Department of Forensic Science

DIGITAL & MULTIMEDIA EVIDENCE SECTION PROCEDURES MANUAL

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Introduction

The Digital & Multimedia Evidence Section encompasses the analysis of evidence in analog or digital form. The section is divided into the sub-disciplines of Audio Analysis, Computer Forensics, Image Analysis and Video Analysis.

- Forensic Audio Analysis is the scientific examination of recordings for the purpose of increased intelligibility, attenuation of noise, improvement of intelligibility of the recorded material and/or improvement of the over all quality. Forensic Audio Analysis can be applied to both analog and digital recordings. These recordings include, but are not limited to the following: recordings from mobile devices, body microphones, answering machines, 911 phone recordings, etc. Additionally, this discipline includes the reconstruction (repair)of analog media if required

- Computer Forensics involves the scientific examination, analysis and/or evaluation of digital evidence contained on a wide variety of devices. These devices include, but are not limited to the following: computer towers, laptops, tablets, mobile devices, hard drives, CD's, DVD's and other digital storage devices.

- Forensic Image Analysis is the application of image science and domain expertise to examine and interpret the content of an image and/or the image itself. Image analysis can be conducted on areas of interest obtained from video evidence. Image analysis can include:

  - Image clarification: the process applied to images in an effort to improve the visual appearance of an image or specific features within an image.
  - Image comparison: the process of comparing images of unknown objects or persons to known objects, persons or images, making assessment of the correspondence between features in these images and rendering an opinion regarding individualization or elimination.
  - Image analysis: the drawing of a conclusion regarding an image. Targets for analysis include, but are not limited to: the subjects/objects within an image, the conditions under which the image was captured or created, the physical aspect of the scene (i.e. environmental conditions) and/or the origin of the image.

- Forensic Video Analysis involves the scientific examination and comparison of video (analog or digital) evidence. Video clarification is a process intended to improve the visual appearance of video recording sequences or specific features within the video recording. Additionally this discipline includes the reconstruction (repair) of analog media if required.

1.2 Examination Documentation

1.2.1 Documentation may be accomplished through handwritten or electronically generated hardcopy notes, photographs and/or photocopies that can be retained as hard copies or stored electronically in the case folder.

1.2.2 Prior to examination, verify that the submitted evidence does not require any additional analyses that would include other disciplines for example, latent prints, forensic biology, etc.

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

1.2.4 The following steps shall be performed on all submitted digital media:

- Create an electronic case file on the appropriate workstation.
- Generate a hash for the submitted media and save the value in the electronic case file
- Access and transfer a bit-for-bit copy from the submitted media onto the appropriate workstation
- Generate a hash for the data on the workstation and save the value in the electronic case file

- Generate a hash for the submitted media after the transfer and save the value in the electronic case file.
- Compare the hash value of the data on the workstation to the hash values associated with the submitted media, before and after transfer of a bit-for-bit copy.
- Document in the notes the result of the verification or any discrepancies.
- When utilizing a Read-Only drive, it is not required to generate a hash for the submitted media after the transfer.

1.2.5 Worksheets DFS Document 242-F101 and DFS Document 242-F102 are controlled forms and shall be use in taking of handwritten analytical notes.

1.2.6 Examination documentation (case notes) shall contain sufficient detail to allow another qualified examiner to understand the sequence of testing performed such that it is possible to repeat the analysis under conditions as close as possible to the original, evaluate the data, interpret the results and come to the same conclusion.

1.2.7 Examination documentation shall include the start date, dates of the performance of tests and the end date. The ending date reflects the date when the analysis was completed.

1.2.8 The electronic case folder is a temporary storage location on the workstation computer which contains the original (raw), captured, clarified and recovered files. The case folder may also contain the electronic documentation of the performance check, generated hash values and other pertinent information.

1.3 Results

1.3.1 Verify that all content was transferred successfully and the quality of the output accurately reflects the results of the analysis. Any results provided on digital media shall be verified by conducting a hash. This verification shall be documented in the notes.

1.3.2 All digital media containing examination results shall have a hash value generated, documented in the electronic case file and noted as the "Results Hash" prior to returning the media to the submitting agency.

1.3.3 Document in the notes, on the original RFLE and in the CoA which container the media is being returned in or with.

1.3.3.1 It is acceptable to have one piece of media containing results from numerous items of evidence as long as it is documented clearly in the notes. If multiple pieces of media are necessary, the contents of each shall be clearly described in the notes.

1.3.4 If the media does not fit in the original container, seal the results media in an appropriate container and attach it to the original evidence container.

1.4 Password Protection

In order to prevent unauthorized access to computer systems used for examining digital evidence, all workstations will be password protected and these passwords will remain confidential within the section.

1.5 Accessing Restricted Internet Sites

At times, it is necessary for the forensic scientists (examiners) in this section to access internet sites to download, print and/or store information that may be considered to be in violation of the Department of Human resource Management Policy Number 1.75 - Use of the Internet and electronic Communication System (effective date: 8/10/01) and Virginia Code 2.2-2827.

Routinely, the forensic scientists (examiners) in this section are requested by law enforcement agencies and attorneys for the Commonwealth to perform analysis on computers and other digital/multimedia devices to retrieve suspected child pornographic images. Once files on the device are located, it is necessary for the scientist to access the proprietary software on the internet, using the information that is embedded in the data, to observe and

authenticate the images/video clips on the multimedia device. Without the proprietary software, the files cannot be viewed. The necessity to access, download, print and store information from these sites is a function that is primarily required in the computer and mobile device recovery sub-disciplines. There are also situations that may require access in the sub discipline of forensic image and video analysis. Images and sites that are accessed will be documented in the case notes.

1.6 Short Term Storage

Short term storage is used when evidence is in the process of examination. The length of time evidence may remain in short term storage will be thirty (30) days. After this time period, evidence must be placed into long term storage and properly sealed according the Quality Manual.

2 EQUIPMENT MAINTENANCE/QUALITY ASSURANCE

2.1 Introduction

2.1.1 The reliability and performance of the systems used in the analysis of digital evidence is done to establish a baseline and reference point to ensure the equipment is operating properly.

2.1.2 It is expected that the examiners will report any unacceptable or anomalous performance of the equipment/instrumentation immediately to the Section Supervisor

2.2 Equipment

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

2.2.2 All maintenance is to be documented and retained in the appropriate log book located in the respective laboratory.

2.3 Performance Checks

A performance check is a quality assurance measure to assess the functionality of the laboratory instruments and equipment associated with the workstation being utilized for the analysis that may affect the accuracy of forensic analysis. A performance check shall be completed and documented, electronically or as a hard copy, in the case file each time the system(s) is powered up (minimally) or at the examiner discretion.

The hardware performance check is the same for all workstations within the section. The utilized software checks the functionality of the computer and renders a numerical value.

- The values for the performance check shall be a value of $^{+}$/- 100 of the previous performance check.
- Values between systems and their components will vary and should be considered when determining if the results are acceptable for the particular workstation being checked.
- Case file documentation will include the current and previous values.

2.3.1 Video Analysis

2.3.1.1 An analog and/or digital media hardware performance check for the video analysis systems will consist of a prerecorded color bar, frame counter and audio tone recording utilizing the proper media format per case requirements.

2.3.1.2 An 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.

2.3.2 Audio Analysis

2.3.2.1 Analog and digital performance checks will consist of a prerecorded audible tone on the appropriate media for that particular analysis to be conducted.

2.3.2.2 The acceptable result is a series of audible tones.

2.3.3 Computer Analysis

No additional checks are required other than the hardware performance check listed above.

2.4 Verification Checks

A verification check is confirmation that the equipment or instrument performs as expected after repair or maintenance.

2.4.1 In the event that repairs or modifications are performed on equipment/instruments, a verification check will be conducted before the system or any of its components are utilized for casework purposes.

2.4.2 The performance check procedure may be used for the verification check. If other methods or procedures are conducted, the proper documentation shall be maintained in the maintenance log.

2.4.3 Documentation of equipment maintenance and verification checks shall be maintained in the section maintenance logs in accordance with the Quality Manual using DFS Documents 242-F106, 242-F107 and 242-F111.

2.5 Archiving

2.5.1 Archiving is the process of storing data in a manner suitable for long-term availability and retrieval, from which subsequent working copies can be produced.

2.5.2 A case file shall include, but is not limited to the following: performance check results, hash values, original data, clarified data and other information deemed necessary by the examiner. The case file may be a combination of hard copy documents and electronically saved data.

2.5.2.1 Each electronic file contained in the case file shall have a hash generated prior to archiving to ensure changes can be tracked.

2.5.3 The information/data saved electronically shall be archived onto external media at the completion of the case. In cases where the external media is a hard drive, which contains numerous case files, the hard copy case notes will reflect the hard drive number on which the particular case is stored.

2.5.4 When the external media is a CD/DVD it will be sealed in an envelope, attached to the case notes and stored in the laboratory file storage area.

2.5.5 When the hard drive is at or near capacity, a log sheet containing the electronic case files stored on the device will be produced and forwarded with the device to the laboratory's file storage area. Additional copies of the log sheets may be produced and retained in the laboratory.

2.5.6 Generate a hash for the archived media and document the value on the log sheet.

2.5.7 Prior to working from archived media, generate a hash and verify that values documented on the log sheet or in the case file are the same. If a discrepancy exists notify the Section Supervisor and the Program Manager.

3 AUDIO ANALYSIS

3.1 Purpose

Forensic audio analysis includes the application of various techniques in order to clarify the intelligibility of audio signals recorded onto magnetic media, digital media, analog video recordings, digital video recordings or other media. Certain inherent qualities of audio evidence prohibit the establishment of a rigid set of standard procedures to cover each and every case; therefore, enough latitude has been given to allow for independent thought and individual freedom in selection of alternative courses of action.

3.2 Scope

This procedure applies to analog and digital audio recordings in which clarification may be deemed necessary.

3.3 Equipment

- Consumer and professional grade analog and digital tape players/recorders
- Analog and digital filters
- Professional headphones
- Digital storage devices
- Mobile devices
- Cables and cable connectors
- Magnetic tape developer
- Computer hardware and software

3.4 Limitations

It is not always possible to improve the intelligibility of the voice signal information, especially in instances of:

- extremely poor signal-to-noise ratio
- severe distortion
- insufficient bandwidth
- technical limitations of the recording devices/systems utilized to make the original recording
- the physical environment where the original recording was produced

3.5 Safety

None for this procedure

3.6 Procedures

3.6.1 Prevent modification of submitted media contents.

3.6.1.1 For analog-based media, record tabs shall be removed or moved to the write-protect position. Any items removed will be retained and returned with the evidence.

3.6.1.2 Read-only drives or write-blocking methods, whether hardware or software, should be utilized and documented for any digital media whenever possible.

3.6.2 Determine the most suitable equipment and settings for capturing the audio signal.

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

3.6.2.1.1 Analog

3.6.2.1.1.1 When playback of the evidentiary recording is less than optimal, signal loss occurs and/or player idiosyncrasies are suspected as a potential factor, it may necessitate retrieving the original recorder.

3.6.2.1.1.2 Document if adjustments are done to optimize playback.

3.6.2.1.1.3 Any action or equipment that may cause damage to the original recording is inappropriate and should not be utilized. Such actions may include but are not limited to: maintaining the recording in the "pause" mode for extended periods, unnecessarily repeated playback and placing the media in close proximity to strong magnetic fields.

3.6.2.1.2 Digital

3.6.2.1.2.1 Transfer a bit-for-bit copy to a workstation. Generate a hash to verify the transferred data as described in the Introduction section of this manual.

3.6.2.1.2.2 Identify and document the proprietary file format to access the recording, if applicable.

3.6.3 An overall review shall be conducted and documented to determine the approximate length of the recording, tape speed, type of information recorded and features that may affect or limit intelligibility (interference, environmental noise, multiple voices, etc).

3.6.4 Engage in Critical Listening to locate the specific area of interest (AOI) utilizing the working copy of the original evidence.

3.6.5 Identify, if available, and document an overall analysis of speech frequencies, discrete tones, banded noise and other significant information.

3.6.6 The audio signal may be clarified using a number of processing options that may include but are not limited to the following:

- Bandpass filtering
- Comb filtering
- Adaptive filtering
- Lowpass filter
- Spectral inverse filter

3.6.7 The processes used to generate the final clarified signal shall be documented in the case file notes. The documentation can consist of computer generated printouts and/or handwritten notes.

3.6.8 The clarified audio signals are recorded to digital media (read only CD, DVD), unless otherwise requested by the submitting agency and returned with the submitted evidence.

3.7 References

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

http://www.swgde.org/documents

http://www.theiai.org/guidelines/swgit/index.php

Ballou, Glen M., ed. Handbook for Sound Engineers the New Audio Cyclopedia. 2nd ed. Caramel, IN: SAMS, 1987.

Koening, Bruce E. "Authentication of Forensic Audio recordings", Journal of the Audio Engineering Society, vol. 36, No 36, No. ½, 1990 January/February.

Solari, Stephen J., Digital Video and Audio Compression. New Your; McGraw-Hill, 1997.

Watkinson, John. The Art of Digital Audio. 2nd ed. Oxford: Focal Press, 1994.

4 IMAGE ANALYSIS

4.1 Purpose

Forensic image analysis can involve the examination, clarification and interpretation of images recorded in a variety of formats and media types. Interpretation is the application of specific subject matter expertise to draw a conclusion about the subjects or objects depicted in the images. Examination is the application of image science expertise to extract and/or clarify information present in the image(s). Image clarification, restoration or processing activities are intended to improve the visual appearance or features in an image. This procedure can be used as a stand-alone analysis process or may be the precursor to further forensic analysis. There are inherent qualities that prohibit the establishment of a rigid set of procedures to cover each and every case; therefore, enough latitude has been given to allow for independent thought and individual freedom in selection of alternative courses of action.

4.2 Scope

This procedure applies to all digital still cameras and digital video cameras with transferring capabilities. This can include, but is not limited to the following: digital storage media, flash media, hard drives, etc. Also included within the scope of this procedure is comparative analysis of known images and objects to unknown images and objects.

4.3 Equipment

The following equipment and materials may be utilized:

- Computer hardware and software
- Cameras
- Cleaning materials
- Imaged hard drive(s)
- Mobile device(s)
- Other image storage devices
- Approved graphics viewer software
- Standard computer tools
- Forensic Imaging hardware and software

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

4.4 Limitations

It is not always possible to improve an image, especially in instances of:

- extremely poor resolution
- limited focal length
- compression
- technical limitations of recording device/systems utilized to make the original recording

4.5 Safety

None on this procedure

4.6 Procedures

4.6.1 If applicable, document the make, model, serial number and external markings of the evidence

4.6.2 Obtain applicable User's Manual of the specific device, if necessary.

4.6.3 Perform an assessment of the evidence to determine the appropriate acquisition method.

4.6.3.1 The acquisition of the images shall be done in a manner in which the integrity of the original image is preserved and archived in a manner that permits verification.

4.6.3.2 Document the device utilized in the acquisition of the images to the workstation.

4.6.4 Consult the RFLE, Supplemental Submission form or contact the Investigator to identify of the image(s) requiring analysis.

4.6.5 Produce working copies of the images to be utilized in the analysis.

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

4.6.6 Clarify the images, if required, and document all steps and routines utilized. This can be in the form of handwritten notes, printouts or a combination of the two.

4.6.7 In the cases where a comparison is necessary, the examiner has the discretion to recover the images that best represent the individual or object to compare to the known individual or object.

4.6.8 The following process is applied to the comparison of object(s) or person(s) depicted in the image:

4.6.8.1 Assess the image to determine if it is suitable for comparison. Document technical or visual information which may include, but is not limited to the following: resolution, sharpness, clarity, brightness, contrast and/or obstructed view which may limit the conclusion of a comparison.

4.6.8.1.1 If the image(s) are deemed not suitable for comparison, the notes shall contain sufficient documentation to justify the conclusion.

4.6.8.2 Document characteristics (class and individual) by marking printouts or utilizing approved software (i.e. Adobe Photoshop) and provide a written description in the case notes prior to comparing the known to the unknown. The documentation of characteristics in this step demonstrates the thought process leading into the comparison.

4.6.8.3 Compare the images to determine if they contain class or individual characteristics previously documented in Section 4.6.9.2. Three types of differences may be observed:

4.6.8.3.1 Explainable differences, resulting from the imaging process or conditions in the area of interest (AOI).

4.6.8.3.2 Unexplainable differences, of an unknown source and significance.

4.6.8.3.3 Exclusionary differences, reflecting a true difference between the objects under comparison and establishing elimination.

4.6.8.4 Formulate a conclusion based upon the comparison.

4.6.8.4.1 Individualization: This is the highest degree of an association expressed in comparative analysis examinations. This opinion means that a particular individual or object is one in the same with the known individual or object to the exclusion of all others.

4.6.8.4.2 Inconclusive: This opinion means some similarities are noted; however, there are significant limiting factors in the known image or object that does not permit a specific association.

4.6.8.4.3 Elimination: This is the highest degree of non association expressed in comparative analysis examinations. This opinion means that the two images or objects are not the same.

4.6.8.5 Comparison conclusions shall be verified by another qualified examiner prior to communicating the information, either verbally or in writing.

4.6.8.5.1 Verifications shall be documented by means of the verifying examiner's handwritten notation(s) on the appropriate worksheet, to include their initials and the date.

4.6.9 When requested, perform an image analysis and document, if applicable, the following: the subjects/objects within an image, the conditions under which the image was captured, the process by which the image was captured or created and/or the physical aspect of the scene (i.e. environmental conditions).

4.6.10 Results may be presented as a chart, CD/DVD, printouts or other means that are deemed appropriate by the examiner and/or the requestor.

4.7 References

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

http://www.swgde.org

Blitzer, Herbert L., and Jack Jacobia. Forensic Digital Imaging and Photography. San Diego: Academy Press, 2002.

Damjanovski, Vlado. CCTV Networking and Digital Technology. 2nd ed. Amsterdam: Elsevier Butterworth-Heinemann, 2005.

Inglis, Andrew F. and Arch C Luther. Video Engineering. 2nd ed. New York: McGraw-Hill, 1996.

Kruse, Warren G., and Jay G. Heiser., Computer Forensics Incident response essentials. Boston: Addison-Weslye, 2002.

Madisetti, Vijay K., and Douglass B. Williams, eds. The Digital Signal Processing handbook. N.p.: CRC Press LLC, 1998.

Solari, Stephen J., Digital Video and Audio Comprerssion. New York; McGraw-Hill, 1997.

Utz, Peter. Today's Video. 4th ed. Jefferson, NC: McFarland and Company, Inc., 2006.

Whitaker, Jerry, and Blair Benson. Standard Handbook of Video and Television Engineering. 3rd ed. New York: McGraw-Hill, 2000.

Electronic Crime Scene Investigation a guide for First Responders. Washington, D.C. : U. S. department of Justice, 2001.

Best Practices for Seizing Electronic Evidence a Pocket Guide for First Responders. 3rded. Washington, D. C.: U. S. Department of Homeland Security, United States Secret Service.

Gill, Robert W. Basic Perspective, Thames and Hudson, London, 1974 96 pp.

5 COMPUTER FORENSICS

5.1 Purpose

Computer Forensics includes the recovery of data from a variety of digital devices to include mobile devices. Due to the vast number and types of devices currently in use, there are inherent qualities that prohibit the establishment of a rigid set of procedures to cover each and every case; therefore, enough latitude has been given to allow for independent thought and individual freedom in selection of alternative courses of action applied.

5.2 Scope

This procedure applies to all mobile devices, computers and digital storage media. This can include, but is not limited to the following: towers, laptops, net books, tablets, mobile devices, CD/DVD's, flash media, digital cameras, etc. It should be noted that due to the vast array of types of evidence, there will be cases that require analysis that fall under the other sub-disciplines of Digital & Multimedia Evidence for example, audio analysis, image analysis and video analysis.

5.3 Equipment

- Computer hardware and software
- Cameras
- Hard drives
- Mobile devices
- Other digital storage media
- Standard computer tools
- Proprietary forensic hardware and software

5.4 Limitations – Mobile Devices

Currently there is no software available that will acquire all user data in the memory of all mobile devices. Some type of manual transcription (photography, video recording and/or handwritten notes) may be necessary to recover and document the data on the mobile device's display.

Software tools may not recover all data on all devices. This limitation can be identified through manual review of recovered data, with the exception of a physical acquisition.

Evidence submitted to the Digital & Multimedia Evidence Section that contains the ability to receive or transmit data will be immediately placed in the shielded laboratory and will remain in that location until which time the analysis has been completed or the device(s) have been rendered in a state that prohibits the device(s) from receiving or transmitting data.

5.5 Limitations – Computers

Conducting an examination on the original submitted digital media should be avoided if possible. If an image of the submitted digital media cannot be produced and the media can be appropriately write-protected, it is permissible to analyze the original submitted media without making a forensic image. Notes shall contain documentation indicating why it was not possible to create an image.

5.6 Safety

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

5.7 Procedures – Mobile Devices

5.7.1 Network isolation of the mobile device(s) should be maintained through radio frequency shielding during mobile device examinations. These examinations are to only be conducted within a shielded laboratory.

The device may be removed from the shielded laboratory for documentation purposes once the device has been isolated from the network.

5.7.2 Conduct a physical examination of the device and document manufacturer information (i.e. model number, serial number, etc.) and unusual markings.

5.7.3 Charge the device, if necessary.

5.7.4 Select and document the appropriate data cable to connect the mobile device to the workstation. This documentation may be in the form of handwritten notes or within the recovery software template.

5.7.5 Select and document the appropriate software application for the mobile device. It may be necessary to utilize several different software applications to recover as much data as possible.

5.7.6 For all devices that require a Subscriber Identity Module (SIM), the examiner shall process the SIM twice; installed and uninstalled from the device.

5.7.6.1 If the device is inactive (powered off), remove the SIM and acquire its data with a validated tool first.

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

5.7.6.2 If the device is active (powered on), acquire the data with the SIM in the device using a validated tool

5.7.6.2.1 This may alter the status flags of unread text messages present on the SIM.

5.7.6.3 Verify the data recovered is consistent between the two methods of acquisition. Document any discrepancies in the case notes.

5.7.7 Devices containing removable media (i.e. microSD card) may be processed separate from the device as well as within the device.

5.7.8 If a physical acquisition is requested, to obtain deleted data not recoverable through either a logical acquisition or a manual examination, select and document the method (to include software and hardware) utilized.

5.7.8.1 If the device is not supported by the available mobile device analysis systems then the Computer Procedures shall be followed for the physical acquisition of removable media.

5.7.8.2 The analysis of the removable media, utilizing the Computer Procedures, shall be treated as Instrument Support as described in Section 14 of the Quality Manual.

5.7.9 The examiner shall ensure the data recovered utilizing the software applications is an accurate depiction of what is on the submitted mobile device. Document any discrepancies if present in the examination notes.

5.7.10 All recovered data must be documented in the examination notes

5.7.11 The requested data shall be written to the appropriate media and returned with the original submitted evidence. If the media contains data recovered but not requested, it shall be clearly communicated on the CoA.

5.8 Procedures – Computers

5.8.1 Utilize write-blocking hardware or software to ensure that the submitted digital media data cannot be altered.

5.8.1.1 Not all devices can be accessed through a write-blocker. In the event that a device fails to be accessible or recognized through a write-blocker, it may be necessary to image the device without utilizing a write-blocker. Document in the notes if a write-blocker is not utilized.

5.8.2 Generate and document a hash value for the submitted digital media.

5.8.3 Create a forensic image (backup) of the submitted digital media and document the systems employed.

5.8.3.1 If a forensic copy of the device is generated the target drive must have storage capacity greater than or equal to the storage capacity of the device.

5.8.3.2 If forensic evidence files are generated the storage capacity may vary depending on the type of image file being generated (dd, EO, etc) and if applicable the compression utilized. This type of imaging generates discrete forensic files thus cross contamination is not a concern. It is acceptable that multiple devices from multiple cases be imaged to a single drive if the forensic backup is generated using forensic evidence files. These files shall be placed in a unique folder with the appropriate identifiers for each device.

5.8.4 Generate and document a hash value for the image(s) created on the target drive.

5.8.5 Document the comparison of the hash values of the submitted digital media to the target drive.

5.8.6 Utilize the appropriate forensic data recovery software to process the data. Document the processes utilized and the results. Processes may include, but are not limited to the following: hash file, file signature analysis, text index and data carving.

5.8.7 Analyze the information contained within the processed data to identify the files that meet the request indicated on the RFLE.

5.8.8 Transfer the identified files to the casework folder.

5.8.9 The identified files, those which were requested on the RFLE, should be written to the appropriate media for return with the submitted evidence.

5.9 References

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

http://www.swgde.org/documents

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

Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders. 3rd ed. Washington, D.C.: U.S. Department of Homeland Security United States Secret Service.

Bigelow, Stephen J. Troubleshooting, Maintaining and Repairing PCs. 2nd ed. New York: McGraw-Hill, 1999

Electronic Crime Scene Investigations: A Guide for First Responders. Washington, D.C.: U.S. Department of Justice, 2001.

Growth, David. A+ Complete Study Guide. 3rd ed. San Francisco: SYBEX, 2003.

Hoffman, Daniel V. Blackjacking: Security Threats to Blackberry Devices, PDAs, and Cell Phones in the Enterprise. Indianapolis: Wiley, 2007.

Jurick, David, Adam Stularz, and Damien Stularz. iPhone Hacks. Beijing: O'Reilly, 2009.

Kruse II, Warren G. and Jay G. Heiser, Computer Forensics, Incident Response Essentials. Boston: Addison-Wesley, 2002.

Nelson, Stephen L. Windows XP: An Introduction. New York: Barnes and Noble Books, 2002.

Rathbone, Andy. Windows 95 for Dummies. 2nd ed. Foster City, CA: IDG Books Worldwide, 1997.

Zdziarski, Jonathan. iPhone Forensics. Beijing: O'Reilly, 2008.

6 VIDEO ANALYSIS

6.1 Purpose

The purpose of analyzing a video recording is to clarify details, perform comparisons, if applicable, and provide data that is not readily apparent within the original recording. There are inherent qualities that prohibit the establishment of a rigid set of procedures to cover each and every case; therefore, enough latitude has been given to allow for independent thought and individual freedom in selection of alternative courses of action applied for the recovery of data.

6.2 Scope

This procedure applies to analog and digital video analysis. The procedures in Section 4, Image Analysis, shall be employed when a comparison analysis is requested. Media containing video can include, but is not limited to the following: digital still cameras with video capabilities, digital video cameras, mobile devices, digital storage media, etc.

6.3 Equipment

- Video recorders/players (consumer, professional and security time lapse)
- Multiplexers
- Time base correctors
- Mobile Phones
- Other image/video storage devices
- Professional headphones
- Professional monitors
- Computer hardware and software
- Audio/Video cables (BNC, XLR, RCA, etc)
- Printers and appropriate output media
- A variety of digital storage devices (CD-R, DVD-R, Hard Drives, Thumb Drives, etc)

6.4 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 may also hinder and/or limit the results of the analysis

6.5 Safety

None for this procedure

6.6 Procedures

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

6.6.2 Prevent modification of the submitted media contents.

6.6.2.1 For analog-based media, the record tab shall be removed or moved to the write-protect position. Any items removed will be retained and returned with the original submitted evidence.

6.6.2.2 Read-only drives or write-block methods, whether hardware or software, should be utilized and documented for any digital media whenever possible. Note: when analyzing DVR's technical situations may arise that may prevent the recovery of data when a write-blocking method is applied; therefore, when this situation arises, it will be evaluated on a case-by-case basis and documented in the case notes.

6.6.3 Determine the most suitable equipment and settings for capturing the video signal.

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

6.6.3.2 Document the playback device utilized to provide the optimal video signal.

6.6.3.3 Analog

6.6.3.3.1 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 tape. In some cases this may necessitate retrieving the original recorder.

6.6.3.3.2 Document if adjustments are done to optimize playback (i.e. reverse playback).

6.6.3.3.3 Any action or equipment that may cause damage to the original recording is inappropriate and should not be utilized. Such actions may include, but are not limited to the following: maintaining the recording in the pause mode for extended periods, unnecessarily repeated playback or placing the media in the proximity to strong magnetic fields.

6.6.3.4 Digital

6.6.3.4.1 Transfer a bit-for-bit copy to a workstation. Generate a hash to verify the transferred data per Section 1 of this manual.

6.6.3.4.2 Identify and document the proprietary file format of the recording. Obtain, download and document the required proprietary player, if necessary.

6.6.3.5 Digital Video Recorder (DVR)

6.6.3.5.1 An image of the hard drive shall be created and utilized for the analysis. If it is not possible to create an image the reason shall be documented in the notes.

6.6.4 Review the recording to locate the area of interest (AOI).

6.6.4.1 The AOI will be documented, if possible, by using the date/time stamp on the recording, the player counter information or other identifying information. In the case of a DVR, the same process will take place unless the proprietary software is file based. In this case, the proper file containing the indicated date and time will be accessed.

6.6.4.2 Capture the AOI in its original condition (raw) and save in an uncompressed or lossless file format in the electronic case folder.

6.6.4.3 If working from something other than the image, document the steps taken to acquire the AOI. Steps may include, but are not limited to the following: disengaging the overwrite function, use of cross over cables and exporting to media.

6.6.5 Conduct and document the examination process.

6.6.5.1 Steps or techniques applied to the recording/image to clarify the AOI shall be documented in the order in which they were applied to ensure the reproducibility of the results.

6.6.5.1.1 Techniques requiring documentation shall include, but are not limited to the following: brightness/contrast, color correction, cropping/resizing, noise reduction, sharpening, speed adjustment, frame averaging and video stabilization.

6.6.5.1.2 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.

6.6.6 Clarified files, video recordings and/or still images shall be saved in an uncompressed or lossless file format, in the electronic case folder.

6.6.7 Results may be presented as a chart, CD/DVD, printouts or other means that are deemed appropriate by the examiner and/or requestor.

6.7 References

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

Blitzer, Herbert L., and Jack Jacobia. Forensic Digital Imaging and Photography. San Diego: Academy Press, 2002.

Damjanovski, Vlado. CCTV Networking and Digital Technology. 2nd ed. Amsterdam: Elsevier Butterworth-Heinemann, 2005.

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

Blitzer, Herbert L., and Jack Jacobia. Forensic Digital Imaging and Photography. San Diego: Academy Press, 2002.

Inglis, Andrew F. and Arch C. Luther. Video Engineering. 2nd ed. New York: McGraw-Hill, 1996.

Kruse, Warren G., and Jay G. Heiser., Computer Forensics Incident Response Essentials. Boston: Addison-Weslye, 2002.

Madisetti, Vijay K., and Douglass B. Williams, eds. The Digital Signal Processing Handbook. N.P.: CRC Press LLC, 1998.

Solari, Stephen J., Digital Video and Audio Compression. New York; McGraw-Hill, 1997.

Utz, Peter. Today's Video. 4th ed. Jefferson, NC: McFarland and Company, Inc., 2006.

Whitaker, Jerry, and Blair Benson. Standard Handbook of Video and Television Engineering. 3rd ed. New York: McGraw-Hill, 2000.

Electronic Crime Scene Investigation a guide for First Responders. Washington, D.C. : U. S. department of Justice, 2001.

Best Practices for Seizing Electronic Evidence a Pocket Guide for First Responders. 3rded. Washington, D. C.: U. S. Department of Homeland Security, United States Secret Service.

Gill, Robert W. Basic Perspective, Thames and Hudson, London, 1974 96 pp.

7 REPORTING GUIDELINES

7.1 Introduction

Reports should seek to address case specific requests from the investigator 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 underlined italicized portion in the proposed statements serve as examples and the intent is to utilize the correct item number and/or reason for the result in the case. There is no need to further describe the item beyond the number as that information is available in the evidence lists.

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

7.2 Audio Analysis

7.2.1 Audio analysis software was utilized to analyze the recording from *Item 1*. The analysis rendered an increase in the intelligibility of the area of interest. When monitoring the results, it is suggested that headphones be utilized.

The clarified audio recording has been written to digital media and is being returned with the original submitted evidence within *Container 2*.

7.2.2 Audio analysis software was utilized to analyze the recording from *Item 1*. The area of interest was clarified; however, portions of the clarified recording remain unintelligible due to the *recording method utilized at the time the recording was produced*. When monitoring the results, it is suggested that headphones be utilized.

The clarified audio recording has been written to digital media and is being returned with the original submitted evidence within *Container 2*.

7.2.3 Audio analysis software was utilized to analyze the recording from *Item 1*. The analysis rendered limited improvement of the intelligibility of the area of interest due to the *excessive background noise*. To continue the suppression process would further degrade the intelligibility of the area of interest. When monitoring the results, it is suggested that headphones be utilized.

The clarified audio recording has been written to digital media and is being returned with the original submitted evidence within *Container 2*.

7.2.4 Audio analysis software was utilized to analyze the recording from *Item 1*. The analysis rendered limited improvement of the intelligibility of the area of interest due to the *excessive interference*. To continue the suppression process would further degrade the recording. When monitoring the results, it is suggested that headphones be utilized.

The clarified audio recording has been written to digital media and is being returned with the original submitted evidence within *Container 2*.

7.2.5 Audio analysis software was utilized to analyze the recording from *Item 1*. Due to the proprietary nature of the files, access could not be gained to the recording. Should the proprietary player be located, it is suggested the evidence and proprietary player be resubmitted for analysis.

7.3 Image Analysis

7.3.1 An image analysis was conducted utilizing image clarification software on *Item 2*. Tools and filters were applied to the area of interest rendering an improved visual appearance to the image.

The results have been written to digital media and are being returned with the original submitted evidence within *Container 2*.

7.3.2 An image analysis was conducted utilizing image clarification software on *Item 2*. The analysis did not render an improvement in the appearance of the area of interest due to *exposure and focal length*.

The results have been written to digital media and are being returned with the original submitted evidence within *Container 2*.

7.4 Comparative Analysis

7.4.1 Identification: The recovered image from *Item 2* was compared and identified to the known image of *Item 5.*

The results have been written to digital media and are being returned with the original submitted evidence within *Container 2*.

7.4.2 Inconclusive: The recovered image from *Item 2* was compared to *Item 6* and found to be similar in all class characteristics with respect to *make, model and apparent damage*. Due to *compression* in the original recording some characteristics are not visible; therefore the result of the comparison is inconclusive. It is not possible to conclude the objects as being the same or different.

The results have been written to digital media and are being returned with the original submitted evidence within *Container 2*.

7.4.3 Elimination: The recovered image from *Item 2* was compared and is not the same as *Item 7.*

The results have been written to digital media and are being returned with the original submitted evidence within *Container 2*.

7.4.4 No Comparison: The recovered image from *Item 2* lacks of sufficient detail due to *poor lighting and obscured areas* for comparison to the know object or image.

7.5 Computer Forensics Analysis

7.5.1 Forensic computer software was utilized to analyze *Item 2.* The requested files, listed below have been recovered.

Image files
E-mails containing phrases "on-line banking"
Internet History Log

The above files have been written to digital media and are being returned with the original submitted evidence within *Container 4.*

Additional data may be present on *Item 2*; however only those files requested are provided on the returned media.

7.5.2 Forensic computer software was utilized to analyze *Item 2*. No files or data related to the request were located.

7.5.3 Forensic computer software was utilized to analyze *Item 2*. Access could not be gained due to the device being password protected; therefore the files requested cannot be provided. Should the password be recovered, it is suggested that the evidence be resubmitted the item for analysis.

7.5.4 Forensic computer software was utilized to analyze *Item 2*. Due to excessive damage to the media the data requested data cannot be provided.

7.6 Mobile Device Analysis

7.6.1 Mobile device software was utilized to analyze *Item 3*. The requested files, listed below have been recovered.

Text messages
Contact list
Images

The above files have been written to digital media and are being returned with the original submitted evidence within *Container 4.* The digital media contains all files recovered from the mobile device; it is not limited to those requested due to the features of the software utilized in the analysis

As with all submitted electronic devices, it is possible that all files contained on the device have not been recovered.

7.6.2 Mobile device software was utilized to analyze *Item 3*. Access could not be gained due to the device being *password protected*; therefore the data requested can not be provided. Should the *password* be recovered, resubmitted the evidence for analysis.

7.6.3 Mobile device software was utilized to analyze *Item 3.* Due to excessive damage to the device the data requested can not be provided.

7.6.4 The below statements shall be included on all mobile device CoA when the analysis rendered results:

The dates and times associated with recovered data are dependant upon the date and time settings of the device and/or the cellular network and may not necessarily reflect the actual date and time.

Network isolation should be maintained if future reanalysis is required.

7.7 Video Analysis

7.7.1 Video analysis software was utilized to analyze *Item 4.* The analysis rendered limited improvement of the area of interest due to the *focal length, resolution and compression* in use at the time the original recording was produced. Some amount of compression is typical in digital video; however, it is possible that additional compression may have occurred when the files were written to digital media.

The clarified *still images* have been written to digital media and are being returned with the submitted original evidence in *Container 5*.

7.7.2 Video analysis software was utilized to analyze *Item 4*. The analysis rendered limited improvement of the area of interest due to the *existing lighting conditions* at the time the recording was produced.

The *clarified video recording* has been written to digital media and is being returned with the submitted original evidence in *Container 5*.

7.7.3 Video analysis software was utilized to analyze *Item 4.* The analysis did not result in improvement of the area of interest due to excessive media wear.

7.7.4 Video analysis software was utilized to analyze *Item 4*. The analysis resulted in limited improvement due to the format utilized at the time the recording was produced.

The clarified *still images* were written to digital media and are being returned with the submitted original evidence in *Container 5*.

7.7.5 Video analysis software was utilized to analyze *Item 4*. After an extensive review of the recording, the area of interest could not be located.

7.7.6 Video analysis software was utilized to analyze *Item 4*. Due to the proprietary nature of the files, access could not be gained to the recording. Should the proprietary player be located, it is suggested the evidence and proprietary player be resubmitted for analysis.

7.8 Disposition of Evidence

Document in the CoA according to Section 16 of the Quality Manual.

7.9 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 andor description of the area to be clarified. Requested items may include additional formats, proprietary viewers, additional images or recordings, or passwords.

Appendix A - Abbreviations

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

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

Admin - Administration

AOI - Area of Interest

.avi - graphics/video file format

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

CW - clockwise

DAT - Digital Audio Tape

dB - decibel

dBv - decibel (voltage reference)

DVD - Digital Video Disc

DVR - Digital Video Recorder

EP – extended play

ESN – Electronic Serial Number

EXT Data – Extended Data

Fps - frames per second

Freq - frequency

FTK - Forensic Tool Kit

GSM – Global Systems for Mobile Communications

HD - high density

HDD – Hard Drive

Hi-8 - Hi-8mm video cassette

Hz - hertz

ICCID - Integrated Circuit Card Identifier

iDEN - Integrated Digitally Enhanced Network

IMEI - International Mobile Equipment Identity

IMG - image

IMSI – International Mobile Subscriber Identity

.jpeg - graphics file format

kHz - kilohertz

Ki – 128 Bit Encryption Key

L - left

LAI – Location Area Identifier

LP - long play mode

MDN – Mobile Directory Number

MDV - mini digital video

Min(s) - minute(s)

MMS – Multimedia Message

Mono - monophonic

MSISDN – Mobile Station International Subscriber Directory Number

NTSC - National Television Standards Committee

PIN – Personal Identification Number

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

.trv - proprietary file format

SBB - sealed brown box

SBPB - sealed brown paper bag

SBX – sealed box

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

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

.tiff - graphics file format

TMSI – Temporary Mobile Subscriber Identity

VCR - Video Cassette Recorder

VHS - standard video

.wav - Microsoft Windows audio file format