Department of Forensic Science

COPYRIGHT © 2022

DIGITAL & MULTIMEDIA EVIDENCE SECTION PROCEDURES MANUAL

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

TABLE OF CONTENTS

1 Introduction

2 Equipment Maintenance, Usage & Quality Assurance

- **2.1 Introduction**
- **2.2 Equipment**
- **2.3 Equipment Validation, Verification and Use**
- **2.4 Performance Verification**
- **2.5 System and Network Security**
- **2.6 Accessing Restricted Internet Resources**

3 Examination Documentation & Media

- **3.1 Examination Documentation**
- **3.2 Evidence Sources**
- **3.3 Examination Results**
- **3.4 Electronic Case File**

4 Initial Examination & Data Acquisition

- **4.1 Initial Examination**
- **4.2 Data Acquisition**
- **4.3 Short Term Storage**

5 Computer & Mobile Device Analysis

- **5.1 Purpose**
- **5.2 Scope**
- **5.3 Equipment**
- **5.4 Limitations – Computer & Mobile Devices**
- **5.5 Safety**
- **5.6 Procedures – Computer Devices and Associated Digital Storage Devices**
- **5.7 Procedures – Mobile Devices and Associated Digital Storage Devices**
- **5.8 Procedures – National Center for Missing & Exploited Children (NCMEC) Child Recognition and Identification System (CRIS)**
- **5.9 Procedures – Data Authentication**
- **5.10 References**

6 Video & Image Analysis

- **6.1 Purpose**
- **6.2 Scope**
- **6.3 Equipment**
- **6.4 Limitations**
- **6.5 Safety**
- **6.6 Procedures – Video & Image Analysis**
- **6.7 Procedures – Data Authentication**
- **6.8 References**

7 Reporting Guidelines

- **7.1 Introduction**
- **7.2 Evidence Items**
- **7.3 Examination Results**
- **7.4 Summary of Examination**
- **7.5 Evidence Sources**

COPYRIGHT © 2022
VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

7.6 Methods
7.7 Disposition of Evidence
7.8 Requests for Additional Submissions

Appendix A Acronyms and Abbreviations

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

1 INTRODUCTION

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

- Computer & Mobile Device Analysis is the scientific examination of electronically stored information contained on a wide variety of devices. These devices include, but are not limited to computer devices, such as servers, desktops, digital video recorders (DVR), laptops, game systems, and the Internet of Things (IoT); mobile devices, such as cellular telephones and tablets; and digital storage devices, such as hard disk drives, flash memory and optical discs.
- Video & Image Analysis is the scientific examination of analog or digital multimedia and video recordings, or print or digital images in order to clarify details and/or intelligibility, and provide data that is not readily apparent within an original multimedia or video recording or image. These recordings and images can originate from a variety of sources including, but not limited to mobile devices, video and digital cameras, surveillance systems, or video recordings.

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

2 EQUIPMENT MAINTENANCE, USAGE & QUALITY ASSURANCE

2.1 Introduction

2.1.1 The reliability and performance of the equipment used in the examination of digital evidence is monitored 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 Maintenance shall consist of upgrades or replacements of hardware components, and major updates to Operating Systems (OS).

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

COPYRIGHT © 2022

2.2.2.2 All maintenance shall be documented and retained in the appropriate log located in the section.

2.3 Equipment Validation, Verification and Use

2.3.1 The equipment the DME section utilizes in casework are considered its "methods", and are either standard, commercial off-the-shelf (COTS) and non-COTS, or laboratory-developed.

VANCOUVER DEPARTMENT OF FORENSIC SCIENCE

2.3.1.1 Standard, COTS equipment used within its designed application range can be considered to be sufficiently validated, however, may be subject to performance verification, as described in the Performance Verification section of this manual.

2.3.1.2 Standard, non-COTS equipment used within its designed application range is subject to performance verification, as described in the Performance Verification section of this manual.

2.3.1.3 Laboratory-developed, and standard equipment used outside its intended scope, shall undergo formal validation testing prior to being approved and placed into service for section-wide use. The validation process will evaluate the equipment against specific requirements in order to determine its acceptance and suitability. The validation need and requirements will depend on the equipment function(s) used, the nature of the data analyzed, and whether any direct results will be reported.

- Validation testing is not required for equipment designed to decrypt encrypted data and/or identify, remove or bypass security measures.

2.3.1.3.1 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)

2.3.1.3.2 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

UNCONTROLLED COPY

Manager and Section Supervisor. Additional performance verification shall be required.

2.3.2 DME examiners should use the latest version of equipment unless it is not appropriate or possible to do so, or follow procedures for deviation documented in the Quality Manual.

2.3.3 DME examiners are able to use Operating System Equipment (OSE), Native Equipment (NE), Common-Use Equipment (CUE), and Forensic Equipment (FE), and to perform the processes described in this document.

- 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.
- Native Equipment (NE) – Equipment used to acquire, view, process, parse, or analyze data created by a version of that equipment or a compatible engine, or a documented data structure (e.g., file specification). 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.
- Common-Use Equipment (CUE) – Equipment used to acquire, view, process, parse, 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 FE or NE 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, performance verification may be required.
- 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, validation and/or performance verification may be required.

2.3.3.1 FE and CUE validated and/or subject to performance verification, as described in the Performance Verification section of this manual, and placed into service for section-wide use shall be approved by the Section Supervisor or a qualified examiner in the applicable sub-discipline and documented in the appropriate log.

2.3.3.1.1 Subsequently released versions of previously validated and/or verified equipment shall be approved for section-wide use after the Section Supervisor or a qualified examiner in the applicable sub-discipline reviews the available release notes and either determines that additional validation or verification is not required, or completes the additional validation or verification.

2.3.3.2 NE and OSE 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.

2.4.1 The verification process will evaluate the equipment against specific requirements in order to determine its acceptance and suitability. The verification need and requirements will depend on the equipment function used, the nature of the data analyzed, and whether any direct results will be reported.

2.4.2 Relevant hardware is considered performance verified after a successful Power-On Self-Test (POST) and, if applicable, operating system, software and/or firmware load.

Relevant software is considered performance verified after a review of the available product documentation (e.g. specifications) confirms that the software can acquire, view, process, parse, and/or

COPYRIGHT © 2022 VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

analyze data in a way that is applicable to a given task(s), as well as confirmation that the software successfully performs the task(s) on a target dataset. The verification process shall ensure that the acquired, viewed, processed, parsed, or analyzed data is an accurate depiction of the source data. If the volume of data precludes this, a smaller, sampled dataset shall be used.

- Performance verification is not required for equipment designed to decrypt encrypted data and/or identify, remove or bypass security measures.

Additional performance verification requirements are listed below.

2.4.2.1 Computer Analysis

2.4.2.1.1 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.

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

COPYRIGHT © 2022

2.4.2.2 Mobile Device Analysis

2.4.2.2.1 Performance verification of radio frequency shielded enclosures will consist of the annual testing and documentation of which cellular, Wi-Fi, and Bluetooth frequencies are successfully or unsuccessfully shielded.

VIRGINIA

2.4.2.3 Video Analysis

DEPARTMENT

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

OF

2.4.2.3.1.1 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.

FORENSIC SCIENCE

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

2.4.4 Equipment verified and placed into service for section-wide use shall be approved by the Section Supervisor or a qualified examiner in the applicable sub-discipline, and documented in the appropriate log.

2.4.4.1 Subsequently released versions of previously verified equipment shall be approved for section-wide use after the Section Supervisor or a qualified examiner in the applicable sub-discipline reviews the available release notes and either determines that additional verification is not required, or completes the additional validation or verification.

2.4.5 Performance verification of existing equipment returned to service after repair, modification, maintenance or calibration shall be documented in the appropriate log in accordance with the Quality Manual (QM).

2.5 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.

2.6 Accessing Restricted Internet Resources

UNCONTROLLED COPY

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.

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

3 EXAMINATION DOCUMENTATION & MEDIA

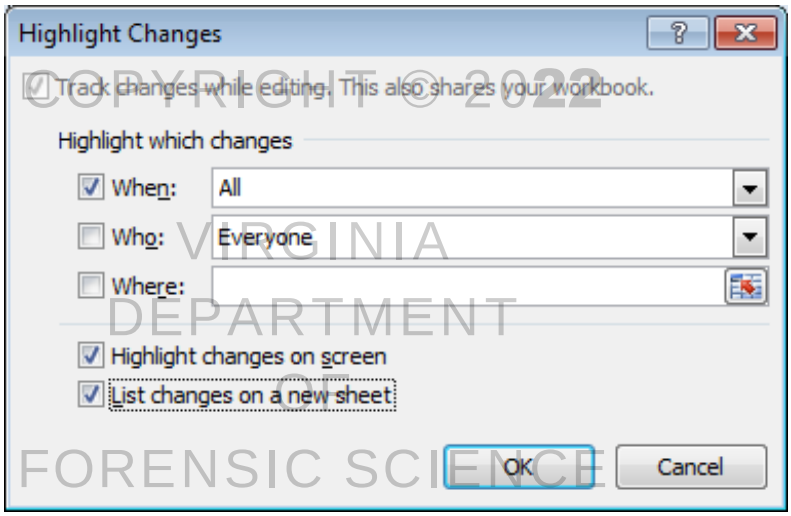
3.1 Examination Documentation

3.1.1 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.

3.1.2 Documentation may occur 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.

3.1.3 Notes originally recorded electronically shall use the current, approved and controlled workbook and appendix templates.

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



Highlight Changes Settings

3.1.3.1.1 "Old Value" should be filtered to not display "<blank>" or temporary placeholder values, or values where changes to cell content do not alter the original content; this will prevent cells that changed from a null to non-null value or from a temporary placeholder value, or did not have their original content altered, from being displayed.

3.1.3.2 Save the entire workbook to PDF, digitally sign the first page with your Department issued "Digital ID", and store in the appropriate Forensic Advantage Object Repository. If generating, signing, and/or storing the document electronically is not available, print the entire workbook to hardcopy and remove any electronic copies from the ECF.

3.1.3.2.1 Follow QM guidelines for any required changes to the notes.

3.1.4 A selection of commonly used acronyms and abbreviations are defined within Appendix A of this manual.

3.2 Evidence Sources

Evidence sources include original, physical evidence devices submitted for forensic examination, as well as data derived from such devices.

3.2.1 Derivative evidence acquired during examination shall be produced 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, produced derivative evidence should be compressed, encrypted and password–protected. The integrity of produced derivative evidence shall be verified by conducting and documenting a hash value comparison between the derivative evidence stored in the ECF and that produced.

COPYRIGHT © 2022 VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

3.2.2 Document in the analytical notes, on the original Request for Laboratory Examination (RFLE) and in the Certificate of Analysis (CoA), how the derivative evidence is identified and the method of return.

3.2.2.1 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.

3.2.2.2 Storage devices shall be assigned a "DME#" (e.g. DME1) item number and entered into the Laboratory Information Management System (LIMS) as an evidence item, stored within a sealed, evidence container, created in the laboratory.

3.3 Examination Results

3.3.1 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.

3.3.1.1 A malware scan shall be conducted against all native files exported from an evidence item and produced as an examination result. Details about the malware scanner (e.g., name, definition file version, etc.) shall be documented in the examination documentation. Information about any infected files shall be reported, but the files themselves shall not be produced.

COPYRIGHT © 2022 VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

3.3.2 Prior to preparing the case for technical review, examination results shall be preliminarily reviewed by another qualified examiner, and the review and any recommended changes made by the reviewer documented in the analytical notes. Follow the procedure described in the QM for disparities that arise between the examiner and reviewer. When required, reviewed results may be provided to approved parties, per the QM, prior to the completion of an examination or issuance of a CoA.

3.3.3 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.

3.3.4 Document in the analytical notes, on the original RFLE and in the CoA how the results are identified and the method of return.

3.3.4.1 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.

3.3.4.2 Storage devices shall be stored in a sealed container and attached to an evidence container (preferably evidence sources), or a documented, alternative method of return.

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

3.4 Electronic Case File

3.4.1 The Electronic Case File (ECF) is a temporary storage location that contains organized 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.

3.4.1.1 Examination results should be retained in the ECF unless the size of the dataset precludes (e.g. requires the use of storage media other than optical disc) it or with supervisor approval to exclude it.

3.4.1.2 Derivative evidence sources, excluding "Before First Unlock" (BFU) acquisitions, shall be retained in the ECF if they cannot be reacquired to the same degree (e.g., "After First Unlock" [AFU] / live devices, flash memory, etc.). If not retained, any supplemental acquisition information (e.g., logs, etc.) shall be retained.

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

3.4.2 At the completion of the case, the ECF shall be archived in a manner suitable for long-term availability and retrieval.

3.4.2.1 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.

3.4.2.2 The ECF archive shall be placed onto an external storage device, with an appropriate storage capacity. The storage device will be sealed in an appropriate container, labeled with the date sealed and initials of the sealer, 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 sealer.

3.4.3 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.

COPYRIGHT © 2022

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

4 INITIAL EXAMINATION & DATA ACQUISITION

4.1 Initial Examination

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

4.1.2 Follow any applicable initial examination guidelines, listed in the Computer Devices and Associated Digital Storage Devices, Mobile Devices and Associated Digital Storage Devices or Video & Image Analysis procedures sections of this manual.

4.2 Data Acquisition

4.2.1 The following steps shall be performed when acquiring original digital evidence physically or logically:

4.2.1.1 Select and document the approved and appropriate equipment utilized in the examination, as defined in the Equipment Validation, Verification and Use section of this manual.

COPYRIGHT © 2022

4.2.1.2 Access digital evidence as read-only or utilizing write-protecting mechanisms to ensure that data cannot be altered.

4.2.1.2.1 Not all devices can be accessed read-only or utilizing write-protection. If an eligible device is accessed as read-write, the reason shall be documented.

VIRGINIA

4.2.1.2.2 Read-only and write-protecting mechanisms are not required for mobile devices, or other devices where their internal storage is not removable, and/or is not accessible and/or recognizable by available equipment.

DEPARTMENT

4.2.1.3 Generate and document a source 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.

OF

4.2.1.3.1 When the original digital evidence is acquired using a method that automatically verifies it against its derivative copy, it is not required to generate a source hash value.

FORENSIC SCIENCE

4.2.1.3.2 A source hash is not required for a mobile device, or other devices where their internal storage is not removable, and/or is not accessible and/or recognizable by available equipment.

4.2.1.4 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. Document the date the copy was generated in the examination documentation.

4.2.1.4.1 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.

4.2.1.4.2 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.

4.2.1.4.3 Manual documentation (photography, video recording and/or transcription) of the information observed in a device’s displayed output may be necessary in situations where physical or logical data cannot be acquired.

4.2.1.5 Generate and document a hash value for the acquired derivative evidence.

4.2.1.6 Generate and document a post-acquisition 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.

4.2.1.6.1 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-acquisition hash value.

4.2.1.6.2 A post-acquisition hash is not required for a mobile device, or other devices where their internal storage is not removable, and/or is not accessible and/or recognizable by available equipment.

4.2.1.7 Compare the source, derivative evidence and, if applicable, post-acquisition hash values and document the result of the verification.

4.2.1.8 The DME section does not have the authority to access or acquire evidence source data that is stored on a cloud source; however, cloud data already obtained from a cloud source may be submitted for analysis.

4.3 Short Term Storage

4.3.1 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 to the QM.

COPYRIGHT © 2022
VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

5 COMPUTER & MOBILE DEVICE ANALYSIS

5.1 Purpose

Computer and mobile device analysis is the scientific examination of electronically stored information originating from a variety of computer, mobile and digital storage 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.

5.2 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.

5.3 Equipment

- Computer systems and peripherals
- Digital storage devices
- Mobile devices
- IoT devices
- Digital cameras
- Cables and adapters
- Operating System Equipment, Native Equipment, Common-Use Equipment, and Forensic Equipment

COPYRIGHT © 2022
VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

5.4 Limitations – Computer & Mobile Devices

- Remote lock /erase: 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.
- Device / data not supported by available equipment: currently there are no available methods that will acquire or parse all electronically stored information from all computer, mobile or digital storage devices.

  Conducting an analysis directly on the original submitted digital evidence should be avoided whenever possible. If the device can be accessed read-only or utilizing write-protection, and 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.
- Physical damage: devices may be nonfunctional or have limited functionality that prevent certain examinations. Repair or alternative methods may be necessary.

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.

5.5 Safety

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

Electrical shocks can occur if a device or its components are dismantled.

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

5.6 Procedures – Computer Devices and Associated Digital Storage Devices

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

5.6.2 Conduct a physical examination of the computer and document identifying information (i.e.,

manufacturer, model number, unique identifier, etc.), unusual markings, and defects.

5.6.3 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.

5.6.3.1 If defects or damage 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(s).

5.6.5 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.

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

5.6.6 The acquisition and verification of digital evidence shall be handled following the guidelines described in the Data Acquisition section of this manual.

COPYRIGHT © 2022

5.6.7 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 of this manual.

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

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

5.6.7.1.1 Unless otherwise directed, when possible, empty, incorrect, non-functional, system-generated data (i.e. generated by a device, OS, or application process, or part of the default installation of an OS or application, and not related to a user's actions), and/or data unrelated to the request should be excluded from reported examination results. In addition to manual review, filters, including data category, type, existence, hash set/category (e.g. NSRL) responsiveness, ownership, size, path, and other metadata and logic filters can be utilized in an exclusive or inclusive manner.

5.6.7.1.2 Unless otherwise directed, a date/time filter may be applied to parsed data encompassing a time frame beginning (at most) six (6) months prior to the offense date listed on the RFLE, and ending with the most recent date/time of activity identified within the parsed data.

5.6.7.1.3 For cases where the scope of the request is broad (e.g., all data on a device, all communications) the examination results identified via automated processes will be returned to the requesting agency as soon as practicable.

5.6.7.1.3.1 No manual analyses should be performed unless specifically requested or deemed necessary by the examiner. Any additional information related to the request, that would require such manual analyses to produce as a result, will be documented on the CoA.

5.6.7.1.3.2 After the review of the automated results, if the submitting agency determines additional data is required, the agency may resubmit the original and/or derivative evidence for an expedited, supplemental examination.

5.6.7.1.4 The examiner shall, when possible, verify that any identified and recovered data produced as an examination result, is an accurate depiction of what is on the submitted computer device. If the volume of data precludes this, a smaller, sampled dataset shall be used. Document any discrepancies.

5.6.7.1.4.1 Data associated with a broad request case that was identified via automated processes is exempt from verification.

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

UNCONTROLLED COPY

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

5.6.10 The use and retention of the ECF shall be handled following the guidelines as described in the Electronic Case File section of this manual.

5.7 Procedures – Mobile Devices and Associated Digital Storage Devices

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

5.7.2 Document the shielding method(s) employed.

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

5.7.4 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.

COPYRIGHT © 2022

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

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

5.7.6 Charge the device's battery, if necessary.

5.7.7 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.

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

5.7.8 The acquisition and verification of digital evidence shall be handled following the guidelines described in the Data Acquisition section of this manual.

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

5.7.8.2 For devices containing a [Universal] Integrated Circuit Card (U/ICC) or flash memory card, device data may be acquired while the U/ICC or flash memory card is removed from or installed in the device.

5.7.8.2.1 If the device is powered off, remove the U/ICC or flash memory card, acquire their data and, if required, create a clone of the U/ICC.

5.7.8.2.1.1 Powering on a device without the active U/ICC or flash memory card may result in the loss of data.

5.7.8.2.2 If the device is powered on, acquire the data with the U/ICC or flash memory card in the device.

5.7.8.2.2.1 This may alter certain metadata present on the U/ICC or flash memory card.

5.7.8.2.2.2 Once the device data is acquired, follow 5.7.9.2.1

5.7.8.2.3 If applicable, verify that the extracted data is consistent between the two methods of acquisition and document any issues or discrepancies.

5.7.9 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 of this manual.

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

5.7.9.1.1 Unless otherwise directed, when possible, empty, incorrect, non-functional, system-generated data (i.e. generated by a device, OS, or application process, or part of the default installation of an OS or application, and not related to a user's actions), and/or data unrelated to the request should be excluded from reported examination results. In addition to manual review, filters, including data

category, type, existence, hash set/category (e.g. NSRL) responsiveness, ownership, size, path, and other metadata and logic filters can be utilized in an exclusive or inclusive manner.

5.7.9.1.2 Unless otherwise directed, a date/time filter may be applied to parsed data encompassing a time frame beginning (at most) six (6) months prior to the offense date listed on the RFLE, and ending with the most recent date/time of activity identified within the parsed data.

5.7.9.1.3 For cases where the scope of the request is broad (e.g., all data on a device, all communications) the examination results identified via automated processes will be returned to the requesting agency as soon as practicable.

5.7.9.1.3.1 No manual analyses should be performed unless specifically requested or deemed necessary by the examiner. Any additional information related to the request, that would require such manual analyses to produce as a result, will be documented on the CoA.

COPYRIGHT © 2022

5.7.9.1.3.2 After the review of the automated results, if the submitting agency determines additional data is required, the agency may resubmit the original and/or derivative evidence for an expedited, supplemental examination.

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

5.7.9.1.4 The examiner shall, when possible, verify that any identified and recovered data produced as an examination result, 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.

5.7.9.1.4.1 Data associated with a broad request case that was identified via automated processes is exempt from verification.

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

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

5.7.12 The use and retention of the ECF shall be handled following the guidelines as described in the Electronic Case File section of this manual.

5.8 Procedures – National Center for Missing & Exploited Children (NCMEC) Child Recognition and Identification System (CRIS)

When examining evidence associated with a child exploitation offense, or if requested to do so by the submitting agency, the following steps list the process for identifying, submitting, and producing picture and video file examination results that are compared against the NCMEC CRIS:

5.8.1 Identify picture and video files related to the examination request;

5.8.2 Create a list of file metadata, including hash values, for the identified files;

5.8.3 Upload the unique hash values to the NCMEC's Law Enforcement Services Portal (LESP);

5.8.4 Receive the "Initial Hash Value Comparison Report" (IHVCP);

5.8.5 Organize examination results responsive to the NCMEC "Identified Child" category, and include only the NCMEC IHVCP report that contains "Identified Child" hash values;

5.8.5.1 Summarize the results of all categorized files in the CoA;

5.8.6 Provide any additional instructions that guide the submitting agency on any further interaction with the NCMEC.

5.9 Procedures – Data Authentication

Data authentication is the process of confirming the origin (i.e. provenance) and integrity of data. When

UNCONTROLLED COPY

examining evidence associated with a request for data authentication, the following guidelines should be followed:

5.9.1 Identification and review of applicable source device settings;

5.9.2 Identification and review of installed applications and functions with applicable editing capabilities;

5.9.3 File naming convention and file path analysis;

5.9.4 Identification and analysis of exact, near and visual duplicates;

5.9.5 Timeline analysis to include file system and internal timestamps;

5.9.6 Metadata (file system and internal) analysis;

5.9.7 File structure analysis;

5.9.8 Critical observation to include identification of unique content;

5.9.9 Identification and analysis of related and supporting files;

5.9.10 Comparison against reference files.

COPYRIGHT © 2022

5.10 References

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

VIRGINIA

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

DEPARTMENT

U.S. Department of Homeland Security, United States Secret Service. *Best Practices For Seizing Electronic Evidence: A Pocket Guide for First Responders*. Version 4.2. 2015.

OF

National Domestic Communications Assistance Center (NDCAC). *Best Practices for the Collection / Seizure of Mobile Devices for Law Enforcement*. Version 2.0. 2018.

FORENSIC SCIENCE

6 VIDEO & IMAGE ANALYSIS

6.1 Purpose

Video & image analysis includes the identification and recovery of electronically stored information originating from a variety of computer, mobile and digital storage devices, as well as the application of various techniques in order to clarify details and/or intelligibility, and provide data that is not readily apparent within an original multimedia or video recording, or image. 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.

6.2 Scope

This procedure applies to analog and digital multimedia and video recordings, and print and digital images in which analysis is requested.

6.3 Equipment

- Computer systems and peripherals
- Analog and digital video players/recorders
- Analog and digital storage devices
- Cameras
- Mobile devices
- IoT devices
- Speakers and headphones
- Monitors
- Printers
- Cables and adapters
- Operating System Equipment, Native Equipment, Common-Use Equipment, and Forensic Equipment

COPYRIGHT © 2022
VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

6.4 Limitations

It is not always possible to improve the clarity and/or intelligibility of the recordings or images, especially in instances of:

- Low resolution
- Limited focal length
- Compression
- Media wear
- Extremely poor signal-to-noise ratio
- Severe distortion
- Insufficient bandwidth
- 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.

6.5 Safety

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

Electrical shocks can occur if a device or its components are dismantled.

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

6.6 Procedures – Video & Image Analysis

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

6.6.2 For original digital recordings or images submitted on a computer or mobile device, or their associated digital storage devices, follow any applicable guidelines, listed in the Computer Devices and Associated Digital Storage Devices or Mobile Devices and Associated Digital Storage Devices procedures sections of this manual.

6.6.3 For original analog recordings or images, and derivative digital recording or images, conduct a physical examination of the analog or digital storage device and document identifying information (i.e., manufacturer, model number, unique identifier, etc.), unusual markings and defects.

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

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

6.6.6 The acquisition and verification of digital evidence shall be handled following the guidelines described in the Data Acquisition section of this manual.

6.6.6.1 Determine and document the model and settings (e.g., recording format, codec [FourCC], pixel dimensions, and frame rate) used to produce the original recording, if possible.

6.6.6.2 Document the device utilized to provide the optimal playback of the recording.

6.6.6.2.1 Analog Recordings

6.6.6.2.1.1 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.

6.6.6.2.1.2 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.

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

6.6.6.2.1.4 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.

6.6.6.2.2 Digital Recordings

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

6.6.6.3 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.

6.6.6.3.1 Print Images

6.6.6.3.1.1 This may require digitization of prints or conversion from other media.

COPYRIGHT © 2022 VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

6.6.6.3.1.2 Document any adjustments done during digitization.

6.6.6.3.2 Digital Images

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

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

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

6.6.7.2 Review the recording/image and document the steps applied to locate, capture and analyze the Area of Interest (AoI).

6.6.7.2.1 The AoI should be documented, when applicable, by using the date/time stamp on the recording, the player counter information or other identifying information (e.g. visual and/or audible activity identified from critical observation and/or listening).

COPYRIGHT © 2022

6.6.7.2.2 Capture the AoI and, when available and appropriate, save in an uncompressed, lossless or visually lossless file format.

6.6.7.2.3 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.

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

6.6.7.2.3.1 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.

6.6.7.3 Clarified recordings/images shall, when available and appropriate, be saved in an uncompressed, lossless or visually lossless file format.

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

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

6.6.10 The use and retention of the ECF shall be handled following the guidelines as described in the Electronic Case File section of this manual.

6.7 Procedures – Data Authentication

Data authentication is the process of confirming the origin (i.e. provenance) and integrity of data. When examining evidence associated with a request for data authentication, the following guidelines should be followed:

6.7.1 Identification and review of applicable source device settings;

6.7.2 Identification and review of installed applications and functions with applicable editing capabilities;

6.7.3 File naming convention and file path analysis;

6.7.4 Identification and analysis of exact, near and visual duplicates;

6.7.5 Timeline analysis to include file system and internal timestamps;

6.7.6 Metadata (file system and internal) analysis;

6.7.7 File structure analysis;

6.7.8 Track duration analysis;

6.7.9 Pixel dimensions and Display Access Ratio (DAR) analysis;

6.7.10 Frame-level analysis to include frame-level hashing and frame-by-frame review;

6.7.11 Group of Picture (GOP) analysis;

6.7.12 Critical listening and observation to include identification of anomalies (e.g., jump cuts, A/V synchronization);

6.7.13 Identification and analysis of related and supporting files;

6.7.14 Comparison against reference files.

6.8 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*.

U.S. Department of Homeland Security, United States Secret Service. *Best Practices For Seizing Electronic Evidence: A Pocket Guide for First Responders*. Version 4.2. 2015.

COPYRIGHT © 2022
VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

7 REPORTING GUIDELINES

7.1 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.

To ensure consistency within the section, the following report statements shall be used, to the extent possible, when reporting results. Report statements that address all situations cannot be provided; therefore, the following statements should be considered as example wording. If appropriate report wording is not available in the manual, look for wording that was previously applied in a similar situation, or consult with the Section Supervisor, 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.

7.2 Evidence Items

Information about submitted or "generated in-lab" evidence items.

COPYRIGHT © 2022
VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

7.2.1 Item #was the subject of a previous Digital & Multimedia Evidence examination report dated [month day, year].

AND/OR

Item # contains the derivative evidence, previously acquired from [Item # / INSERT SOURCE], that was utilized in this examination.

AND/OR

Sub-items not originally listed on the Request for Laboratory Examination (RFLE) were identified on or within their respective, submitted, parent items during the course of the examination.

AND/OR

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

7.3 Examination Results

Information about examination results media that is being provided.

7.3.1 Examination results include the data identified as being responsive to the examination request (see below "Request").

Please review the produced examination results, and if additional information is required, you may resubmit the original and/or derivative evidence (see below "EVIDENCE SOURCES") for an expedited, supplemental examination. Please contact the Department of Forensic Science's Digital & Multimedia Evidence Section, to discuss the type of testing that is needed prior to resubmission of the evidence.

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

A copy of these examination results [is / is not] being retained by the Department of Forensic Science [as part of the case file and for archival purposes only].

OR

No examination results are being returned.

7.4 Summary of Examination

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

7.4.1 Universal Statements

Request: Examine Item(s) [#] for [Insert requested data].

Initial examination and data acquisition procedures were utilized to acquire [physical / logical] data from Item(s) [#]. Due to the nature of electronically stored information, all data related to the request may not have been acquired.

OR

[Computer / Mobile device / Video / Image] analysis procedures were utilized to analyze Item(s) [#] and identify information related to the request. Due to the nature of electronically stored information, all information related to the request may not have been identified and/or produced, and additional information unrelated to the request may still be present on Item(s) [#].

AND/OR

In an effort to focus the examination results on activity occurring on and about the offense date (MM/DD/YYYY) listed on the Request for Laboratory Examination (RFLE), a date/time filter was applied to include activity beginning [six (6)] months prior to the offense date, and ending with the most recent date/time of activity identified on Item(s) [#]. Accordingly, the information listed below includes activity occurring [on and after / after / between] MM/DD/YYYY HH:MM:SS AM/PM TZ [and MM/DD/YYYY HH:MM:SS AM/PM TZ] [, as well as activity for which no timeframe could be determined].

COPYRIGHT © 2022

AND/OR

The information listed below was identified on Item(s) [#] using only automated processes. Additional information related to the request [may still be / is still] present on Item(s) [#], but will require additional analysis to produce.

VIRGINIA

AND/OR

DEPARTMENT

Due to the method of data acquisition, only existing data and limited, previously existing data on Item(s) [#] was accessible. Additional previously 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.

OF
FORENSIC SCIENCE

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

II. The requested information listed below has been identified on Item(s) [#], but will require additional analysis to produce:
    A. INSERT CATEGORY [Add additional as required]
        1. INSERT NAME/LOCATION OF INFORMATION
            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 data network] and may not necessarily reflect the actual date and time of the recorded event. The date and time settings for Item(s) [#] [could not be determined / were set manually / were set to allow for automatic updates from a network source], [and:

- The system clock for Item(s) [#]{was accurate / had a time difference of (+ / -) #} when compared to the current, local time].
    - [This time difference is most likely due to Item(s) [#] being without power and/or network connectivity for an extended period of time; additional analysis will be required in order to determine if the time difference affected the dates and times associated with the produced data.]

UNCONTROLLED
COPY

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.

AND/OR

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

AND/OR

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

AND/OR

[Full] Access could not be gained to Item(s) [#] due to [INSERT REASON] OR [the presence of INSERT SECURITY MEASURE which could not be [identified / bypassed; therefore, [no / limited] results were produced. Should the INSERT SECURITY MEASURE be identified or circumventable in the future, Item(s) [#] can be resubmitted for analysis].

COPYRIGHT © 2022

AND/OR

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

AND/OR

A malware scan [was / was not] performed against Item(s) [#]. Malware was not identified on Item(s) [#].

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

AND/OR

No analysis was performed on Item(s) [#].

AND/OR

The requested Digital & Multimedia Evidence examination was terminated at the request of INSERT REQUESTOR NAME, of the INSERT REQUESTOR AGENCY, on INSERT DATE.

If it is determined that an examination(s) is still required, please contact the Department of Forensic Science's Digital & Multimedia Evidence Section, to discuss the type of testing that is needed prior to resubmission of the evidence.

AND/OR

Usage of Item(s) [#] is not recommended should future analysis be required. In order to prevent possible data loss, Item(s) # is being returned with ["Airplane mode" enabled (device radios that transmit data are turned off), and its associated UICC (Universal Integrated Circuit Card) / storage device(s) removed/disconnected/disabled].

7.4.2 Video & Image Analysis Statements

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

AND/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

Proper aspect ratio must be maintained when viewing the produced [multimedia/video recording(s) / still image(s)]. The analysis determined that the aspect ratio of the submitted [multimedia/video recording(s) / still image(s)] was [#:#]; however, due to the nature of recorded [multimedia/video / still image(s)], the determined aspect ratio may differ from the actual aspect ratio in use at the time the submitted [multimedia/video recording(s) / still image(s)] [was/were] originally recorded.

AND/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.

AND/OR

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.

AND/OR

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

AND/OR

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

7.5 Evidence Sources

COPYRIGHT © 2022

Information about derivative evidence media that is being provided.

7.5.1 Evidence sources include the acquired data available for extraction from supported, submitted evidence items. This acquired data is considered derivative evidence, and should be maintained and submitted if additional analysis is required.

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

Initial examination and data acquisition procedures were utilized to acquire [physical / logical] data from Item(s) [#]; this acquired data was used as the primary, derivative evidence source for this analysis.

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

A copy of [this / these] evidence source(s) [is / is not] being retained by the Department of Forensic Science [as part of the case file and for archival purposes only].

OR

No evidence sources are being returned.

7.6 Methods

Information about methods utilized in the examination.

7.6.1 The following methods were utilized during the examination:

- Equipment Name

Date(s) of testing: mm/dd/yyyy – mm/dd/yyyy. Supporting examination documentation[, including a method {deviation, addition, exclusion},] is maintained in the case file. The above listed methods are those approved for use at the time of analysis. Current procedures can be found in the Digital & Multimedia Evidence Section Procedures Manual, which can be found at www.dfs.virginia.gov/documentation-publications/manuals/.

7.7 Disposition of Evidence

Document in the CoA according to the Quality Manual.

7.8 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

AFU – After First Unlock

AoI – Area of Interest

A/V – Audio/Visual

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

API – Application Programming Interface

BD – Blu–ray Disc

BD-DL – Dual-layer Blu-ray Disc

BD-TL/XL – Triple-layer Blu-ray Disc

BFU – Before First Unlock

BGA – Ball Grid Array

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

DAR – Display Aspect Ratio

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

E – Existing

ECF – Electronic Case File

EDT – Eastern Daylight Time

eMMC- embedded MultiMediaCard

COPYRIGHT © 2022
VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

eMCP – embedded Multi-Chip Package

EP – Extended Play mode

ESN – Electronic Serial Number

EST – Eastern Standard Time

ET – Eastern Time

EXT Data – Extended Data

FBE – File-Based Encryption

FDE – Full-Disk Encryption

FE – Forensic Equipment

FourCC – Four Character Code

Fps – Frames per second

Freq – Frequency

FSE – File System Extraction

GOP – Group of Pictures

GSM – Global Systems for Mobile Communications

HD – High Density

HDD – Hard Disk Drive

Hi–8 – Hi–8mm video cassette

Hz – hertz

IC – Integrated Circuit

ICC – Integrated Circuit Card

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

IO – Investigating Officer

IoT – Internet of Things

IPS – Images Per Second

ISP – In-System Programming

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

JTAG – Joint Test Action Group

kHz – Kilohertz

Ki – 128 Bit Encryption Key

L – Left

LAI – Location Area Identity

LE – Logical Extraction

COPYRIGHT © 2022
VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

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)

MMC - MultiMediaCard

MMS – Multimedia Messaging Service

Mono – Monophonic

MSISDN – Mobile Station International Subscriber Directory Number or Mobile Subscriber Integrated Services Digital Network Number

COPYRIGHT © 2022

NE – Native Equipment

NSRL - National Software Reference Library

NTSC – National Television Standards Committee

VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

NVMe – Non-Volatile Memory Express

OSD – On-System Display

OSE – Operating System Equipment

PATA – Parallel AT Attachment

PCIe - Peripheral Component Interconnect Express

PE – Physical Extraction or Previously Existing

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

RM – Restricted Mode

ROM – Read–Only Memory

Rtn – Return

[R]VS – [Refine] Volume Snapshot

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)

SE – Secure Element

SEN – Sealed Envelope

SIM – Subscriber Identity Module

SLP – Standard Long Play mode

SMS – Short Message Service

SMSC – Short Message Service Center

COPYRIGHT © 2022

S/N – Serial Number

SO – Small Outline

SP – Standard Play mode

SPI – Serial Peripheral Interface

VIRGINIA
DEPARTMENT
OF
FORENSIC SCIENCE

SPLB – Sealed Plastic Bag

SSD – Solid State Drive

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

TAP – Test Access Port

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

UART - Universal Asynchronous Receiver/Transmitter

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