Department of Forensic Science

COPYRIGHT © 2017

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

DIGITAL & MULTIMEDIA EVIDENCE SECTION PROCEDURES MANUAL

UNCONTROLLED COPY

TABLE OF CONTENTS

1 INTRODUCTION

The Digital & Multimedia Evidence (DME) Section encompasses the preservation, processing, and analysis of evidence in an analog or digital format. The section is divided into the sub-disciplines of Computer & Mobile Device Analysis and Video Analysis (including Image Analysis).

> Computer & Mobile Device Analysis involves the scientific examination, repair (if possible), analysis and/or evaluation of electronically stored information contained on a wide variety of data storage devices. These devices include, but are not limited to: computer systems, such as servers, desktops, digital video recorders (DVR), and laptops; mobile devices, such as cellular telephones and tablets; digital storage devices, such as hard disk drives, flash memory and optical discs.
>
> Video Analysis involves the scientific examination, repair (if possible) and clarification of analog or digital video recordings for the purpose of improving the visual appearance of specific features within the video recording or the overall recording. These recordings can originate from a variety of recording devices including, but not limited to: mobile devices, video cameras or surveillance systems.
>
> > Image Analysis involves the clarification of analog or digital images for the purpose of improving the visual appearance of specific features within an image or the overall image itself. Image analysis can be conducted on an area of interest (AoI) obtained from video evidence and other sources.

2 EQUIPMENT MAINTENANCE & QUALITY ASSURANCE

2.1 Introduction

2.1.1 The reliability and performance of the equipment used in the examination of digital evidence is checked to ensure the equipment is operating properly.

2.1.2 It is expected that the examiners will report any anomalous performance of the equipment immediately to the Section Supervisor.

2.2 Equipment

2.2.1 Equipment consists of hardware (e.g., computer system, audio/video player/recorder), firmware and/or software (e.g., application, program, utility, command, component).

2.2.2 All equipment is to be maintained in accordance with the manufacturer's specifications and recommendations as per operating and warranty manuals.

2.2.3 All maintenance is to be documented and retained in the appropriate log located in the section.

2.3 Equipment Validation, Verification and Use

2.3.1 DME examiners should use approved and appropriate equipment or follow procedures for deviation documented in the Quality Manual.

2.3.2 DME examiners are able to use Forensic Equipment, Common-Use Equipment, Native Equipment, and Operating System Equipment, and to perform the processes described in this document.

2.3.3 The following definitions apply regarding equipment used for processes described in this document:

- Forensic Equipment (FE) – Equipment used to acquire, view, process, or analyze data created by other equipment and intended for specific use within digital and multimedia forensic analyses. This equipment is generally regarded as reliable by merit of the testing and validation conducted by the developer, as well as by the widespread use in the digital and multimedia forensic community; however, additional validation may be required.
- Common-Use Equipment (CUE) – Equipment used to acquire, view, process, or analyze data created by other equipment or the CUE, and intended for general use within the computing industry, but appropriate for digital and multimedia forensic analyses. Use of CUE may be necessary for data with proprietary formatting/encoding where no Forensic Equipment has been developed and/or validated or no Native Equipment is available or with the needed functionality. This equipment is generally regarded as reliable by merit of the testing and validation conducted by the developer, as well as by the widespread use in the computing industry and the digital and multimedia forensic community; however, additional internal verification may be required.
- Native Equipment (NE) – Equipment used to acquire, view, process, or analyze data created by a version of that equipment or a compatible engine. Use of NE may be necessary for data with proprietary formatting/encoding for which no Forensic Equipment has been developed and/or validated. This equipment is generally regarded as reliable by merit of the testing and validation conducted by the developer, as well as by the widespread use in the computing industry and the digital and multimedia forensic community.
- Operating System Equipment (OSE) – Any equipment integrated into an operating system or developer/resource package issued by an operating system developer that is intended for routine consumer or commercial use. This equipment is generally regarded as reliable by merit of the testing and validation conducted by the operating system developer, as well as by the widespread use within the computing industry, laboratory and digital and multimedia forensic community.

2.3.3.1 Forensic Equipment shall undergo validation testing prior to first use or concurrent with casework. The validation process will evaluate the equipment against specific requirements in order to determine its overall acceptance and suitability.

- Validation testing is not required for equipment solely designed to decrypt encrypted data and/or identify, remove or bypass security measures.
- Prior to beginning a validation process, consult the Program Manager, Section Supervisor and available guidelines in order to develop an appropriate validation procedure. A validation procedure should consist of the following elements:
  - Purpose and scope (a description of the equipment being tested)
  - Requirements (equipment features being evaluated)
  - Methodology (the hardware/software, settings and test details)
  - Test data sets (used to evaluate requirements)
  - Findings (observations, anomalies, concerns, or limitations)
  - Usage requirements (tool usage conditions required to compensate for any identified limitations)
  - Results (requirements satisfied or not satisfied)
- Validation testing completed by a reputable external entity can be used in lieu of internal testing if the validation procedure is deemed acceptable by the Program Manager and Section Supervisor. Additional internal verification shall be required.
- Subsequently released versions of previously validated equipment shall be approved for use after a review of available release notes by the Section Supervisor or a qualified examiner in the applicable sub-discipline.

2.3.3.2 Common-Use Equipment shall undergo internal verification testing prior to first use or concurrent with casework. The verification process will evaluate specific functionality of the equipment in order to determine its overall acceptance and suitability. The verification requirement will depend on the equipment function being used, the nature of the data being analyzed, or whether any direct results will be reported. The verification need and process will be determined by the Section Supervisor or a qualified examiner in the applicable sub-discipline.

- Verification testing is not required for equipment subject to performance verification, as described in the Performance Verification section 2.4.
- Subsequently released versions of previously verified equipment shall be approved for use after a review of available release notes by the Section Supervisor or a qualified examiner in the applicable sub-discipline.

2.3.3.3 Forensic Equipment and Common-Use Equipment validated or verified and available for use shall be approved by the Section Supervisor or designee and listed in the DME Approved Equipment Log on the DME network.

2.3.3.4 Native Equipment and Operating System Equipment shall not require validation or verification testing, or specific approval for use.

2.4 Performance Verification

Performance verification is a quality assurance measure used to assess the functionality of the laboratory equipment that may affect the accuracy of forensic examination results. Performance verifications shall be documented in the analytical notes or appropriate maintenance log prior to and during use in casework, each time the equipment is powered up and after repair, modification, maintenance or calibration.

2.4.1 Relevant equipment (i.e., hardware) is considered performance verified after a successful Power-On Self-Test (POST) and, if applicable, operating system, software and/or firmware load. Additional performance verification requirements are listed below.

2.4.1.1 Computer Analysis

2.4.1.1.1 Performance verification of write-protecting hardware will consist of confirmation that the hardware's write-protect setting(s) is enabled. Confirmation will be dependent on the method of indication employed by the device.

2.4.1.1.2 Performance verification of write-protecting software will consist of confirmation that the target device indicates a write-protected and/or read-only status.

2.4.1.2 Video Analysis

2.4.1.2.1 Analog performance verifications will consist of a prerecorded color bar, frame counter and audio tone recording utilizing the proper media format per case requirements.

2.4.1.2.2 The acceptable result is a visual display of the color bar, an audible tone and visual display of the frame counter in frames per second to ensure frames are not being dropped.

2.4.2 When equipment used for an examination is uniquely identified in the analytical notes, it indicates that it successfully passed performance verification unless otherwise noted.

2.4.3 In the event that a repair, modification, maintenance, or calibration is performed on equipment, performance verification will be conducted before the system or any of its components are utilized in casework. Documentation of equipment repair, modification, maintenance, or calibration shall be maintained in the section maintenance logs in accordance with the Quality Manual.

3 EXAMINATION & ANALYSIS SETUP

3.1 Examination Documentation

3.1.1 Documentation may be accomplished through handwritten or electronically generated hardcopy analytical notes, photographs and/or photocopies and other pertinent information that can be retained as hard copies or stored electronically in the case file.

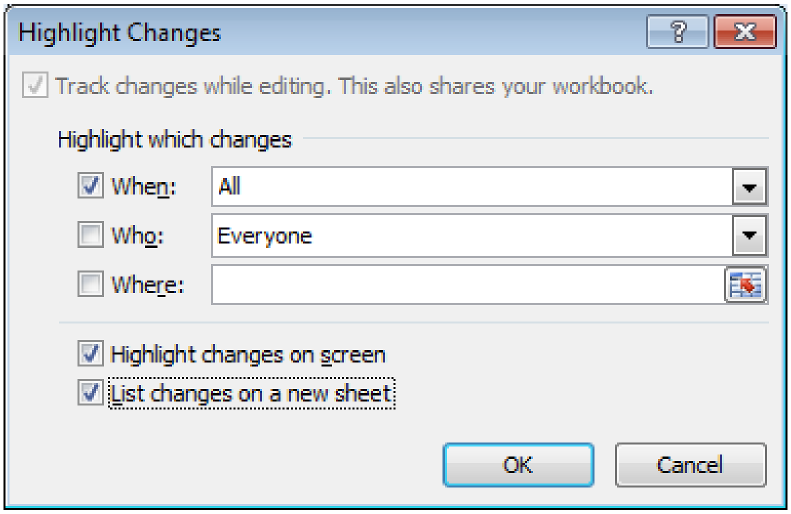
3.1.2 Examination documentation shall contain sufficient detail to allow another qualified examiner to repeat the analysis under conditions as close as possible to the original and interpret the data.

3.1.3 Examination documentation shall include the start date and the end date. The end date reflects the date when the analysis was completed.

3.1.4 Analytical notes originally recorded electronically will be done so using the current, approved and controlled workbook and appendix templates.

3.1.4.1 An examination results verification will be completed by another qualified examiner using the appropriate workbook worksheet; see Examination Results section 3.4.2 for further information.

3.1.4.2 Prior to technical review, tracked changes history will be generated into a new "History" worksheet (Review > Track Changes > Highlight Changes).



Highlight Changes

☑ Track changes while editing. This also shares your workbook.

Highlight which changes

☑ When: All

□ Who: Everyone

□ Where:

☑ Highlight changes on screen

☑ List changes on a new sheet

Highlight Changes Settings

3.1.4.2.1 "Old Value" should be filtered to not display "<blank>" or temporary place-holder values; this will prevent cells that changed from a null to non-null value or from a temporary place-holder value from being displayed.

3.1.4.2.2 Run the "History_Format" macro to apply print formatting to the "History" worksheet.

3.1.4.3 Print the entire workbook to hardcopy and remove any electronic copies from the ECF.

3.1.4.3.1 Follow QM guidelines for any required changes to the printed notes.

3.1.5 A selection of commonly used acronyms and abbreviations are defined within Appendix A of this document.

3.2 Initial Examination & Data Acquisition

3.2.1 Prior to examination, verify that the submitted evidence does not require any additional analyses that would include other disciplines. Review the Request for Laboratory Examination (RFLE) and any supplemental documentation and determine the specifics of the examination request. If possible, contact the requestor in an attempt to confirm the need for analysis and the request or any modification to the request.

3.2.2 A general physical inspection of the submitted evidence shall be conducted and obvious defects documented. If defects are present, the item may require cleaning and/or repair prior to any analysis.

3.2.3 The following steps shall be performed when examining original digital evidence physically or logically:

- Create an electronic case file (ECF) in the appropriate storage location. The ECF is a temporary storage location that contains organized electronic data, documentation and other pertinent information related to the examination.
- Select and document the approved and appropriate equipment utilized in the examination, as defined in the Equipment Validation/Verification and Use section 2.3 of this manual.
- Access digital evidence as read-only or utilizing write-protecting mechanisms to ensure that data cannot be altered.
    - Not all devices can be accessed read-only or utilizing write-protection. If the device is accessed as read-write the reason shall be documented.
    - Read-only and write-protecting mechanisms are not required for mobile devices.
- Generate and document a pre-examination hash value for the original digital evidence. If it is not possible to generate a hash value (e.g., flash memory) the reason shall be documented.
    - A pre-examination hash is not required for a mobile device.
- Acquire a derivative copy of the original digital evidence, document the acquisition method and organize the derivative copy using a naming convention that reflects the original evidence's laboratory designation.
    - If a clone of the original digital evidence is generated, the storage capacity of the destination storage location must be greater than or equal to the total capacity or size of the original digital evidence.
    - If a bit-stream image or other container-type file is generated, the storage capacity of the destination storage location may vary depending on the type of file being generated (e.g., RAW, Expert Witness / EnCase, Zip) and if compression is utilized.
- Generate and document a hash value for the acquired derivative evidence.
- Generate and document a post-examination hash value for the original digital evidence. If it is not possible to generate a hash value (e.g., flash memory) the reason shall be documented.
    - When the original digital evidence is stored on a read-only device or is accessed using write-protecting methods, it is not required to generate a post-examination hash value.
    - A post-examination hash is not required for a mobile device.
- Compare the pre-examination, post-examination and derivative evidence hash values and document the result of the verification.

3.2.3.1 Conducting an analysis on the original submitted digital evidence should be avoided whenever possible. If the device can be appropriately write-protected, but an acceptable derivative copy of the submitted digital evidence cannot be acquired or analyzed, it is permissible to analyze the original submitted device. Justification for directly analyzing the original submitted digital evidence, excluding mobile devices, shall be documented.

3.3 Evidence Sources

3.3.1 Derivative evidence acquired during examination shall be provided to the requestor, unless it is directly duplicative (e.g., clone) of the original evidence, the size of the derivative evidence precludes it or with supervisor approval to exclude it. When possible, provided derivative evidence should be compressed, encrypted and password–protected. The integrity of provided derivative evidence shall be verified by conducting and documenting a hash value comparison between the derivative evidence stored in the ECF and that provided.

3.3.2 Document in the analytical notes, on the original RFLE and in the Certificate of Analysis (CoA) how the derivative evidence is being labeled and what container it is being returned in or attached to.

3.3.2.1 It is acceptable to have one storage device containing evidence sources from numerous evidence items as long as it is clearly documented. If multiple storage devices are necessary, the contents of each shall be clearly documented.

3.3.2.2 Storage devices shall be assigned an item number and entered in to the laboratory information management system (LIMS) as an evidence item.

3.3.3 If the evidence sources media is not returned in the original evidence container, seal the evidence sources media in an appropriate container and attach it to the original evidence container.

3.4 Examination Results

3.4.1 Review the examination request to ensure that the reported results address the examination request. Results may be presented in a format deemed appropriate by the examiner or the requestor. Any requested results not provided and any results exceeding the examination request shall be documented in the analytical notes and in the CoA.

3.4.2 Prior to completing the case, examination results shall be verified by another qualified examiner and the verification documented in the analytical notes. Recommended changes made by the verifier shall be documented in the examination documentation. When required, verified results may be provided to approved parties, per the QM, prior to the completion of an examination or issuance of a CoA.

3.4.3 The results data set shall have a single hash value generated and documented for its total content prior to release to ensure its integrity can be tracked. Unless the size of the results data set precludes it, provided results should be compressed, encrypted and password-protected. The integrity of provided results shall be verified by conducting and documenting a hash value comparison between the results stored in the ECF and those provided.

3.4.4 Document in the analytical notes, on the original RFLE and in the CoA how the results are being labeled and the method of return.

3.4.4.1 It is acceptable to have one storage device containing results from numerous evidence items as long as it is clearly documented. If multiple storage devices are necessary, the contents of each shall be clearly described in the analytical notes.

3.4.4.2 Results can be returned electronically, if encrypted and password–protected and the transfer method documented.

3.4.5 If the results media is not returned in the original evidence container, seal the results media in an appropriate container and attach it to the original evidence container, or document any alternative methods of return.

3.5 Electronic Case File Retention

3.5.1 The ECF shall be stored in a manner suitable for long-term availability and retrieval.

3.5.2 An ECF can include but is not limited to: electronic data, documentation and other pertinent information related to the examination, deemed necessary by the examiner. Generally, information that cannot be easily recreated should be retained in the ECF.

3.5.2.1 A copy of the analytical notes shall not be retained in the ECF.

3.5.2.2 The ECF shall have a single hash value generated and documented for its total content, to ensure its integrity can be tracked. Unless the size of the ECF precludes it, it should be compressed into an archive file format. The integrity of the archive file shall be verified by conducting and documenting a hash value comparison between the original ECF and the archive file.

3.5.3 The ECF shall be placed onto an external storage device, with an appropriate storage capacity, at the completion of the case. The storage device will be sealed in an appropriate container, labeled with the date sealed and initials of the examiner, and stored with the case file. Subsequent access will require the container to be resealed and additionally labeled with the date sealed and initials of the examiner.

3.5.4 Prior to reviewing data from a retrieved ECF, its integrity shall be verified by generating a compatible hash value and comparing it to its documented value. If a discrepancy exists notify the Section Supervisor.

3.6 System and Network Security

In order to prevent unauthorized access to section computer systems (if applicable) and networks:

- Computer systems will employ section-confidential password protection.
- Computer systems will maintain active and current security software.
- Network traffic between the section network and the Internet will be controlled by a firewall.

3.7 Accessing Restricted Internet Resources

At times, it is necessary for section personnel to access, print, download or store Internet resources required for use in conducting research and casework that may be considered to be in violation of the Commonwealth of Virginia Policies and/or statutes. Internet resources that are accessed will be documented.

3.8 Short Term Storage

Short term storage is used when evidence is in the process of examination or is waiting for instrument support results. Generally, evidence will not remain in short term storage for longer than ninety (90) days. After this time period, evidence must be placed into long term storage and properly sealed according the Quality Manual.

4 COMPUTER & MOBILE DEVICE ANALYSIS

4.1 Purpose

Forensic computer analysis includes the identification and recovery of electronically stored information originating from a variety of digital storage devices and mobile devices. Due to the vast number and types of legacy, current and emerging devices, there are inherent qualities that prohibit the establishment of a rigid set of procedures to cover each and every case; therefore, it is acceptable for the examiner to select the appropriate course of action.

4.2 Scope

This procedure applies to the acquisition and analysis of electronically stored information originating from computer systems, mobile devices, and digital storage devices. Due to the varying types of digital evidence, there will be cases that require examinations that involve other Digital & Multimedia Evidence sub-disciplines.

4.3 Equipment

- Computer systems and peripherals
- Digital storage devices
- Mobile devices
- Cameras
- Cables and adapters
- Forensic Equipment, Native Applications, Common Use Applications, and Operating System Tools

4.4 Limitations – Computers & Mobile Devices

Whenever possible, evidence submitted to the DME Section that has the ability to receive or transmit data will be radio frequency shielded, in order to prevent the communication of data, until such time the analysis has been completed.

Currently there is no available method that will acquire or parse all electronically stored information from all mobile devices. Manual preservation (photography, video recording and/or transcription) may be necessary to document the information observed on the mobile device's display.

Equipment may not identify or recover all electronically stored information on all devices. This limitation can be identified through a manual review of identified and recovered data.

4.5 Safety

Sharp points and edges associated with submitted evidence should be avoided.

Electrical shocks can occur if the computer is open or devices or components are dismantled.

Electronic devices may short-circuit causing malfunction, failure and/or disintegration, resulting in smoke or fire hazard.

4.6 Procedures – Computers

4.6.1 Examination documentation shall be handled following the guidelines as described in the Examination Documentation section 3.1 of this manual.

4.6.2 Conduct a physical examination of the computer and document identifying information (i.e., manufacturer, model number, unique identifier**, etc.**), unusual markings and defects.

4.6.3 Document the presence of any digital storage devices (e.g., hard disk drives, solid-state drives) and document identifying information (i.e., manufacturer, model number, unique identifier**, etc.**), unusual markings and defects.

4.6.4 If defects are present, the item may require cleaning and/or repair prior to any analysis.

4.6.5 If available and necessary, obtain any applicable manuals or documentation for the device(s).

4.6.6 If available, document the computer's system date and time and time zone settings, the current local date and time and time zone, boot sequence, security settings, and method used to access such information.

4.6.6.1 Ensure power and data connections are disconnected from any digital storage device prior to access.

4.6.7 The acquisition and verification of digital evidence shall be handled following the guidelines described in the Initial Examination & Data Acquisition section 3.2 of this manual.

4.6.8 Select and document the approved and appropriate equipment utilized in the analysis of the digital evidence, as defined in the Equipment Validation/Verification and Use section 2.3 of this manual.

4.6.8.1 Analyze the digital evidence to identify and recover data that addresses the examination request. Document the details of the analysis.

4.6.9 Evidence sources shall be handled following the guidelines as described in the Evidence Sources section 3.3 of this manual.

4.6.10 Examination results shall be handled following the guidelines as described in the Examination Results section 3.4 of this manual.

4.6.11 The retention of the ECF shall be handled following the guidelines as described in the Electronic Case File Retention section 3.5 of this manual.

4.7 Procedures – Mobile Devices

4.7.1 Examination documentation shall be handled following the guidelines as described in the Examination Documentation section 3.1 of this manual.

4.7.2 Document the shielding method(s) employed.

4.7.3 Conduct a physical examination of the device (handset) and document identifying information (i.e., manufacturer, model number, unique identifier**, etc.**), unusual markings and defects.

4.7.4 Document the presence of any removable digital storage devices (e.g., integrated circuit cards, flash memory) and document identifying information (i.e., manufacturer, model number, unique identifier, etc.), unusual markings and defects.

4.7.5 If defects are present, the item may require cleaning and/or repair prior to any analysis.

4.7.6 If available and necessary, obtain any applicable manuals or documentation for the device.

4.7.7 Charge the device's battery, if necessary.

4.7.8 Document the device's (handset) operating system, system date and time and time zone settings, the current local date and time and time zone, and any relevant configuration settings, if applicable.

4.7.9 The acquisition and verification of digital evidence shall be handled following the guidelines described in the Initial Examination & Data Acquisition section 3.2 of this manual.

4.7.10 Select and document the approved and appropriate equipment utilized in the acquisition of the mobile device, as defined in the Equipment Validation/Verification and Use section 2.3 of this manual.

4.7.10.1 It may be necessary to utilize several different equipment items and acquisition methods in order to extract as much data as possible.

4.7.10.2 For devices requiring a Subscriber Identity Module (SIM) card, the SIM may be acquired while removed from and installed in the device.

4.7.10.2.1 If the device is powered off, remove the SIM, acquire its data and, if required, create a clone.

4.7.10.2.1.1 Powering on a device without the active SIM may result in the loss of data.

4.7.10.2.2 If the device is powered on, acquire the data with the SIM in the device.

4.7.10.2.2.1 This may alter certain metadata present on the SIM.

4.7.10.2.3 Verify that the extracted data is consistent between the two methods of acquisition and document any issues or discrepancies.

4.7.10.3 Devices containing removable storage devices (e.g., flash memory card), when possible, should be processed separate from the device.

4.7.11 Select and document the approved and appropriate equipment utilized in the analysis of the mobile device, as defined in the Equipment Validation/Verification and Use section 2.3 of this manual.

4.7.11.1 Analyze the digital evidence to identify and recover data that addresses the examination request. Document the details of the analysis.

4.7.11.2 The examiner shall ensure that the identified and recovered data is an accurate depiction of what is on the submitted mobile device. If the volume of data precludes this, a smaller sampled dataset shall be used. Document any discrepancies.

4.7.12 Evidence sources shall be handled following the guidelines as described in the Evidence Sources section 3.3 of this manual.

4.7.13 Examination results shall be handled following the guidelines as described in the Examination Results section 3.4 of this manual.

4.7.14 The archival of the ECF shall be handled following the guidelines as described in the Archiving section 3.5 of this manual.

4.8 References

Owner's Manuals, User's Manuals and all appropriate hardware and software manuals should be referenced for equipment operating instructions.

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

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

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.

National Institute of Standards and Technology (NIST). *Guidelines on Mobile Device Forensics*. Revision 1. 2014.

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

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.

5 VIDEO ANALYSIS

5.1 Purpose

Video analysis includes the application of various techniques in order to clarify details and provide data that is not readily apparent within an original video recording. There are inherent qualities that prohibit the establishment of a rigid set of procedures to cover each and every case; therefore, it is acceptable for the examiner to select the appropriate course of action.

5.2 Scope

This procedure applies to analog and digital video recordings in which clarification is requested. Also included within the scope of this procedure is image analysis. Image analysis can involve the examination and clarification of images recorded in a variety of formats and media types, and is intended to improve the visual appearance or features in an image.

5.3 Equipment

- Computer systems and peripherals
- Consumer and professional grade and security time lapse analog and digital video players/recorders
- Multiplexers
- Time base correctors
- Analog and digital storage devices
- Cameras
- Mobile devices
- Professional headphones
- Professional monitors
- Printers
- Cables and adapters
- Forensic Equipment, Native Applications, Common Use Applications, and Operating System Tools

5.4 Limitations

It is not always possible to improve the clarity of the video images, especially in instances of:

- Extremely low resolution
- Limited focal length
- Compression
- Media wear
- Technical limitations and proprietary files of the recording devices/systems used to make the original recording
- The physical environment where the original recording was produced

Some digital cameras may preserve data only so long as power is provided; therefore, care should be taken to examine these devices as soon after submission as possible to reduce the potential for data loss.

5.5 Safety

Sharp points and edges associated with submitted evidence should be avoided.

Electronic devices may short-circuit causing malfunction, failure and/or disintegration, resulting in smoke or fire hazard.

5.6 Procedures

5.6.1 Examination documentation shall be handled following the guidelines as described in the Examination Documentation section 3.1 of this manual.

5.6.2 Document the physical condition of the evidence to include, but not limited to: physical damage to media or housing, contaminants (e.g., dirt, grease), media characteristics (e.g., manufacture, size, format) labels or identifiers.

5.6.3 If defects are present, the item may require cleaning and/or repair prior to any analysis.

5.6.4 If available and necessary, obtain any applicable manuals or documentation for the device.

5.6.5 Select and document the approved and appropriate equipment utilized in the acquisition of the video recording or image, as defined in the Equipment Validation/Verification and Use section 2.3 of this manual.

5.6.5.1 Determine and document the model and settings (recording format and speed) used to produce the original video recording, if possible.

5.6.5.2 Document the playback device utilized to provide the optimal video recording.

5.6.5.2.1 Analog Recordings

5.6.5.2.1.1 The write-protect mechanism shall be activated (e.g., removed, moved) in order to prevent the operation of the recording function. Any items removed will be retained and returned with the evidence.

5.6.5.2.1.2 When playback of the evidentiary recording is less than optimal, signal dropouts occur and/or player idiosyncrasies are suspected as a potential factor, multiple players and/or recorders should be utilized to preview the recording. In some cases this may necessitate retrieving the original recorder.

5.6.5.2.1.3 Document any adjustments done to optimize playback (e.g., reverse playback).

5.6.5.2.1.4 When possible, any action or equipment that may cause damage to the original recording should be avoided. Such actions may include, but are not limited to: maintaining the recording in the "pause" mode for extended periods, unnecessary repeated playback or placing the media in the proximity to strong magnetic fields.

5.6.5.2.2 Digital Recordings

5.6.5.2.2.1 If applicable, identify and document the proprietary file format of the recording and any required proprietary player.

5.6.5.2.2.2 The acquisition and verification of digital evidence shall be handled following the guidelines described in the Initial Examination & Data Acquisition section 3.2 of this manual.

5.6.5.3 Determine and document the recording device model and settings used to produce the original image, if possible. If available and necessary, obtain any applicable manuals or documentation for the device.

5.6.5.3.1 Print Images

5.6.5.3.1.1 This may require digitization of negative(s), prints or conversion from other media.

5.6.5.3.1.2 Document any adjustments done during digitization.

5.6.5.3.2 Digital Images

5.6.5.3.2.1 If applicable, identify and document the proprietary file format of the image and obtain and document any required proprietary viewer.

5.6.5.3.2.2 The acquisition and verification of digital evidence shall be handled following the guidelines described in the Initial Examination & Data Acquisition section 3.2 of this manual.

5.6.6 Select and document the approved and appropriate equipment utilized in the analysis of the video recording or image, as defined in the Equipment Validation/Verification and Use section 2.3 of this manual.

5.6.6.1 Analyze the video recording/image to determine the level of clarification required to address the examination request. Document the details of the analysis.

5.6.6.2 Review the recording/image and document the steps applied to locate, capture and clarify the AoI.

5.6.6.2.1 The AoI will be documented, if possible, by using the date/time stamp on the recording, the player counter information or other identifying information.

5.6.6.2.2 Capture the AoI in its original condition (raw) and save in an uncompressed or lossless file format.

5.6.6.2.3 Steps or techniques applied to the recording to clarify the AoI shall be documented in the order in which they were applied to ensure the reproducibility of the results.

5.6.6.2.3.1 If adjustments for aspect ratio are required for printing, in most cases they should be done after all image processing and clarifications are conducted. Prior to output, ensure the pixel aspect ratio is correct for the chosen media.

5.6.6.3 Clarified video recordings/images shall be saved in an uncompressed or lossless file format, in the electronic case file.

5.6.7 Evidence sources shall be handled following the guidelines as described in the Evidence Sources section 3.3 of this manual.

5.6.8 Examination results shall be handled following the guidelines as described in the Examination Results section 3.4 of this manual.

5.6.9 The retention of the ECF shall be handled following the guidelines as described in the Electronic Case File Retention section 3.5 of this manual.

5.7 References

Owner's Manuals, User's Manuals and appropriate software manuals should be referenced for equipment operating procedures.

Combating Terrorism Technical Surpport Office (CTTSO). *Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems.* Version 1.0. 2006.

Damjanovski, Vlado. *CCTV Networking and Digital Technology*. Second Edition. Amsterdam: Elsevier/Butterworth Heinemann, 2005.

Law Enforcement & Emergency Services Video Association (LEVA) Inernational, Inc. *Best Practices for the Acquisition of Digital Multimedia Evidence*. Version 3.0. 2010.

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

Scientific Working Group on Imaging Technology (SWGIT). *https://www.swgit.org*.

6 REPORTING GUIDLINES

6.1 Introduction

Reports should seek to address case-specific examination requests and provide the reader with all the relevant information in a clear and concise manner.

The following report formats shall be used to the extent possible when reporting results to ensure consistency within the section. It is recognized that report statements cannot be provided to address all situations; therefore, the following statements should be considered as example wording. When drafting report wording for evidence types not listed or when specific examples do not appear for a particular type of evidence, look first to existing wording that may be applied to the current situation. If a situation is so unusual that appropriate report wording is not available in the manual, it is expected that the examiner will consult with the Section Supervisor for wording that may have been previously applied to the situation, the Physical Evidence Program Manager and/or the Director of Technical Services.

The CoA shall include in the report statement the types of examinations that were conducted to reach the stated conclusions.

6.2 Examination Results

Information about examination results media that is being provided.

6.2.1 Examination results have been written to a(n) INSERT STORAGE MEDIA, which is being returned within a(n) INSERT PACKAGE DESCRIPTION attached to Container [#]. The results (INSERT NAME OF FILE) are encrypted and password protected; the password to extract the results is: "**INSERT PASSWORD HERE**".

OR

No examination results are being returned.

AND

The evidence item submitted as Item(s) [#] was renamed to Item(s) [#] due to a conflict with other submitted evidence items. [Insert as required]

6.3 Summary of Examination

Information about the types of examinations that were conducted and examination results that are being provided.

6.3.1 Computer Analysis

Computer analysis procedures were utilized to analyze Item(s) #.

AND

I. The requested information listed below has been produced from Item(s) #:

   A. INSERT CATEGORY [Add additional as required]

      1. INSERT NAME/LOCATION OF INFORMATION WITHIN EXAMINATION RESULTS

         a. INSERT DESCRIPTION

The dates and times associated with the produced data are dependent upon the date and time settings of the device and may not necessarily reflect the actual date and time of the recorded event. Dates and times reported in Coordinated Universal Time (UTC) may need to be adjusted by the appropriate time zone offset (e.g., Eastern Standard Time [EST] = -0500, Eastern Daylight Time [EDT] = -0400) in order to reflect the local time of the recorded event.

Due to the nature of electronically stored information, all data related to the request may not have been identified and provided. Additional data may be present on Item(s) [#]; however only those items related to the request are provided.

OR

No requested information was identified on Item(s) #.

OR

Access could not be gained to Item(s) # due to [INSERT REASON] OR [the presence of INSERT SECURITY MEASURE which could not be bypassed. Should the INSERT SECURITY MEASURE be circumvented in the future, Item(s) # can be resubmitted for analysis].

OR

Item(s) # was used to access Item(s) #.

OR

No analysis was performed on Item(s) #.

6.3.2 Mobile Device Analysis

Mobile device analysis procedures were utilized to analyze Item(s) #.

AND

I. The requested information listed below has been produced from Item(s) #:

  A. INSERT CATEGORY [Add additional as required]

    1. INSERT NAME/LOCATION OF INFORMATION WITHIN EXAMINATION RESULTS

      a. INSERT DESCRIPTION

The dates and times associated with the produced data are dependent upon the date and time settings of the device and/or the cellular network and may not necessarily reflect the actual date and time of the recorded event. Dates and times reported in Coordinated Universal Time (UTC) may need to be adjusted by the appropriate time zone offset (e.g., Eastern Standard Time [EST] = -0500, Eastern Daylight Time [EDT] = -0400) in order to reflect the local time of the recorded event.

Due to the nature of electronically stored information, all data related to the request may not have been identified and provided. Additional data may be present on Item(s) #; however only those items related to the request are provided.

Due to the method of data acquisition, only existing data [and limited, previously-existing data] on Item(s) # was accessible. [Additional] P[p]reviously-existing data related to the request may be present on Item(s) #; but will require an alternative method of data acquisition that can result in device destruction or data loss.

[A/No] security measure(s) [was/were] present on Item [#] [that was bypassed AND/OR documented AND/OR removed].

Network isolation of Item(s) # is recommended should future analysis be required. The device is being returned with "Airplane mode" enabled (device radios that transmit data are turned off).

OR

No requested information was identified on Item(s) #.

OR

Access could not be gained to Item(s) # due to [INSERT REASON] OR [the presence of INSERT SECURITY MEASURE which could not be bypassed. Should the INSERT SECURITY MEASURE be circumvented in the future, Item(s) # can be resubmitted for analysis].

OR

Item(s) # was used to access Item(s) #.

OR

No analysis was performed on Item(s) #.

6.3.3 Video Analysis

Video analysis procedures were utilized to analyze Item(s) #.

AND

The analysis of Item [#] rendered an improvement in the visual appearance of the area of interest.

OR

The analysis of Item [#] rendered a limited improvement in the visual appearance of the area of interest due to the [focal length, resolution and compression in use] OR [existing lighting conditions] OR [format utilized] at the time the original recording was produced.

AND

I. The requested information listed below has been produced from Item(s) #:

    A. INSERT CATEGORY [Add additional as required]

        1. INSERT NAME/LOCATION OF INFORMATION WITHIN EXAMINATION RESULTS

            a. INSERT DESCRIPTION

AND

The dates and times associated with the produced data are dependent upon the date and time settings of the device and/or the data network and may not necessarily reflect the actual date and time of the recorded event.

OR

The analysis of Item [#] did not result in improvement of the area of interest due to excessive media wear; therefore, no results were produced.

After an extensive review of Item [#], it was determined that the image quality was insufficient for clarification due to the [focal length, resolution and compression in use] OR [existing lighting conditions] OR [format utilized] at the time the original recording was produced; therefore, no results were produced.

OR

After an extensive review of Item [#], the area of interest could not be located; therefore, no results were produced.

OR

Access could not be gained to Item [#] due to its proprietary format; therefore, no results were produced. Should the proprietary player be located in the future, the item can be resubmitted for analysis.

OR

Access could not be gained to Item(s) # due to [INSERT REASON] OR [the presence of INSERT SECURITY MEASURE which could not be bypassed. Should the INSERT SECURITY MEASURE be circumvented in the future, Item(s) # can be resubmitted for analysis].

OR

No analysis was performed on Item(s) #.

OR

Item(s) # was used to access Item(s) #.

6.4 Evidence Sources

Information about derivative evidence media that is being provided.

6.4.1 Data acquisition procedures were utilized to acquire physical and logical data from Item(s) #; this acquired data was used as the primary, derivative evidence source for further analyses. These derivative evidence sources should be maintained and resubmitted if future analysis is required.

Derivative evidence sources have been written to Item DME [#], a(n) INSERT STORAGE MEDIA, which is being returned within a(n) INSERT PACKAGE DESCRIPTION with Container [#]. The evidence sources (INSERT NAME OF FILE) are encrypted and password protected; the password to extract the evidence sources is: "**INSERT PASSWORD HERE**".
OR

No evidence sources are being returned.

6.5 Disposition of Evidence

Document in the CoA according to the Quality Manual.

6.6 Requests for Additional Submissions

If additional items or information are required to complete an analysis, the request shall be documented in the CoA. Requested information may relate to the area of interest, date and time and/or description of the area to be clarified. Requested items may include additional formats, proprietary viewers, additional images or recordings, or passwords.

Appendix A – Acronyms and Abbreviations

00:00:00.000 – hours; minutes; seconds; hundredths of seconds; (audio)

00:00:00.000 – hours; minutes; seconds; portions of frame; (video)

ADB – Android Debug Bridge

Admin – Administration

AoI – Area of Interest

AVI/.avi – Audio Video Interleaved / Multimedia Container Format

API – Application Programming Interface

BD – Blu–ray Disc

BD-DL – Dual-layer Blu-ray Disc

BD-QL – Quad-layer Blu-ray Disc

CD – Compact Disc

CDMA – Code Division Multiple Access

CD-R – Recordable Compact Disc

CD-RW – Re–recordable Compact Disc

CoA – Certificate of Analysis

Config – Configuration

Cont – Continued

CUE – Common–Use Equipment

CW – Clockwise

DAT – Digital Audio Tape

DB/db - Database

dB – Decibel

dBv – Decibel (voltage reference)

DFU – Device Firmware Update

DST – Daylight Savings Time

DVD – Digital Versatile Disc

DVD-DL – Dual-layer Digital Versatile Disc

DVR – Digital Video Recorder

ECF – Electronic Case File

EDT – Eastern Daylight Time

EP – Extended Play mode

ESN – Electronic Serial Number

EST – Eastern Standard Time

ET – Eastern Time

EXT Data – Extended Data

FE – Forensic Equipment

Fps – Frames per second

Freq – Frequency

FSE – File System Extraction

GSM – Global Systems for Mobile Communications

HD – High Density

HDD – Hard Disk Drive

Hi–8 – Hi–8mm video cassette

Hz – hertz

ICCID – Integrated Circuit Card Identifier

IDE – Integrated Drive Electronics

iDEN – Integrated Digitally Enhanced Network

IMEI – International Mobile Equipment Identity

IMG – Image

IMSI – International Mobile Subscriber Identity

JPEG/.jpeg – Joint Photographic Experts Group / Picture File Format

kHz – Kilohertz

Ki – 128 Bit Encryption Key

L – Left

LAI – Location Area Identity

LE – Logical Extraction

LIMS – Laboratory Information Management System

LP – Long Play mode

MDN – Mobile Directory Number

MEID – Mobile Equipment Identifier

MDV – Mini Digital Video

MIN – Mobile Identification Number

Min(s) – Minute(s)

MMS – Multimedia Messaging Service

Mono – Monophonic

MSISDN – Mobile Subscriber Integrated Services Digital Network Number

NE – Native Equipment

NTSC – National Television Standards Committee

OSD – On-System Display

OSE – Operating System Equipment

PATA – Parallel AT Attachment

PE – Physical Extraction

PIN – Personal Identification Number

POST – Power–On Self–Test

PUK – Personal Unlock Key

PV – Performance Verification

QA – Quality Assurance

Quad – Four images to a frame

R – Right

RAM – Random Access Memory

RFLE – Request for Laboratory Examination

ROM – Read–Only Memory

Rtn – Return

SAS – Serial Attached SCSI

SATA – Serial AT Attachment

SBB – Sealed Brown Box

SBPB – Sealed Brown Paper Bag

SBX – Sealed Box

SCSI – Small Computer System Interface

SD – Secure Digital

SDN – Service Dialed Number

Sec(s) – Second(s)

SEN – Sealed Envelope

SIM – Subscriber Identity Module

SLP – Standard Long Play mode

SMS – Short Message Service

SMSC – Short Message Service Center

S/N – Serial Number

SP – Standard Play mode

SPLB – Sealed Plastic Bag

Stereo – Stereophonic

S–VHS – Super Video Home System

SPB – Sealed Paper Bag

SWB – Sealed White Box

SWEN – Sealed White Envelope

SWPB – Sealed White Paper Bag

SYEN – Sealed Yellow Envelope

TBC – Time–Base Corrector

TDMA – Time Division Multiple Access

Telcon – Telephone Conference

TIFF/.tiff – Tagged Image File Format / Graphics File Format

TMSI – Temporary Mobile Subscriber Identity

UICC – Universal Integrated Circuit Card

USB – Universal Serial Bus

USIM – Universal Subscriber Identity Module

UTC – Coordinated Universal Time

VCR – Video Cassette Recorder

VHS –Video Home System

WAV/.wav – Waveform Audio File Format / Audio File Format