use in the laboratory. The goal of a forensic acquisition is to create an exact digital copy (forensic image) of the evidence without altering it. The integrity of the digital copy should be verified by comparing the hash value of the original evidence to that of the digital copy. The forensic analysis can then be performed on the forensic image in order to limit the handling of original evidence.

1.2 Practical

Following the completion of training, the trainee will be able to:

- A. Navigate the user interface and create forensic images using EnCase®, FTK Imager, Tableau Forensic Duplicator, or other current acquisition tools approved for use in the laboratory.
- B. Generate a hash value of the forensic image if not done automatically by the forensic imaging tool.

2 Training Outline

2.1 Lesson Plan

- A. The trainee will observe the trainer or experienced examiner perform acquisitions with EnCase®, FTK Imager, Tableau Forensic Duplicator, or other current acquisition tools or methods approved for use in the laboratory.
- B. The trainee will observe the creation and comparison of hash values to verify the integrity of the forensic image. The trainer will acquire multiple types of digital media using various acquisition methods.
- C. Under the supervision of a trainer or an experienced examiner, the trainee will perform acquisitions using EnCase®, FTK Imager, Tableau Forensic Duplicator, or other current acquisition tools or methods approved for use in the laboratory.
- D. The trainee will create and compare hash values to verify the integrity of the forensic image.
- E. The trainee will acquire multiple types of digital media, using various acquisition methods.
- F. The trainee must successfully complete practical examinations on acquisition using EnCase®, FTK Imager, Tableau Forensic Duplicator, or other current acquisition tools or methods approved for use in the laboratory.



2.2 Required Readings

- A. Texas DPS DM SOP “DM-03-02 Acquisition of Digital Evidence”
- B. EnCase® Computer Forensics I (Private Sector Series). 2007. Lesson 11, pages 119-126.
- C. Access Data® FTK BootCamp Training Manual. 2010 Pages 49-74. (Not required for A/V Analysts)
- D. TD3 Forensic Imager User Guide or TD2u Forensic Duplicator User Guide from the Guidance Software website www.guidancesoftware.com
- E. EnCE Study Guide, 3rd Edition. Chapter 4, pages 120-176 and 180-197 (Not required for A/V Analysts)
- F. NW3C BDRA (2016) Course Material – Imaging at the Scene, Shutdown Process, Duplicate Imaging
- G. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. “SWGDE Best Practices for Computer Forensic Acquisitions” 2018.
- H. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. “SWGDE Capture of Live Systems” 2014.
- I. Additionally, Audio/Video/Image Analysts are required to read the DVR Examiner User Certification Course Training Manual

3 Practice

3.1 Basic or Special Skills

The ability to

- A. Create forensic images using EnCase®, FTK Imager, Tableau Forensic Duplicator, or other current acquisition tools or methods approved for use in the laboratory.
- B. Create and compare hash values to verify the integrity of the forensic image.
- C. Use various acquisition methods.
- D. Acquire various types of digital media.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation
- Various types of digital media
- Controlled boot floppy, disk/disc, or USB (For CF Analysts only)
- EnCase®, FTK Imager, Tableau Forensic Duplicator, and other forms of acquisition methods.

3.4 Supervised Performance

The acquisition of digital media using EnCase®, FTK Imager, Tableau Forensic Duplicator, or other current acquisition tools or methods approved for use in the laboratory are necessary in



casework encountered while in supervised work. Use of these tools or methods will be performed under observation by the trainer or experienced examiner until authorized.

3.5 Independent Exercises

- A. The trainee must successfully complete practical exercises on acquisitions of various types of digital media using tools such as EnCase®, FTK Imager, Tableau Forensic Duplicator, or other current acquisition tools or methods approved for use in the laboratory.
- B. The trainee must complete practical exercises for the following:
 1. Acquisition of various types of Digital Media, such as hard disk drives, SD cards, thumb drives, DVRs, and/or CDs/DVDs – note that hash values do not need to be calculated for CD/DVD evidence if acquired using Windows, IsoBuster or Roxio (or comparable software) to generate the copy as the media is not easily written to or altered. (A/V Analysts should also include a DVR acquisition)
 2. Boot disk acquisition or live acquisition (with FTK Imager, Paladin, or similar acquisition tool. (For CF Analysts only)
 3. Acquisition using a software tool such as FTK Imager or EnCase® in conjunction with a physical or software write-blocker. (A/V Analysts should use DVR Examiner in place of FTK Imager)
 4. Acquisition using a hardware component such as the Tableau Forensic Imager (TD3) or Tableau Forensic Duplicator (TD2u), if approved for use in the laboratory.

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Competency

The trainee must complete a competency in the forensic acquisition of digital evidence.

4.2 Written Examination

None

4.3 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-17 FORENSIC ANALYSIS

Duration 2 months

Purpose The trainee will become familiar with performing forensic analysis of digital media using forensic software.

Prerequisite DM-TM-02-01 through DM-TM-02-10, DM-TM-02-12

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will be familiar with performing forensic analysis of digital media using forensic software.

Forensic analysis of digital media is performed on a forensic image of the evidence. There are numerous methods to organize, view, and search the data on the image. Analysis techniques may consist of performing complex keyword searches, signature analysis, carving data from unallocated space, or viewing data at the byte level.

1.2 Practical

Following the completion of training, the trainee will be able to:

- A. Analyze forensic images and conduct various forensic analysis functions using software approved for use in the laboratory
- B. Navigate the user interface of the software and conduct forensic analysis functions available within the forensic software

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing various analysis techniques.

2.2 Required Readings

- A. Texas DPS DM SOP "DM-03-04 Examination of Digital Evidence"
- B. EnCase® Computer Forensics II. 2007. Lesson 5 Recovery Module pages 49-82.
- C. Module 20 Notebook with articles and white papers on EnCase®, FTK, signature analysis, dtSearch, EnScripts, file/image mounting, and partition recovery.
- D. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. "SWGDE Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis" 2018.

3 Practice

3.1 Basic or Special Skills

The ability to analyze forensic images using various analysis techniques.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.



3.3 Equipment

- Forensic workstation
- Various forensic images
- Software approved for use in casework

3.4 Observed Performance

The trainee will observe the trainer or experienced examiner perform various analysis techniques such as keyword searching, data carving, and file signature analysis.

3.5 Supervised Performance

The analysis of digital media using various analysis techniques is necessary in actual casework, and when encountered while in supervised work, will be performed under observation by the trainer or experienced examiner until authorized.

Note: If the opportunity to observe a process is unavailable during this training, the process will be discussed. All listed processes are included in the Required Readings.

3.6 Independent Exercises

The trainee must complete practical exercises for the following forensic analysis functions:

- A. Navigation of the user interface of forensic analysis software
- B. Signature analysis and byte level analysis
- C. Keyword search (including Indexed Search and Live Search, if using FTK)
- D. Hashing
- E. Data carving
- F. Examination of Volume Shadow Copies
- G. Windows Registry analysis
- H. Creating and using filters to view only specific data (if using FTK)
- I. Mounting compound files
- J. View file metadata
- K. Internal and external file viewers
- L. Bookmarking
- M. Exporting
- N. Restoring a forensic image

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Competency

The trainee must demonstrate competency by successful completion of practical exercise(s) on forensic analysis using various analysis techniques

4.2 Written Examination

None



4.3 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-18 MOBILE DEVICES

Duration 2 months

Purpose The trainee will become familiar with the isolation and extraction of data from various types of mobile devices.

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with various types of mobile devices, isolation methods, and data extraction types and methods. Mobile devices may consist of mobile phones, tablets, drones, GPS devices, Internet of Things (IoT) devices, and credit card/gas pump skimmers.

1.2 Practical

Following the completion of training, the trainee will be able to:

- A. Identify various mobile devices, recognize data ports/cables, identify operating systems and relevant configuration settings
- B. Isolate various mobile devices from signals, as applicable
- C. Identify and explain various extraction types
- D. Extract data from mobile devices using various extraction methods
- E. Conduct a manual examination of a mobile device
- F. Perform minor repairs to a mobile device, as applicable

2 Training Outline

2.1 Lesson Plan

- A. The trainee will be required to read articles on mobile devices.
- B. Under guidance from the trainer or an experienced examiner, the trainee will be required to observe the isolation and extraction of data from various mobile devices. The trainee will also use various mobile devices to become familiar with their capabilities.

2.2 Required Reading

NOTE: Mobile device technology changes on a daily basis. For this reason, the trainer or experienced examiner will provide the most current relevant white papers and/or articles for the trainee to read and document.

- A. Module 24 Notebook with articles and white papers on Cellebrite, cell phone forensics, and GPS forensics.
- B. Hoog, Andrew. 2011. Android Forensics. Chapter 6.
- C. Kubasiak & Morrissey. 2009. Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit. Chapters 13-16.
- D. Reiber, Lee. 2016. Mobile Forensic Investigations.
- E. Mahalik & Bommisetty. 2016. Practical Mobile Forensics.



- F. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents.
“SWGDE Best Practices for Chip-off” 2016.
- G. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents.
“SWGDE Best Practices for Examining Magnetic Card Readers” 2018.
- H. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents.
“SWGDE Best Practices for Examining Mobile Phones Using JTAG” 2015.
- I. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents.
“SWGDE Best Practices for Portable GPS Device Examinations” 2012.

3 Practice

3.1 Basic or Special Skills

The ability to isolate and extract data from various mobile devices

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Various mobile devices and their peripherals
- Radio Frequency (RF) Room
- Ramsey Isolation Box (RIB)
- Forensic workstation
- Camera
- Repair kit
- Sterile or blank digital media/target media (USBs, SD cards, SIM cards, HDDs, etc)

3.4 Observed Performance

The trainee will observe the trainer or experienced examiner isolate various mobile devices, perform a manual examination, and perform a logical, file system, and physical extraction from a mobile device.

3.5 Independent Exercises

The trainee must complete practical exercises for the following:

- A. Isolate a minimum of three (3) mobile devices and document the method used
- B. Perform a logical extraction and document the steps
- C. Perform a file system extraction and document the steps
- D. Perform a physical extraction of one (1) iOS device and one (1) Android device, as available, and document the steps
- E. Perform a manual examination and document the steps

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

None



4.2 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-19 MOBILE DEVICE ANALYSIS

Duration 2 months

Purpose The trainee will become familiar with performing analyses of mobile devices

Prerequisite DM-TM-02-18 (Mobile Devices)

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will be familiar with performing forensic analyses of various mobile devices, such as mobile phones, tablets, drones, GPS devices, Internet of Things (IoT) devices, and credit card/gas pump skimmers.

1.2 Practical

Following the completion of training, the trainee will be able to analyze the content various types of mobile devices. The trainee will become familiar with the functions of forensic software used during the analyses of mobile devices.

2 Training Outline

2.1 Lesson Plan

The trainee will be required to read articles describing analyses of mobile devices.

2.2 Required Readings

NOTE: Mobile devices technology changes on a daily basis. For this reason, the trainer or experienced examiner will provide the most current relevant white papers and/or articles to read and document.

- A. User Guides for each software application to be used in analysis.
- B. NW3C iDF (2017) Course Material – All PDFs
- C. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. “SWGDE Best Practices for Mobile Phone Forensics” 2013.

3 Practice

3.1 Basic or Special Skills

The ability to analyze mobile devices

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation
- Various mobile devices and data cables
- Various forensic software such as:
 - Cellebrite Touch and Physical Analyzer
 - XRY
 - Axiom
 - BerlaCorp Blackthorn2



3.4 Observed Performance

The trainee will observe the trainer or experienced examiner perform analyses of various types of mobile devices, as available.

3.5 Supervised Performance

- A. The trainee will observe the trainer or experienced examiner perform analyses of various types of mobile devices until the trainer and trainee believe the trainee is competent to perform analysis independently.
- B. Under the supervision of a trainer or an experienced examiner, the trainee will perform analyses of various types of mobile devices, as available.

3.6 Independent Exercises

The trainee must demonstrate ability by successful completion of practical exercises on the analysis of mobile devices, including various analyses functions such as:

- A. Examine various mobile phone/tablet operating systems (iOS and Android)
- B. Examine other mobile devices, as available, such as drones, GPS devices, Internet of Things (IoT) devices, and credit card/gas pump skimmers
- C. Examine peripheral media such as SIM cards and micro SD cards
- D. Hash extracted data
- E. Data carve
- F. Scan for malware
- G. Examine relevant databases
- H. Keyword search

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Competency

The trainee must demonstrate competency by the successful completion of a competency test on the analysis of a mobile device.

4.2 Written Examination

None

4.3 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



DM-TM-02-20 REPORTING

Duration 1 week

Purpose The trainee will become familiar with reporting the results of forensic analysis of digital media.

Prerequisite None

1 Objectives

1.1 Theoretical

Following completion of training, the trainee will be familiar with reporting the results of forensic analysis of digital evidence.

The results of a forensic analysis are sometimes complicated and can seem overly technical to a layperson if not reported in a clear manner. In order to successfully convey the results, it is necessary to create a report that is clear and concise.

1.2 Practical

Following the completion of training, the trainee will be able to report results of a forensic analysis. The trainee will become familiar with the reporting functions included with various forensic software applications.

2 Training Outline

2.1 Lesson Plan

- A. The trainee will be required to review at least 10 digital reports and LIMS reports created by the trainer or an experienced examiner
- B. Under the supervision of a trainer or an experienced examiner, the trainee will create a mock report of a forensic analysis (including the digital report and entry into LIMS).
- C. The trainee must demonstrate ability by successful completion of practical exercise(s) on reporting.

2.2 Required Readings

- A. Pixley, B.W. (2013). Report Writing Handbook for the Computer Examiner.
- B. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents. "SWGDE Requirements for Report Writing in Digital and Multimedia Forensics" 2018.
- C. Texas DPS Crime Laboratory Service Manual:
 1. Laboratory Reports, Letters, and Certificates Chapter
 2. Electronic Storage and Archival of Records Chapter

3 Practice

3.1 Basic or Special Skills

The ability to create a report from results of a forensic analysis.

3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.



3.3 Equipment

- Forensic workstation
- Forensic software

3.4 Independent Exercises

- A. The trainee will be required to review at least 10 reports created by the trainer or an experienced examiner, specifically reviewing the following:
 - A. Name and address of the laboratory and the location where the tests were carried out
 - B. Case report title
 - C. Page number and total number of pages on all pages of the report
 - D. Issue date of the report (defined as the date the administrative review is completed) on all pages of the report
 - E. Laboratory case number on all pages of the report
 - F. Name of the requesting agency representative and agency name and address
 - G. Submitting agency's case number (if available)
 - H. Item number (including agency assigned item number if different from LIMS assigned number) and description of that item's packaging (i.e. one-gallon metal can, etc.)
 - I. Offense information (county and date, if available)
 - J. Description of evidence (if available)
 - K. Date of receipt and date of analysis
 - L. Results and explanation of results
 - M. Any qualifying statements (i.e. possible contamination issues, proper seal issues, etc.)
 - N. Type of analysis performed and test method used
 - O. Name and title of analyst performing work
 - P. Statement of Qualifications and Disclosures, where practicable

4 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

4.1 Written Examination

The trainee will complete either a verbal or written test on report writing.

4.2 Requirements for use in casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework.

4.3 Dependent modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-02-21 CASE REVIEW

Duration 1 week

Purpose To familiarize the trainee with the process of technical and administrative review.

Prerequisite None

1 Objectives

1.1 Theoretical

The laboratory reports and conclusions must be reviewed prior to release. In order to ensure quality, accuracy, and conformance to approved methods and applicable laboratory policies and procedures, it is necessary to conduct thorough reviews of case documentation.

1.2 Practical

Following the completion of training, the trainee will be able to:

- A. Technically review a completed case record.
- B. Administratively review a completed case record.

2 Training Outline

2.1 Lesson Plan

- A. The components of a DM specific technical review include:
 1. Ensure proper technical procedures were followed during testing
 2. Ensure data transfers are accurate (example: verify hash values)
 3. Verify that sufficient documentation is contained within the case record, including evidence inventory, chain-of-custody, disposition of evidence (as appropriate)
 4. Ensure conformance with approved methods and applicable management system documents
 5. Ensure that items within the DM specific technical review worksheet (LAB-DM-11 for CF/MF or LAB-DM-12 for A/V) are included in the technical review process
 6. Ensure test reports contain all required information and are accurate
 7. Ensure the technical records support the results, interpretations, opinions, and conclusions in the test report
 8. Ensure qualified statements are included where relevant
- B. The components of an administrative review include:
 1. Ensure that all administrative and test records are uniquely identified, such as by case number
 2. Ensure that the test report contains all required elements and accurate information
 3. Ensure the accuracy of spelling and grammar. Ensure that logical and complete statements are used and that the information in the report is supported by the test record



C. Special Circumstances

Preliminary results: Preliminary results may be released to submitting agencies per their request in order to aid in investigation as long as they have been technically reviewed and documented in the case record. A technical review worksheet (LAB-DM-11 for CF/MF or LAB-DM-12 for A/V) is not required when technically reviewing preliminary results as long as the technical review is otherwise documented in the case record.

2.2 Required Readings

Texas DPS Crime Laboratory Service Manual –Technical Review Chapter and Administrative Review Chapter

3 Practice

3.1 Safety

None

3.2 Observed Performance

The trainer or experienced examiner will demonstrate and discuss the technical and administrative review of at least three (3) cases.

3.3 Independent Exercises

The trainee will perform five (5) technical and administrative reviews on previously examined case records. The process and results should be documented.

4 Assessment

4.1 Competency and Qualifying Examination

The trainee will complete either a verbal or written test on case review.

4.2 Evaluation of Training

Successful completion of this module is determined by the trainer and is a prerequisite for casework.



03 FORENSIC AUDIO/VIDEO/IMAGE ANALYSIS UNIT

DM-TM-03-01 FORENSIC IMAGE ANALYSIS

Duration 1 month

Purpose Familiarize the trainee with theoretical and practical aspects of Forensic Image Analysis

Prerequisite DM-TM-02-01, DM-TM-02-04, DM-TM-02-13, DM-TM-02-14, DM-TM-02-16

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will be familiar with performing forensic image analysis of analog and digital media using various forensic image analysis tools.

Forensic image analysis of digital media is performed on a forensic image of the evidence. Forensic image analysis of analog media is performed on a digital copy of the original analog evidence. There are numerous methods to extract, capture and enhance the image or digital copy. Commercial forensic software allows many of these methods to be automated or simplified. Each forensic software suite has a different user interface and capabilities.

1.2 Practical

Following the completion of training the trainee will be able to perform forensic image analysis on evidentiary image media, in both analog and digital formats.

2 Training Outline

2.1 Lesson Plan

- A. The trainee will observe the trainer or experienced examiner perform analysis with various forensic image analysis tools. The trainer will examine multiple types of media and formats.
- B. The trainee must complete practical exercise(s) on analysis using the various forensic image analysis tools.

2.2 Required Readings

- A. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents, "SWGDE Image Processing Guidelines" 2016.
- B. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents, "SWGDE Best Practices for Maintaining the Integrity of Imagery" 2017.
- C. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents, "SWGDE Digital Image Compression and File Formats Guidelines" 2016.
- D. Amped FIVE Training Material
- E. Adobe Photoshop User Guide

2.3 Basic or Special Skills

The ability to analyze image evidence using various forensic image analysis tools.



2.4 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

2.5 Equipment

- Forensic workstation
- Various forensic image analysis tools
- Still Image files
- Analog media

2.6 Supervised Performance

- A. The analysis of analog and digital media using the various forensic image analysis tools necessary in actual casework encountered while in supervised work will be performed under observation by the trainer or experienced examiner until authorized.

Note: If the opportunity to observe a process is unavailable during this training, the process will be discussed.

- B. The trainee will successfully complete practical exercises on analysis of forensic image copies using various forensic image analysis tools. The trainee must complete practical exercises for the following:

1. Forensic Image creation, verification, and integrity
2. Hashing
3. Viewing and understanding metadata
4. Image processing techniques
5. Image enhancement techniques
6. Evidence handling and packaging

3 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

3.1 Competency

Competency samples containing known data will be given to the trainee to ensure proper procedures and techniques are used in the analysis of image evidence.

3.2 Written Examination

The trainer will administer a written examination.

3.3 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework, both supervised and independent.

3.4 Dependent Modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-03-02 FORENSIC VIDEO ANALYSIS

Duration 4 months

Purpose Familiarize the trainee with theoretical and practical aspects of Forensic Video Analysis

Prerequisite DM-TM-02-01, DM-TM-02-02, DM-TM-02-04, DM-TM-02-05, DM-TM-02-06, DM-TM-02-13, DM-TM-02-14, DM-TM-02-16

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will be familiar with performing forensic video analysis of analog and digital media using various forensic video analysis tools.

Forensic video analysis of digital media is performed on a forensic image of the evidence. Forensic video analysis of analog media is performed on a digital copy of the original analog evidence. There are numerous methods to extract, capture and enhance the image or digital copy. Commercial forensic software allows many of these methods to be automated or simplified. Each forensic software suite has a different user interface and capabilities.

1.2 Practical

Following the completion of training the trainee will be able to perform forensic video analysis on evidentiary video media, in both analog and digital formats.

2 Training Outline

2.1 Lesson Plan

- A. The trainee will observe the trainer or experienced examiner perform analysis with various forensic video analysis tools. The trainer will examine multiple types of media and formats.
- B. The trainee must successfully complete practical exercise(s) on analysis using the various forensic video analysis tools.

2.2 Required Readings

- A. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents, "SWGDE Technical Overview of Digital Video Files" 2017.
- B. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents, "SWGDE Technical notes on FFmpeg" 2018.
- C. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents, "SWGDE Best Practices for Digital Forensic Video Analysis" 2018.
- D. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents, "SWGDE Best Practices for Data Acquisition from Digital Video Recorders" 2018.
- E. Amped FIVE Training Manual

2.3 Basic or Special Skills

The ability to analyze video evidence using various forensic video analysis tools.

2.4 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.



2.5 Equipment

- Forensic workstation
- Various forensic video analysis tools
- Video files
- Analog media

2.6 Supervised Performance

- A. The analysis of digital media using the various forensic video tools necessary in actual casework encountered while in supervised work will be performed under observation by the trainer or experienced examiner until authorized.

Note: If the opportunity to observe a process is unavailable during this training, the process will be discussed.

- B. The trainee will successfully complete practical exercises on analysis of forensic images or copies using various forensic video tools. The trainee must complete practical exercises for the following:

1. Video data recovery
2. Forensic image creation, verification, and integrity
3. Hashing
4. Viewing and understanding metadata
5. Playback optimization
6. Video processing techniques
7. Video editing
8. Video enhancement techniques
9. Evidence handling and packaging

3 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

3.1 Competency

Competency samples containing known data will be given to the trainee to ensure proper procedures and techniques are used in the analysis of video evidence.

3.2 Written Examination

The trainer will administer a written examination.

3.3 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework, both supervised and independent.

3.4 Dependent Modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



DM-TM-03-03 FORENSIC AUDIO ANALYSIS

Duration 1 month

Purpose Familiarize the trainee with theoretical and practical aspects of Forensic Audio Analysis

Prerequisite DM-TM-02-01, DM-TM-02-04, DM-TM-02-13, DM-TM-02-14, DM-TM-02-16

1 Objectives

1.1 Theoretical

Following the completion of training, the trainee will be familiar with performing forensic audio analysis of analog and digital media using various forensic audio analysis tools.

Forensic audio analysis of digital media is performed on a forensic image of the evidence. Forensic audio analysis of analog media is performed on a digital copy of the original analog evidence. There are numerous methods to extract, capture and enhance the image or digital copy. Commercial forensic software allows many of these methods to be automated or simplified. Each forensic software suite has a different user interface and capabilities.

1.2 Practical

Following the completion of training the trainee will be able to perform forensic audio analysis on evidentiary audio media, in both analog and digital formats.

2 Training Outline

2.1 Lesson Plan

- A. The trainee will observe the trainer or experienced examiner perform analysis with various forensic audio analysis tools. The trainer will examine multiple types of media and formats.
- B. The trainee must successfully complete practical exercise(s) on analysis using the various forensic audio analysis tools.

2.2 Required Readings

- A. Scientific Working Group on Digital Evidence Website, www.swgde.org/documents, "SWGDE Best Practices for Forensic Audio" 2016.
- B. Introduction to Forensic Audio Analysis training materials

2.3 Basic or Special Skills

The ability to analyze audio evidence using various forensic audio analysis tools.

2.4 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

2.5 Equipment

- Forensic workstation
- Various forensic audio analysis tools
- Audio files
- Analog media



2.6 Supervised Performance

- A. The analysis of analog and digital media using the various forensic audio tools necessary in actual casework encountered while in supervised work will be performed under observation by the trainer or experienced examiner until authorized.

Note: If the opportunity to observe a process is unavailable during this training, the process will be discussed.

- B. The trainee will successfully complete practical exercises on analysis of forensic image copies using various forensic audio tools. The trainee must complete practical exercises for the following:

1. Forensic image creation, verification, and integrity
2. Hashing
3. Viewing and understanding metadata
4. Playback optimization
5. Audio processing techniques
6. Audio editing
7. Audio enhancement techniques
8. Evidence handling and packaging

3 Assessment

The trainee and trainer will complete a checklist and sign-off sheet.

3.1 Competency

Competency samples containing known data will be given to the trainee to ensure proper procedures and techniques are used in the analysis of audio evidence.

3.2 Written Examination

The trainer will administer a written examination.

3.3 Requirements for use in Casework

Successful completion of this module is determined by the trainer and is a prerequisite for casework, both supervised and independent.

3.4 Dependent Modules

Successful completion of this module is determined by the trainer and is a prerequisite for all further training.



04 INTERNAL DEPARTMENT PHOTOGRAPHIC SUPPORT UNIT

DM-TM-04-01 SUSPECT LINEUP ENHANCEMENTS

Duration 1 week

Purpose Familiarize the trainee with creating composite imagery using portions of other images or artwork, or with removing unwanted persons or details from an image to achieve a predetermined effect.

Prerequisite DM-TM-03-01

1 Objectives

1.1 Theoretical

The physical layering of items in a controlled manner (superimposed on layers and scaled proportionately) enables the examiner to create a merged image to achieve a desired effect. Successful superimposition of multiple images requires that the subject matter be scaled so that the proportions and the perspective of the individual elements appear correct in relationship to each other.

1.2 Practical

Following the completion of training the trainee will be able to:

- A. Format and align desirable characteristics on layers
- B. Create a composite image to achieve a predetermined effect
- C. Remove unwanted characteristics from an image

1.3 Theory

Many times investigating officers will have a picture of a suspect that they want to use in a lineup, but it contains other persons or things that need to be removed. In other instances, the officer may have obtained more current information on the suspect and want to reflect those changes in an image that is to be widely distributed.

2 Training Outline

2.1 Lesson Plan

- A. Master all aspects of the computer software associated with transparency layers, extracting selections, repairing images, and other controls relating to merging images.
- B. Experienced imaging specialist will demonstrate these techniques and show the trainee how to enhance these types of images.

2.2 Required Readings

Current edition Adobe Photoshop User Guide / Ref. "Transparency layers, Repairing images, Extracting selections, Merge" (May include others as needed)

3 Practice

3.1 Basic or Special Skills

Basic familiarity with Enhancement software usage and digital image acquisition.



3.2 Safety

The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation
- Various digital images
- Enhancement software

3.4 Practical Exercises

- A. Trainee will practice enhancing an APB (all-points bulletin) photograph by changing the characteristics of the person. They will practice removing and repairing a group photograph so that one individual can be used in a lineup format.
- B. Trainee will perform these techniques to understand the basic strategy that is required for these types of images.



DM-TM-04-02 PHOTOGRAPHIC OVERLAYS

Duration 1 week

Purpose Familiarize the trainee with creating life-size images in an overlay format for forensic assessment of corresponding features or areas of interest for the purpose of rendering an opinion as to whether the subject is consistent with or clearly different from an original.

Prerequisite DM-TM-03-01

1 Objectives

1.1 Theoretical

The physical comparison of items in a controlled manner (1:1 and superimposed) involves demonstrating unique characteristics of an item, which would differentiate it from other objects, persons, or areas of forensic interest that are similar in nature. Successful superimposition of 2 images to show similarities necessitates a similar camera angle in addition to life-size scaling. If there is distortion present in the increment of measurement within the image, then it becomes useless as a tool for extracting an accurate life-size image for forensic comparisons.

1.2 Practical

Following the completion of training the trainee will be able to:

- A. Format and align life-size characteristics for optimum comparisons.
- B. Determine the forensic expertise needed for comparison if the evidence was not already transferred by an examiner for enhancement.
- C. Work with that examiner to enhance the areas that they indicate may or may not be of significant forensic value.

2 Training Outline

2.1 Lesson Plan

- A. Master all aspects of the computer software associated with transparency layers, extracting selections, perspective grid, and other controls relating to the creation of overlays.
- B. Experienced imaging specialist will demonstrate these techniques and show the trainee how to create overlays using two images.
- C. Experienced imaging specialist will demonstrate how to isolate different types of evidence so that they can be used most effectively in the creation of an overlay.

2.2 Required Readings

- A. Current edition Adobe Photoshop User Guide / Ref. "Transparency layers, Perspective grid, Extracting selections" (May include others as needed).
- B. Robinson, Edward M. 2010. Crime Scene Photography Second Edition. Page 550-556.
- C. The Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Maintaining the Integrity of Imagery, Version 1.0, July 18, 2017.
- D. The Scientific Working Group on Digital Evidence (SWGDE) Digital Image Compression and File Formats Guidelines, Version 1.0, June 23, 2016.



3 Practice

3.1 Basic or Special Skills

Basic familiarity with enhancement software usage and digital image acquisition

3.2 Safety

- A. Standard evidence handling precautions (where applicable).
- B. The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.

3.3 Equipment

- Forensic workstation
- Various digital images
- Enhancement software

3.4 Practical Exercise

- A. Trainee will create several overlay comparisons (to scale) for court displays as indicated by an examiner for each discipline. Trainee will label and show unique characteristics in a manner which is appropriate for each discipline.
- B. Trainee will perform techniques from this module until able to create overlay displays.

3.5 Quality Control

The examiner in each discipline has the final approval as to whether the resulting overlay comparison is to scale and forensically appropriate for Courtroom display. Any experienced examiner (or the examiner submitting the evidence for enhancement) has the ability to show whether the resulting image is in fact life-size or if it contains distortions by referencing the final result using an appropriate scale.

4 Assessment

4.1 Competency

Known competency samples will be given to the trainee to ensure proper procedures and techniques are used in the creation of photographic overlays.



DM-TM-04-03 DIGITAL DISPLAYS FOR COURT

Duration 1 week

Purpose Familiarize the trainee with creating large-format evidentiary displays in all forensic disciplines

Prerequisite DM-TM-03-01

1 Objectives

1.1 Theoretical

Displays can be unmounted or mounted on mat board or foam core, hinged or unhinged to fold for easier transport, have text, lines, arrows, highlighting, or other desired features added digitally. Features overlaid on top of evidence can have a specified degree of transparency.

1.2 Practical

Following the completion of training the trainee will be able to:

- A. Format and align evidence, text, and highlighting for optimum visibility
- B. Add transparency overlays if desirable
- C. Scale proportionately and print to the large-format printer
- D. Finish display by mounting to a foam core or mat board

2 Training Outline

2.1 Lesson Plan

- A. Master all aspects of the computer software associated with canvas size, cropping, layers, and other controls relating to the creation of Court displays.
- B. Experienced imaging specialist will demonstrate these techniques and show the trainee how to create displays.
- C. Experienced imaging specialist will demonstrate the different types of labeling required for different types of evidence and the typical layouts used by each discipline.
- D. Experienced imaging specialist will demonstrate mounting techniques.

2.2 Required Readings

Current edition Adobe Photoshop User Guide / Ref. "Canvas size, Cropping, Layers, Text Controls, Image size, Transparency" (May include others as needed)

3 Practice

3.1 Basic or Special Skills

Basic familiarity with Enhancement software usage and digital image acquisition.

3.2 Safety

- A. The trainee should be aware that installed computer components have the potential danger of electrical shock and should be handled accordingly.
- B. The trainee should be aware that the hot mounting press and taking iron could cause burns if the platen is touched (100°– 300°F).
- C. The trainee should use caution when handling sharp objects.



3.3 Equipment

- Forensic Workstation
- Various digital images
- Enhancement software
- Dry Mounting/Laminating Press

3.4 Practical Exercises

- A. Trainee will perform techniques from this module until able to create Court displays.
- B. Trainee will create several displays as indicated by an examiner for each discipline. Trainee will label and show unique characteristics in a manner which is appropriate for each discipline, add transparencies if desired, then mount each display.

3.5 Quality Control

The examiner in each discipline has the final approval as to whether the resulting comparison is to scale and forensically appropriate for Courtroom display.

4 Assessment

4.1 Competency

Known competency samples will be given to the trainee to ensure proper procedures and techniques are used in the creation of court displays.



05 FORMS

TRAINING FORMS

	Document Name	FRN
1	Digital/Multimedia Computer Cases	LAB-DM-TM-01
2	External Training Courses	LAB-DM-TM-02
3	Digital/Multimedia Computer Forensics/Mobile Forensics Training Checklist	LAB-DM-TM-03
4	Digital/Multimedia Audio/Video/Image and Photography Training Checklist	LAB-DM-TM-04