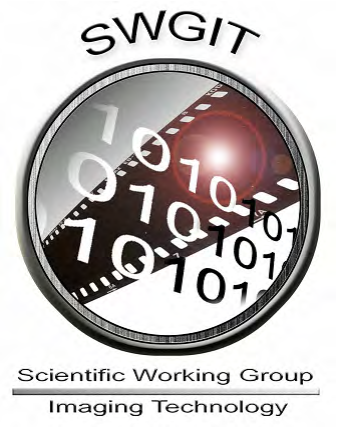
SWGIT Table of Contents



Disclaimer:

As a condition to the use of this document and the information contained herein, the SWGIT requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that SWGIT be notified as to its use and the outcome of the proceeding. Notifications should be sent to: SWGIT@yahoogroups.com

Redistribution Policy:

SWGIT grants permission for redistribution and use of all publicly posted documents created by SWGIT, provided that the following conditions are met:

1. Redistributions of documents, or parts of documents, must retain the SWGIT cover page containing the disclaimer.

2. Neither the name of SWGIT, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

Section 1

Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System

*** Released previously as "Guidelines for the Use of Imaging Technologies in the Criminal Justice System* and *"Definitions and Guidelines for the Use of Imaging Technologies in the Criminal Justice System" ***

1. Introduction

Although digital imaging technologies have been used in a variety of scientific fields for decades, their application in the criminal justice system is more recent. Consequently, there has been a need to gather and disseminate accurate information regarding the proper application of this and other imaging technologies (including silver-based film and video) in the criminal justice system.

1.1 Mission Statement

The mission of the Scientific Working Group on Imaging Technology (SWGIT) is to facilitate the integration of imaging technologies and systems within the criminal justice system (CJS) by providing definitions and recommendations for the capture, storage, processing, analysis, transmission, and output of images.

1.2 SWGIT Membership

The Technical Working Group on Imaging Technology was formed by the Federal Bureau of Investigation in December of 1997. In 1999, the name of the group was changed to the Scientific Working Group on Imaging Technology (SWGIT). From the beginning the group has been comprised of individuals from federal, state, and local law enforcement agencies, the American military, academia, foreign law enforcement agencies, and other researchers. Those selected for membership in the group are experienced professionals working in the field of imaging technology or a related field and demonstrate the willingness to participate by consulting on the release of best practices and guidelines for the use of imaging technology in the Criminal Justice System. All SWGIT documents represent the consensus opinion of this membership and should not be construed as the official policy of any of the represented agencies.

1.3 Purpose of this Document

This document will familiarize the reader with important considerations in the capture, preservation, processing, and handling of images, whether the images are in digital, analog, or film format. This document will also refer the reader to other SWGIT documents for more complete details and guidelines.

1.4 Admissibility of Digital Images

Digital imaging is an accepted practice in forensic science, law enforcement, and the courts. Relevant, properly authenticated digital images that accurately portray a scene or object are admissible in court. Digital images that have been enhanced are admissible when the enhancement can be explained by qualified personnel.

1.5 Other SWGIT Documents

A complete list of documents that have been published by the SWGIT is attached.

2. Image Capture

"Capture" is the process of recording data such as an image or video sequence. The taking of photographs with a digital, film, or video camera is an example of capture. Digitizing images, documents, or objects with a scanner is another example of capture. When images are captured by those law enforcement or forensic laboratory personnel who are charged with the responsibility for processing or analyzing images, it is possible to control the equipment, methods, and techniques used. This may not be possible when images are captured by others and are submitted for processing or analysis. The handling of this evidence differs dependent on the source.

2.1 Image Capture Equipment

Image capture devices should be capable of rendering an accurate representation of the item or items of interest. Different applications will dictate different standards of accuracy. At a minimum, the following should be considered when selecting appropriate devices:

- Resolution requirements which are in turn driven by the intended use of the image (first responder, crime scene work, preserve impressions, etc.)
- Characteristics (size, movement, location, etc.) of the scene, item, or items of interest
- Lighting of the items of interest
- Dynamic range of the scene
- Time constraints
- Required end product(s)

Specific information and additional SWGIT recommendations relating to different law enforcement field applications may be found in the SWGIT document "*Field Photography Equipment and Supporting Infrastructure."*

2.2 Image Compression

Compression is the process of reducing a digital file's size. Compression may be lossy or lossless. The decision to use lossy or lossless compression will be dictated by the intended use of the image. When lossy compression is used, critical image information can be lost and unwanted artifacts introduced as a result. Repeatedly saving a file using lossy compression may exacerbate the loss of image information. Therefore, if an image is to be subjected to scientific analysis and compression is necessary, lossless compression is strongly recommended. Likewise, due to the fact that the end use of an image cannot always be predicted, it is recommended that original images be recorded using no compression or lossless compression. If lossy compression must be used,

then the lowest level of compression should be used.

Specific information and additional SWGIT recommendations relating to image compression may be found in the following SWGIT documents: "*Issues Relating to Digital Image Compression and File Formats*", "*Guidelines for Image Processing*", *"General Guidelines for Capturing Latent Impressions Using a Digital Camera", "General Guidelines for Photographing Tire Impressions", and "General Guidelines for Photographing Footwear Impressions".*

3. Image Integrity

A legal prerequisite to the admissibility of any evidence is that the evidence being offered in court can be authenticated. An exhibit is authenticated when there is sufficient evidence that the exhibit is what the proponent claims it to be. In the case of images the authentication requirement is usually satisfied when a witness can testify that the image accurately portrays the scene or objects that were captured. If authenticity is challenged, the proponent must be prepared to show that the image (or data) has not been altered.

In the case of images processed using advanced enhancement techniques, qualified witnesses must be able to testify concerning the process used.

3.1 Identifying and Handling the Original Image

A primary image refers to the first instance in which an image is recorded onto any media that is a separate identifiable object. An original image is an accurate and complete replica of the primary image, irrespective of media. See the SWGDE/SWGIT document "*SWGDE and SWGIT Digital & Multimedia Evidence Glossary*".

3.2 Preserving Original Images

The original image should be stored and maintained in an unaltered state. This includes maintaining original digital images in their native file format. To preserve the original image when processing is required SWGIT recommends:

- Film-based media originals may be processed if the processing is non-destructive.
- With analog video, minimal playback of the original is recommended to avoid degradation of signal.
- Original digital images should not be altered. Processing should be performed on working images only.

3.3 Archiving

Care must be taken to ensure that archival media is maintained in such a manner that the information contained thereon may be retrieved in the future (within statutory and agency guidelines).

Specific information and additional SWGIT recommendations relating to archiving may be found in the SWGIT document *"Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System"*.

4. Image Processing and Analysis

Image processing is any activity that transforms an input image to an output image. Image analysis, on the other hand, involves the application of image science and domain expertise to examine and interpret the content of an image and/or the image itself in legal matters.

Specific information and additional SWGIT recommendations relating to image processing and analysis may be found in the SWGIT documents "Guidelines for Image Processing" and "*Best Practices for Forensic Image Analysis*".

4.1 Documenting Image Enhancement

The intended use of the image dictates the level to which the enhancements are documented. Any processed image subjected to image analysis should be documented with an image processing log. An image not subjected to image analysis does not need an image processing log.

Specific information and additional SWGIT recommendations relating to image enhancement may be found in the SWGIT document "*Best Practices for Documenting Image Enhancement*".

4.2 Software

Software used in processing and analyzing digital images should produce consistent results, permitting comparably trained personnel to achieve comparable analytical results.

LEGAL NOTE: Manufacturers of software used for image processing may be required to make the software source code available to litigants, subject to an appropriate protective order designed to protect the manufacturer's proprietary interests. Failure on the part of the manufacturer to provide this information to litigants could result in the exclusion of imaging evidence in court proceedings. This should be considered when selecting software.

5. Outputting Images

An output device should be capable of producing an accurate representation of the input image. The following should be considered in the selection of output devices:

- Final use of image
- Time constraints
- Longevity/permanence of output image
- Spatial resolution required
- Range of colors and brightness to be produced

6. Distributing Images

Received images should accurately reflect the distributed images. The following should be considered in the selection of distribution methods and transmission devices:

- Final use of image
- Time constraints
- File size
- Security of transmission
- Integrity of transmission
- Hardware and software compatibility of transmitters and receivers
- File format compatibility

7. Quality Assurance

Personnel utilizing images and imaging technology in the criminal justice system should implement quality assurance programs to ensure that results achieved are repeatable and valid. As part of these programs, performance checks and corrective actions should be documented.

7.1 Equipment

Where applicable, equipment utilized in imaging should be checked regularly for proper performance and calibration, and findings documented. Where applicable, an end-to-end system check for consistency within specified system parameters should be performed on a regular basis and whenever modifications are made to the system. All equipment should be maintained according to the manufacturers' specifications and recommendations as contained in the operating manuals.

When a piece of equipment or a system falls outside the specifications and recommendations, the equipment or system should be taken out of service until it has been corrected. Evaluation of equipment and system checks should be documented to include corrective actions.

7.2 Software

If software errors that significantly affect the results of a processing step are detected, then corrective actions should be taken. If the manufacturer identifies software errors and provides corrective remedies for them, the remedies should be implemented before the software is used again. Once corrective actions have been taken, an end-to-end system check should be performed prior to putting the system back into operation.

7.3 Personnel and Training

All personnel utilizing imaging technologies shall be trained and competent in the operation of the relevant imaging technologies.

Issues relating to personnel and training in imaging technology are addressed in the SWGIT documents, "*Guidelines and Recommendations for Training in Imaging Technology in the Criminal Justice System*", "*SWGDE/SWGIT Guidelines and Recommendations for Training in Digital and Multimedia Evidence*" and "*SWGDE/SWGIT Proficiency Test Program Guidelines*".

7.4 Standard Operation Procedures (SOPs)

Personnel engaged in the capture, storage, processing, analysis, transmission, or output of imagery in the criminal justice system should ensure that their use of images and imaging technology are governed by documented policies and procedures.

For issues relating to SOPs see SWGDE/SWGIT "*Recommended Guidelines for Developing Standard Operating Procedures*".

Section 2

Staying Current in Digital Imaging Technologies: Considerations for Managers

Previously released as "*Considerations For Managers Migrating to Digital Imaging Technology*"

Introduction

Advances in digital imaging technologies often lead to changes in work processes and training requirements. Whether migrating from film or upgrading existing digital imaging technologies, these changes should be done only after examining current operating procedures and completing a needs assessment. This should involve the participation of the organization's imaging and/or subject matter experts.

Needs Assessment[1]

- Prior to selecting any digital imaging technology, current practices should be examined to determine if there is a need to replace or enhance existing technology.

- The ability to make use of archived images (e.g., negatives, media, file formats) needs to be considered.

Cost Analysis[1,2,3]

- Prior to selecting an imaging system, a cost-benefit analysis should be conducted to determine the cost justification of a system purchase and to determine the possible advantages and disadvantages to the agency with its implementation.

- This analysis would allow a financial comparison between the current and proposed imaging systems to make a procurement decision.

- The analysis must consider every relevant step of the imaging chain: acquisition/capture; transmission; storage; processing; archiving and retrieval.

- To determine a cost estimate, the following components for each step of the imaging chain should be considered: hardware; software; maintenance; security; training; facilities upgrades; site preparation; staffing and consumables.

- Managers should be aware of the recurring costs associated with maintaining and upgrading imaging systems. Unless these costs are factored into the budget, the system is in danger of becoming obsolete. Some agencies annually budget approximately 15 percent of the original system acquisition cost for upgrades, training, and maintenance.

Image Quality and Storage[1,4,5,9]

- When determining resolution requirements, the intended usage and data storage requirements should be considered.

- The selection of a storage media may depend on file size, the number of files, the length of time the files are to be retained, the storage media, the archiving system, and the integration with existing systems.

- Image compression can affect image quality and should be considered carefully.

Equipment Evaluation

- Information used to evaluate suitability of new imaging technology should include feedback from agencies currently using the equipment in similar applications, product reviews, and vendor specification sheets.

- Prior to making a final selection, request a demonstration of new imaging technologies using representative samples of casework and do not rely solely upon prepackaged demonstrations.

Standard Operating Procedures (SOPs) and Training

- SOPs must be developed to ensure consistency, quality, integrity, and repeatability of the process.

- Staff should be trained to competency in photography, all imaging equipment, hardware, software, and processes to include SOPs.

- Continuing training in imaging technology and processing is required.

Legal Considerations[8]

- Review of SOPs by departmental counsel may be helpful.

- Personnel should be familiar with how the rules of evidence apply with respect to the admissibility of evidence and expert testimony.

- Case law supports the admissibility of digital images on the same principles as film-based images. For details, in your jurisdiction, consult with your local legal council

[1] *See SWGIT Guidelines for Field Applications of Imaging Technologies in the Criminal Justice System*
[2] *See SWGIT Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System*
[3] See SWGDE/SWGIT *Proficiency Test Program Guidelines*
[4] See SWGIT Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System
[5] *See SWGIT Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System*
[6] See SWGDE/SWGIT *Recommended Guidelines for Developing Standard Operating Procedures*
[7] See SWGDE/SWGIT *Guidelines & Recommendations for Training in Digital & Multimedia Evidence*
[8] *See SWGIT Digital Imaging Technology Issues for the Courts*
[9] *See SWGIT Issues Relating to Digital Image Compression and File Format*

Section 3

Field Photography Equipment and Supporting Infrastructure

** Previously called "*Guidelines for Field Applications of Imaging Technologies in the Criminal Justice System*" **

Introduction

The purpose of this document is to provide guidance and recommendations for equipment, infrastructure, training, Standard Operating Procedure (SOP) development and security and integrity issues for photography in the field environment.
This document addresses the photographic documentation of events or subjects that are not in a forensic laboratory or studio, or other controlled environment.

General Equipment Considerations

Equipment needs depend on the tasks performed and the intended use of the image. Agencies should identify specific requirements for resolution, color fidelity, exposure capability, dynamic range, durability, file formats, and storage. For example, Crime Scene Technicians should use a camera that is capable of manual override and has interchangeable lenses, off-camera flash, cable release, and a tripod mount. On the other hand, a good quality point-and-shoot camera may be sufficient for first responders. Cellular telephone and other personal electronic devices with integrated cameras should not be used unless their use is an operational necessity.

Digital cameras are widely used and images produced by them are accepted in the Criminal Justice System. Advances in imaging technology have allowed the images from digital cameras to be comparable to traditional film-based imaging. One study of footwear impression photography found no difference between the images from 35 mm film and 6 megapixel digital cameras and greater. (Blitzer, H. Effect of Photographic Technology on Quality of Examination of Footwear Impressions. *Journal of Forensic Identification, 2007; 57(5);*641-657)

The agency should have a specific mechanism for determining whether a piece of hardware meets a requirement. Some applications, such as impression evidence, have specific quantitative requirements regarding equipment or resolution (see SWGIT documents "*General Guidelines for Capturing Latent Impressions Using a Digital Camera*", "*General Guidelines for Photographing Tire Impressions*" and "*General Guidelines for Photographing Footwear Impressions*". Specification sheets may be used as a guide, but in most cases it will be necessary to test the equipment under operational conditions.

Equipment acquisition and SOPs should ensure that field personnel are provided with adequate consumables (e.g., batteries, removable storage media) and accessories (e.g., flash, tripods, cable release). In addition, adequate physical storage and protection of equipment and media is necessary to maintain operations.

Infrastructure

Infrastructure refers to both hardware and software necessary to store, secure, process, transmit and output data. Creating and maintaining a sound infrastructure requires developing a needs assessment, and validating, verifying, maintaining and upgrading the systems. Inadequate infrastructure will undermine the ability to secure and efficiently utilize the images.

- *Needs assessment*

  An agency should perform a needs assessment to determine what infrastructure is necessary for its specific tasks and should demonstrate how it plans to fulfill those obligations. This assessment should identify what tasks are to be performed, under what circumstances those tasks will be performed, and the end use of the imagery. Specific hardware, software, and training requirements can be targeted to each one of those tasks, circumstances, and end uses.

  Important aspects to consider are data transmission and output. Transmission includes the electronic transfer of the images from temporary storage media to permanent storage and movement across networks. The amount of data transmitted will determine the requirements for network bandwidth and storage capacity. Output of images refers to display devices, printers, and/or optical media. The end use of an image determines the appropriate output method. For example, the hardware requirements will differ significantly between images that are to be analyzed on an 8 x 10" print versus those that will be viewed with a projector or monitor.

- *Validation and Verification*

  Validation is a necessary part of infrastructure design and usage. The degree and type of validation should be reasonably targeted to the context within which the assets will be used; it is not necessary to validate functions or capabilities that will not be used. Verification that assets are functioning appropriately (sometimes called quality-control tests) should be an integral part of any SOP. The frequency and degree of verification may be application and agency-specific.

- *Maintenance*

  Agencies should plan for and adopt strategies and responsibilities for preventive maintenance, repair, and inspection of hardware and software to maintain optimum performance and to prevent catastrophic failure.

- *Lifecycle*

  Infrastructure assets, particularly in a high-technology area such as imaging, are subject to wear, tear and obsolescence. Equipment used will be subject to physical stress and will eventually require repair or replacement. Other assets, such as rechargeable batteries, have a finite lifespan. Technology advances quickly, and newer, less expensive hardware/software may provide better results at a lower operational cost. New technologies may allow expansion of service opportunities or provide capabilities that were previously not available. Agencies

should periodically assess their needs and determine if new technologies or upgrades are warranted.

Training

A training program is essential for successful image acquisition, processing and output of digital images. Training programs should be designed and implemented to provide the skills and knowledge required to successfully perform at an appropriate level of responsibility. See SWGIT document Section 6 "*Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System*."

SOP Development

SOPs are agency-specific and are important to provide structure and guidance, and to ensure consistency. See the SWGIT/SWGDE document "*Recommended Guideline for Developing Standard Operating Procedures*."

Security and Integrity

Integrity ensures that the digital images are complete and unaltered from the time of acquisition through its final disposition. Security is imperative to maintain integrity, which includes protection of portable data storage devices, computer facilities, and data stored and/or transmitted on computer systems. It involves the use of management, personnel, and operational and technical controls. Refer to SWGIT Document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*."

Categories of Field Photography

Field photography generally falls into two different categories depending on the extent of documentation required. Each category will require different levels of training, knowledge, experience, and equipment.

- General photography
    - Requires basic knowledge of camera operation and photographic composition
    - May involve the use of a point-and-shoot camera
    - Utilized for documentation purposes
    - Advanced photography
    - Requires knowledge of manual exposure control, flash photography and other lighting controls, alternative light sources, use of tripods and remote shutter releases, filters
    - Requires the use of a SLR camera with interchangeable lenses and off-camera flash capabilities
    - Utilized for documentation and potential analysis, such as with latent fingerprints and other impression evidence
    - Images that will undergo analysis should be captured at the highest available resolution with no or lossless compression

In addition to general or advanced photographic knowledge, there are specialized applications that require additional training based upon specific needs, such as with aerial, surveillance, arson or hazardous materials (HAZMAT) photography.

Example of General Photography - First Responder

First responders are frequently called upon to document conditions they find at an incident where a crime scene photography unit or specialist may not be requested or available. Examples may include: domestic violence incidents, traffic accidents, minor property crimes, and other incidents as defined by agency-specific policies. Photography may not be the first responder's primary responsibility, and they may have general photography training. The first responder must be cognizant that the images captured may contain important information that was not recognized at the time the photograph was taken.

Equipment for First Responder Photography:

- A non-disposable camera with flash and close-up capability. The suggested minimum resolution for a digital camera is 6 megapixels and it should utilize removable storage media. The minimum requirement for a film camera is 35 mm.
- Other standard photographic equipment, such as off-camera flash or scales, can be utilized as necessary.
- Videography, when used, should be in a supplementary capacity.

Agencies should designate what first responders should photograph and what circumstances would prompt a request for individuals with advanced photographic training.

Example of Advanced Photography - Crime Scene Photography

Crime scene photography is directed towards documenting evidence and other details of a crime scene in a fair and accurate manner. Crime scene photography generally requires advanced photography with the ability to:

- Accurately represent the details and colors in a scene
- Capture overall, intermediate, close-up, and examination images with accurate spatial relationships
- Deal with varying lighting and physical conditions
- Record information that crime scene personnel may not have known was important at the time the images were captured

Crime scene photography is usually a time-sensitive activity with only one opportunity to correctly complete the task. Depending on the nature of the crime or incident, conditions at a crime scene may dictate the selection and use of a variety of equipment and techniques.

Equipment for Crime Scene Photography:

- A Single Lens Reflex (SLR) camera that is capable of manual override, with interchangeable lenses, off-camera flash, remote shutter release, and a tripod mount.

- Digital cameras should have at least 6 megapixels, and should be set to either uncompressed or lowest compression (highest quality format or fewest numbers of pictures per media card).
- The minimum requirement for a film camera is 35mm.

- Other standard equipment may include:
  - External battery packs
  - Sturdy tripod
  - Extra media
  - Gray card and/or color checker
  - Various types of known scales
  - Various types of filters
  - External flashes and cords
  - Remote shutter release
  - Light meter
  - Various types of lenses (macro, normal, wide-angle, telephoto)

- Videography, when used, should be in a supplementary capacity

Example of Photography Utilizing Special Applications - Surveillance Photography

Surveillance photography documents events and individuals engaged in acts as they occur. Surveillance activities may involve highly specialized techniques and equipment that require technical training and knowledge and are best accomplished by trained specialists.

Equipment for Surveillance Photography:

- A Single Lens Reflex (SLR) camera that is capable of manual override, with interchangeable lenses, remote shutter release, and a tripod mount.
  - Digital cameras should have at least 6 megapixels, a high sensitivity sensor, and should be set to either uncompressed or lowest compression (highest quality format or fewest numbers of pictures per media card).
  - The minimum requirement for a film camera is 35mm.
  - The ability to disable the flash, display screen, and infrared auto-focus transmitter as well as any other features that would compromise operational security. In covert surveillance situations, illumination of the photographer by the LCD screen may compromise safety.

- Other photographic equipment depending on operational necessity.

- Specialized equipment, which may include night vision or thermal imaging equipment.

- Videography can be used as the primary method or in a supplementary capacity.

The successful capture of images sufficient for identification of depicted individuals and/or objects (e.g., license plates) will require close attention to the selection and appropriate use of equipment.

Section 4

Recommendations and Guidelines for Using Closed-Circuit Television Security Systems in Commercial Institutions

1. Purpose

The purpose of this document is to provide recommendations and guidelines for the use of closed-circuit television (CCTV) security systems in commercial institutions, such as banks, convenience stores and other facilities. For the purpose of this document, fixed-site cameras and recording devices will be discussed. The basic principles and recommendations can, in most cases, be applied to any system using CCTV cameras and video recorders. This document addresses analog and digital video systems. The intent of these recommendations and guidelines is to optimize image quality to facilitate the identification of unknown people and objects depicted therein.

This document does not specifically address employee theft or other internal security issues, although some of the recommendations can be applied to those problems. Likewise, this document does not address live monitored surveillance systems. References that address such systems are included in Appendix A, CCTV References.

Furthermore, these guidelines are not intended to replace or take precedence over other regulatory requirements in the specific jurisdiction of the facility to which these guidelines will be applied.

2. Position

The use of closed-circuit television systems and the recording of security images is an accepted practice in commercial institutions, such as banks, convenience stores, and other facilities. This practice can contribute to the investigation of criminal activity. It is the position of the Scientific Working Group on Imaging Technology (SWGIT) that in order to optimize the use of these systems, the following criteria should be met:

- Recordings must be preserved in a manner that permits law enforcement officials to recover the original images with a documented chain of custody.
- The number, placement, and type of cameras should be sufficient to provide adequate coverage and detail in the monitored area.
- There should be adequate, balanced lighting in the monitored area.
- Institutions should establish and follow a program of regular system maintenance.
- Institutions should have documented procedures to ensure that employees know what to do in the event of a criminal incident.

3. Introduction

A CCTV security system may include a single camera or multiple cameras. Coverage can include checkout areas, walk-up or drive-up automated teller machines, public-service areas, entrance or exit doors, work areas, interior corridors or common building hallways, and exterior or interior parking areas.

A CCTV system may include cameras, a monitor to view the camera images, a recording device to capture selected images, and software or a switching system to control the method of selecting and storing images. Depending on the location and situation, CCTV systems may use an analog videocassette recorder (VCR) or a digital video recorder (DVR) to record images from the cameras. DVRs may either be computer based or a stand-alone embedded system. Finally, a means of retrieving and storing images must be incorporated into the system.

This document addresses CCTV systems in the following four areas:

- Functional Requirements (Section 4)
- System Design (Section 5)
- System Maintenance (Section 6)
- Evidence Handling (Section 7)

4. Functional Requirements

The purpose of these requirements is to increase the likelihood that images recovered from CCTV systems are sufficient to enable law enforcement officials to identify the people and objects of interest depicted therein.

In order to identify a person, specific individual features, such as the detailed shape of the eyes, ears, nose, mouth, and chin, must be distinguishable. Identification is facilitated if the ability to distinguish smaller features such as moles, scars, tattoos, and freckle patterns, as well as the ability to derive measurements of these features, is possible. Likewise, identifying a vehicle requires that the license plate numbers or other identifying characteristics be distinguished.

In **Figure 1**, the images on the left are more likely to allow for personal identification than the images on the right. The lower part of the figure shows the head of the subject from each image after it has been enhanced.

Figure 1(a). A CCTV image likely to be suitable for personal identification.

Figure 1(b). A CCTV image not likely to be suitable for personal identification.

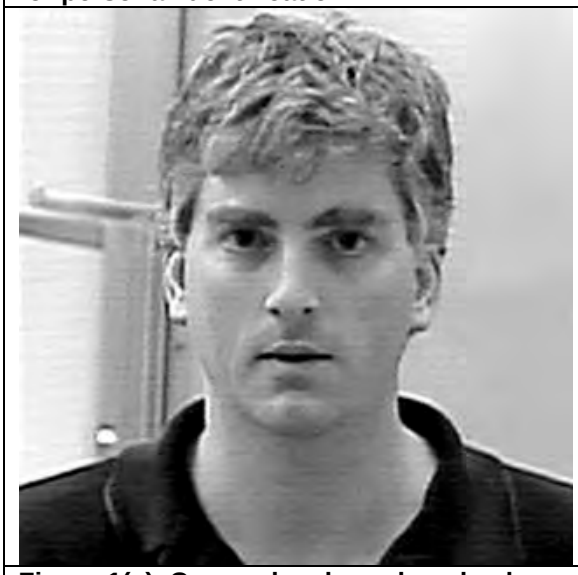


Figure 1(c). Cropped, enlarged, and enhanced image processed from Figure 1(a).

Figure 1(d). Cropped, enlarged, and enhanced image processed from Figure 1(b).

5. System Design

The ability of a CCTV system to record images that will be of greatest assistance to law enforcement depends on multiple factors including the choice and placement of cameras and lenses, recorders, storage space, compression schemes and data transmission. These factors are dependent on one another and must be coordinated. As an example, adding cameras to an existing system may require adjustments to the amount of storage or the rate at which images from each camera are recorded.

A careful survey of the facility in which the system will be installed must be completed and analyzed as an integral part of the total design process. A site plan documenting the location and field-of-view of each camera in the facility should be included as a part of this survey. Finally, upon installation, the system must be tested to confirm that images produced by the system as output (e.g., those that would be provided to law enforcement in the event of a criminal investigation) are of sufficient quality to maximize the likelihood of identifying people or objects depicted therein.

5.1. Components

CCTV systems should include the following components, at a minimum: a camera or cameras, moveable and/or fixed; a recording device, including the means by which the recording may be extracted from the device; and a monitor. Consideration should also be given to any need for recording audio with the video from one or more cameras and any legal problems unique to audio recording. Guidelines for devices are addressed in the following subsections.

5.2. Cameras

Cameras used in CCTV systems should adhere to the following recommendations:

5.2.1. Number and Placement

The number of cameras needed for an institution will vary depending on a variety of factors, including the specific security needs of the institution and the monitored area(s). Care should also be exercised to ensure that cameras are not located in places where they may be subject to tampering or accidental adjustments. Camera disabling and tampering can be minimized by using components that feature concealed wiring and protection of the camera and lens assembly from weather and/or physical damage.

The cameras' fields-of-view should not be obstructed, nor should cameras be pointed directly at bright light sources, such as picture windows or spot lights. If bright areas cannot be avoided in a scene, cameras with backlight illumination or compensation adjustments are preferred to optimize the resulting image.

As a minimum, there must be at least one camera for every exit. Exit cameras should be aimed toward the interior of the facility, and each one should be located where it can obtain an unobstructed frontal view of the head and shoulders of everyone exiting the facility. The lenses on exit cameras should be configured to have a depth-of-field that extends from three feet to at least ten feet from the camera in order to provide images of exiting people which are in focus. Exit cameras that have a depth-of-field extending from three feet to beyond ten feet will have the added benefit of providing overviews of the interior and head-to-foot views of people as they enter and exit the facility.

Cameras should be placed where they can record images with unobstructed views at each point of customer transactions, such as teller windows (walk-up and drive-through), cash registers, automated teller machines, or customer-service stations. There must be at least one camera at each point-of-customer transaction. Cameras should be adjusted to ensure that they are in focus at the location where a customer can be expected to stand. If a window or other security barrier is present, care must be taken to position the camera in a manner that minimizes reflection, glare, and other obstructions that can interfere with a clear view of the persons or objects being recorded.

Figure 1(a) illustrates a head and shoulders image that is preferable for the exit and transaction cameras. The camera lenses needed to achieve the fields-of-view are discussed in Section 5.2.6.

Cameras that provide overviews of the interior and exterior portions of a facility can be useful in an investigation but cannot be relied on to provide images suitable for identification purposes. Therefore, in these guidelines they are considered to be of reduced importance. However, if the combination of the exit and customer transaction cameras do not provide complete coverage of the interior of the facility, then it is recommended that additional cameras be included for this purpose.

Exterior cameras intended to record images of vehicles should be placed to provide direct views of the vehicle so that the license plate is clearly visible and legible. Additional exterior cameras covering wider fields of view can provide additional vehicle information.

Moveable dome and pan/tilt cameras can be used to provide additional coverage through automatic alarm presetting and parking. Motion detection or door contact alarms can automatically initiate a camera preset providing a high-resolution view of the alarmed scene. This provides unmanned, additional target coverage. After a predetermined time, the camera can return to a preset parked position or to a scanning pattern to cover site locations not viewed by the fixed devices.

If the system contains a matrix switch with a joystick controller, a guard or observer can manually track a suspect giving a tightly zoomed, high-resolution image of the suspect. Variable speed control and automatic focus are recommended to facilitate smooth target tracking. When in the parked position, the unit can serve as an additional fixed camera.

Finally in some instances, commercial institutions may find it useful to include monitored cameras as part of their overall security strategy. The video or images from such cameras are not intended to be recorded, but provide employees with a means to view areas in a facility that would otherwise be out of employees' sight. However, in the event the video or images from these cameras are not recorded, the potential exists for the loss of valuable evidence.

5.2.2. Lighting

Poor lighting is the most common factor that degrades the quality of video images. Adequate, balanced lighting should be provided in areas viewed by the cameras. Particular care must be taken to ensure that the dynamic range present in a scene does not exceed the capability of the camera.

Strong backlighting or high-contrast lighting may cause the face of a subject to be obscured in shadow, making identification of a suspect from the image difficult or impossible. Likewise, spotlights can create both shadows and highlights on faces, making it difficult to determine if observed tonal variations represent actual features, such as facial hair, or are merely a product of the lighting. The use of non-infrared, high-dynamic range cameras and those capable of operating in low light conditions should be considered to help improve the image quality.

As an example, ceiling-mounted fluorescent lighting that is well distributed throughout interior spaces would be preferred to the use of track-mounted spotlights.

Finally, different light sources have different color temperatures that will affect the apparent color of objects in a scene. Tungsten lamps impart a reddish tint to objects in a scene, whereas fluorescent bulbs can impart a greenish tint. Likewise, sodium lamps can make objects appear more yellow than they actually are. Most color video cameras can be adjusted to compensate for this, and many perform this function automatically.

A color video camera is considered balanced for a particular reference white when a neutral white card is placed in the camera's field-of-view under normal illumination conditions and the red, green, and blue channels provide equal output levels. Therefore, interior color cameras should be balanced for white on installation and rebalanced if the type of lighting used is changed. However, because many commercial institutions will operate under conditions in which lighting is variable, white balance may not be possible at all times.

Infrared lighting can be used to provide improved low light performance for monochrome cameras. Infrared lighting is not supported by standard color cameras as they filter out the infrared spectrum. If an infrared sensitive video camera is used, law enforcement officers should be made aware of this because an infrared sensitive video camera often reproduces clothing that appears to be dramatically differently when compared to images of the same clothing that were recorded with a video camera that is not sensitive to infrared.

A more complete set of technical guidelines for lighting is provided in Appendix B.

5.2.3. Black-and-White Versus Color

Although some black and white video cameras may provide better image quality than color cameras, the information available in color images may provide important investigative information. Therefore, the choice of cameras is left to the commercial institution, depending on the intended use of the recorded images.

5.2.4. Resolution

In order to meet the SWGIT guidelines, analog video cameras must have an output resolution of at least 400 horizontal lines. Digital video cameras must have an output resolution of at least 640 pixels in the horizontal direction and 480 pixels in the vertical direction. The recording resolution of the CCTV system should match the resolution of the cameras. Cameras that have higher resolutions are strongly recommended.

5.2.5. Infrared Characteristics

The detectors used in black and white video cameras may be sensitive to a part of the infrared spectrum that is outside of the normal range of human visual perception. This can improve the ability of the camera to record in situations in which there are low levels of visible light.

Objects in images acquired by infrared-sensitive cameras may not accurately depicted with regards to tone (e.g. a light object may appear darker, or dark object may appear light). Many cameras are equipped with filters that can mitigate this effect.

The use of infrared-sensitive cameras should be noted in the system documentation (see Section 6.1).

5.2.6. Lens, Focal Length, and Field of View

The selection of lenses will be dictated by the field of view to be covered by each camera, as well as by the size of the camera's detector.

For cameras placed to record images at a point of customer transactions, such as a teller window , the area of interest (e.g., face, license plate) should cover approximately 15 percent or more of the camera's field of view (based on the recommended minimum resolution found in Section 5.2.4). For an average human head that is six inches wide, a three foot wide field of view will meet this guideline. For a license plate width of approximately 12 inches, a six foot wide field of view is sufficient.

The focal length necessary to achieve an approximately three foot wide field of view for a given detector size and camera to subject distance is provided in Table 3. The camera must be in focus at the position of this subject.

Table 3. Approximate Focal Length (in mm) Needed for Three-Foot-Wide Field-of-View

	Distance to subject (in feet)	2’	5’	10’	15’	20’	30’
Detector size (inches)	1/4”	2.3	5.9	11.7	17.6	23.5	35.2
	1/3”	3.1	7.8	15.7	23.5	31.3	47.0
	1/2”	4.0	10.1	20.2	30.3	40.4	60.7

(Differences in the units used to describe these resolution recommendations are due to the differences in the industry standards used to describe these media.)

Cameras that provide overviews of interior and exterior locations should have their focal lengths selected so as to meet the field of view requirements of the facility. However, entrance/exit cameras should have sufficient depth of field to be in focus at distances of three feet and beyond to ensure that subjects entering/exiting the facility will be in focus. To gain depth of field, additional lighting to the area of interest should be provided.

5.2.7. Exposure Control

Cameras should be equipped with automatic mechanisms to ensure proper exposure under varying lighting conditions. Such mechanisms include, but are not limited to, automatic gain circuitry, day/night sensor switching, and lenses with automatic iris functions.

5.2.8. Camera Housings

Cameras may require coverings and environmental controls to protect them from the elements or tampering. Clear coverings placed in front of camera lenses will reduce image quality; therefore, unless there are specific environmental or security concerns that require camera housings, it is recommended that they not be used.

5.3. Electrical Power

CCTV systems must be provided with adequate power. Backup power sources and surge protection should be included in the system design to ensure that recordings are preserved in the event of a power loss. Systems that require electrical power to preserve their recordings should have backup power sources sufficient to last for at least 30 minutes, until either the system power is restored or the system is shut down in a manner that preserves the recording. DVRs should also automatically restart in a preprogrammed operation mode on power up from the extended power outages.

NOTE: Abrupt power loss could result in the corruption/loss of the file system and /or video data.

When a VCR or DVR with automatic restart is used, there must be an on/off switch. This is to ensure that no data is lost following an incident that led to the recorder being purposely turned off to preserve the recording of the event.

CCTV systems should be placed on isolated circuits that are properly grounded to reduce interference and signal degradation. If the system is on a long power run, outdoors, or in an area prone to electrical storms, special protection devices to control power surges and nearby lighting strikes are strongly recommended.

5.4. Bandwidth

The bandwidth provided for transmitting the video signal must be compatible with, and sufficient to meet, the resolution requirements listed below for the system's recording device. Although bandwidth minimum standards do not guarantee acceptable video image quality, they do play an important part. To improve the likelihood of acceptable image acquisition, video cameras should have a signal bandwidth of at least 7MHz.

Bandwidth in digital CCTV systems also refers to the throughput capability of the network on which the system resides. The requirements for the network are dependent upon the number of cameras, resolution, and frame rate of the system, as well as other demands being placed o the network (e.g. non CCTV traffic). Requirements for the network will vary depending on whether video is being recorded over the network, or transferred after being recorded locally.

5.5. Signal – to – Noise Ratio

One major problem with picture clarity is noise. Electronic noise is present to some extent in all video signals. Noise manifests itself as artifacts with in images, such as "snow" or graininess. There are several sources of noise: poor circuit design, heat, over amplification, external influences, automatic gain control, and transmission systems. Some video signal noise cannot be overcome in a reasonable manner. However, to improve the likelihood of acceptable image acquisition, video cameras should have a signal to noise ratio of at least 48dB. Further, the line loss between each camera and the multiplexer or recorder that the camera is connected to shall not cause the signal to fall below 45dB.

5.6. Recording System

Recording systems used in CCTV systems should adhere to the following minimum standards.

5.6.1. Recorder Security

Steps must be taken to ensure the physical security and integrity of the system's recording device. Placement of the recording device in a restricted access location, such as a locked cabinet or room, is strongly recommended. Note that proper environmental controls must be implemented according to the manufacturer's specifications. For example, recorders require adequate airflow to prevent overheating.

Policies should be in place to ensure that law enforcement can gain immediate access to the recorded images when necessary.

5.6.2. Recording Resolution for Analog Recording Systems

Analog videocassette recorders must record each image at a minimum line resolution of 240 visible lines. This resolution is typical of most VHS videocassette recorders. The use of videocassette recorders with higher line resolutions (e.g., S-VHS videocassette recorders and tapes) is strongly encouraged because this improves image quality. Analog systems meeting these minimum requirements are still suitable for use, however, their availability and use has declined.

5.6.3. Recording Resolution for Digital Video Recorders

It is strongly recommended that digital video recorders using digital media for storage record each frame at a minimum resolution of 640 pixels in the horizontal direction and 480 pixels in the vertical direction. If images are recorded in field mode, then each field must be recorded at a minimum resolution of 640 by 240.

The recording resolution for a given DVR will vary depending on the specifications, configuration and installation of the system. For example, higher resolution settings may decrease the recording time available, but generally will produce higher quality images.

It should be noted that, among other things, both the recording resolution of the system, the type and level of compression (see Section 5.6.4), and the resolution of the cameras (see Section 5.2.4) will determine the level of detail in the recorded video or images.

The Scientific Working Group on Imaging Technology strongly encourages the use of higher resolutions than those described above whenever possible.

5.6.4. Compression

Compression is a process in which the size of a digital file is reduced. Due to the large amount of information present in each video image, most digital CCTV systems use compression to reduce storage and transmission requirements.

Compression may be lossless or lossy. In lossless compression all data can be retrieved in its original form. When data has been saved using lossy compression it is not possible to recover all of the information.

In the event of an alarm-triggered mode (see Section 5.6.9), it is recommended that lossless compression be used to record the incident. If a system is incapable of lossless compression, it is strongly recommended that the lowest possible amount of compression be used in order to maximize the amount of information available to law enforcement.

Some manufacturers use non-standard formats that require the use of proprietary software to view the video or images. Use of such software can prevent or hinder law enforcement from viewing or otherwise accessing these images. If such software is required, then steps must be taken to ensure its availability to law enforcement. See Section 7 for more guidance.

5.6.5. Analog Video Recording Speeds

Analog videotapes are usually recorded in one of three speeds: SP (standard play), LP (long play), or EP/SLP (extended play/super-long play). A T-120 tape recording at SP speed will record for a period of two hours, whereas a T-120 tape recording at LP speed will record for a period of four hours, and a T-120 tape recording at EP/SLP speed will record for a period of six hours. Changing the recording speed from SP to LP to EP/SLP play does not change the rate at which images are recorded.

5.6.6. Recording Rates and Time-Lapse

National Television Standards Committee (NTSC) video is recorded at a rate of approximately 30 frames per second. Each frame consists of two fields or images, producing an actual rate of 60 images per second. Any recording made at a rate of 60 fields per second is commonly referred to as a real time recording.

Both analog and digital CCTV systems are capable of recording video at rates that are much lower than 60 images per second. This enables the recording of images over a longer period of time.

In digital CCTV systems, this is expressed as the recording (record) rate of the system. The recording rate may be configured for the entire system, or independent to each camera. For example, a ten (10) camera system could be configured to record twenty (20) images per second (ips). As noted above, depending on the system, this could result in each camera being recorded at 2 ips or 20 ips.

In analog CCTV systems, the recording rate is typically expressed as time-lapse rate. A single time-lapse rate is configured on and for the video cassette recorder. In situations involving multiple cameras, such as when using multiplexers, additional configuration can be made to capture additional images from certain cameras (see Section 5.6.9). The images per second captured by the recorder can be affected by the time-lapse rate (or mode), length of the recording media (e.g. VHS videotape), and the recording mode (described in the previous section). For example, using T-120 tapes, a VCR set in SP mode will record 30 frames (60 images) per second for two hours. With a time-lapse setting of 24-hours, a T-120 tape will run for twelve (12) times the normal two-hour tape length, and the VCR will record no more than five images per second. Table 1 provides the image-recording rate for a variety of common time-lapse settings under normal recording conditions.

Table 1. Typical Image Recording Rate for Different Time-Lapse Modes

Time-lapse mode (in hours)	2	12	24	48	72	120	240
Number of fields (images) per second	60	10	5	2.5 (5 every 2 sec.)	1.67 (5 every 3 sec.)	1	0.5 (1 every 2 sec)

(Based on an approximate real-time rate of 60 fields per second.)

Some analog time-lapse video recorders manufactured specifically for CCTV security applications are designed to record a higher number of fields per second in different time-lapse modes than those reported in Table 1. For example, some high-density video recorders can achieve record rates of more than 20 fields per second in 24-hour time-lapse mode.

The recording rate of the system, whether digital or analog, should be configured to adequately capture the activity of interest in the coverage areas. When possible, areas which contain fast movement (e.g. cameras focused on register drawers) or otherwise important (e.g. entrances and exits) should be captured at a higher recording rate. For more information regarding camera placement and importance, refer to Section 5.2.1.

In order to meet the SWGIT guidelines, CCTV systems must capture and record at least one complete field per camera per second. Any rate lower than this may result in inadequate coverage of events in the scene.

5.6.7. Switchers/Multiplexers

Facilities utilizing analog CCTV systems with more than one camera may choose to use a device that enables the recording of images from all of the cameras to a single recorder. The two most common devices used to do this are switchers and multiplexers.

Switchers, as the name implies, alternate among multiple cameras so that the output of the switcher at any one time is the signal from a single camera. Systems in which the output of a switcher serves as the input to the recording device will record images from each camera in succession. The time that it takes for a switcher to return to the same camera is called the camera interval. The reciprocal of this interval is referred to as the camera refresh rate. Therefore, a camera interval of one-half second would correspond to a camera refresh rate of two times per second.

A multiplexer takes the outputs from multiple cameras and adds an encoded signal that allows a picture from each camera to be viewed in succession (as with switchers) or simultaneously. The encoded data carried within the signal is typically proprietary, making it difficult to recover the recorded images, date, time and other information without the proper hardware and software.

Many multiplexers and switchers allow users to view multiple cameras in a multi-screen mode, while also recording a full size image output of each camera. While multi-image viewing is acceptable, multi-image recording is not recommended.

In order to meet the SWGIT guidelines, CCTV systems must not record in multi-image modes, because it significantly decreases the individual camera's image resolution (size) and quality.

Given the requirement in Section 5.6.6 (recordings should capture at least one complete field per camera per second) the refresh rate for each camera in a system with one recorder will have a minimum value. As a reference**, Table 2** relates the number of images per second per camera for given time-lapse recording modes.

Table 2. Images Recorded per Second by Each Camera in a Switched System for Different Time-Lapse Modes

Images (Fields) Recorded per Second by Each Camera							
		Time-Lapse Recording Mode (in hours)					
		2	12	24	48	72	120
Cameras	1	60	10	5	2.5	1.67	1*
	2	30	5	2.5	1.75	^	^
	4	15	2.5	1.25	^	^	^
	8	7.5	1.25	^	^	^	^
	16	3.75	^	^	^	^	^
	32	1.875	^	^	^	^	^
	60	1*	^	^	^	^	^

* Indicates limits fixed by the Scientific Working Group on Imaging Technology requirement of one image per camera per second.

^ Indicates this cannot meet the Scientific Working Group on Imaging Technology requirement of one image per camera per second.

The values reported in Table 2 assume a nominal real-time recording rate of 60 fields per second. As described in Section 5.6.6, some CCTV security system video recorders designed specifically for time-lapse applications are capable of exceeding the values reported in this table. Under such circumstances, it will be possible to record images from more cameras while still meeting the SWGIT requirement of one image per camera per second.

Most digital CCTV systems support the recording of multiple cameras with hardware integrated into the recording unit.

5.6.8. Recordings of Associated Text Information

Both analog and digital CCTV systems include the capability to associate text information, such as date, time, and camera identification, with the images recorded by the system. In some cases, transaction or personal information may also be recorded in association with image data. This is often accomplished by superimposing the text directly on the images.

Date, time, and camera information is useful in investigations and should be preserved. However, text that obstructs the view of subjects' faces or vehicles' license plates may hinder investigations and should be placed to minimize its effect on image content. Test recordings should be performed to ensure that this requirement is being met and that the information being recorded is accurate.

The SWGIT strongly recommends that digital CCTV systems be configured so that associated text information is unalterable and preserved as data records or files that are linked to the respective images. In such cases where date and time, transaction, or personal information is recorded in digital systems along with the image stream, it must be possible for law enforcement to recover the images separate from this information.

For analog CCTV systems in which it is not possible to separate personal or transaction data from the images, systems must be configured to record this information for one second or less for each instance (e.g., transaction) in which such data is required. If the text information is visible on the recorded video, then the text characters must be as small as possible while still being legible, and it must be possible to position the text anywhere on the screen to minimize the effect.

Each individual image and transaction data packet should have a date/time stamp associated with it. Whenever possible the date/time stamp should be generated as close to the image source as possible. For example, when a camera is directly wired to the digital recording device at the same site, then time synchronizing the recorder is sufficient. However, when the camera is located remotely (in another city) and connected to the recorder by a wide-area network (WAN), then the image may be delayed in transit. In those cases, it is highly desirable to associate the time stamp with the image at the source sensor (the camera) instead of at the recorder. A time-tag image file is then transferred over the WAN to the recorder. The trend toward using Internet-protocol (IP) cameras will facilitate this process where the Internet-protocol camera is capable of accepting time synchronization input. The use of an industry standard time synchronization protocol is recommended.

5.6.9. Triggers & Alarms

In some situations, systems may include triggers that lead to the recording of images at a rate, or in a sequence, that differs from the normal operating mode. An example of this would be to change from time-lapse mode to real-time mode when triggered by an alarm button. Another example would be to include an otherwise inactive camera in the recorded sequence if motion was detected in the field of view of that camera.

If such a device is used, its use must not conflict with the recommendation in Section 5.6.6 (e.g., one field per second from every camera in the system must continue to be recorded at a minimum).

Unlike triggers, which are typically activated automatically (e.g. motion detection), alarms are usually activated manually during an incident such as a robbery.

In the event of alarm activation, law enforcement will seek to have the highest possible image quality. Therefore, in order to meet SWGIT guidelines, CCTV systems must have an alarm mode. The following system settings are required for the alarm sequence:

- Lossless compression (Currently installed systems that are incapable of lossless compression should be configured to record the alarm sequence at the lowest possible compression ratio – see Section 5.6.4).

- The recorder must have a buffer capable of retaining the five minutes of data prior to the alarm trigger.

- The system should record the cameras of interest at a rate of 15 images per second, while maintaining the same rate at which the system switches between cameras (e.g., more pictures per camera each second if time-lapse mode is normally used).

- Once triggered, the system should continue to record in this same manner until manually stopped by an authorized agent, according to the facility's policies and procedures. Systems should be configured to prevent overwriting video from the incident for which the alarm was triggered. The recorder shall have sufficient storage to be capable of recording in this mode for a minimum of 30 minutes.

Furthermore, test recordings should be made to ensure that activation of a trigger or alarm does not have a harmful effect on the quality of the recorded images.

5.6.10. Retention of Recordings

It is recommended that analog videotapes be retained for a minimum of 31 days before being reused and only be reused a maximum of 12 times. For ease of retrieval, each videotape should be sequentially numbered, and the dates and times recorded on each tape should be written on a label on the videotape.

Due to the nature of digital recordings, SWGIT recommends that recordings be retained for the longest time possible (minimum of 10 days) with the least amount of compression available in the system's capabilities. Storage capacity to meet these needs must be considered.

Institutions should establish policies regarding the marking of removable media (e.g. VHS videotapes) so that the most recent date of recording will be documented.

Institutional requirements will dictate the length of time for which recordings must be retained.

5.6.11. Network Monitoring & Recording

Some CCTV systems allow for remote monitoring, recording, and device (e.g. camera) control over a network.

The images transmitted this way are often significantly compressed in order to meet bandwidth restrictions. As noted in Section 5.6.4, excessive compression severely degrades image quality.

In situations where remote monitoring is practiced, SWGIT strongly recommends that recording devices be installed at each local facility so that images may be recorded with minimal image compression.

When utilizing device control over a network, the response times experienced may not be equivalent to local control. Tests should be performed to ensure sufficient response time. Due to the increased load placed on the network in these situations (see Section 5.4), tests should be performed to ensure sufficient bandwidth is available. In order to obtain sufficient bandwidth, a dedicated network for CCTV may be required.

5.6.12. Digital CCTV Export

Unlike analog videotape based CCTV systems, retrieving digital video footage is often not as easy as ejecting a videotape. The hardware and file formats vary greatly among digital CCTV systems.

The digital system should provide the capability to export a specific time period and/or camera views. See Section 7 for further information regarding guidelines for export in the event of a criminal incident.

5.6.12.1. Devices

Digital recording systems must be capable of exporting exact duplicates of their recordings to a standard removable media format (e.g. CDs, DVDs). This is necessary so that law enforcement officials can obtain copies of the recorded digital files that are a bit for bit copy of the files stored on the system.

In order to meet SWGIT guidelines, CCTV systems using digital recorders must be configured to export to storage devices including CD/DVD. In order to facilitate larger exports, the system must also include at least one standard port that supports the connection of external storage devices, such as Universal Serial Bus (USB).

Unless absolutely necessary, it is not recommended to output video from a digital CCTV system via an analog signal (e.g. recording to VHS videotape).

Write-once media (e.g. CD-R) should be used whenever possible.

5.6.12.2. File Types

The format of most CCTV data is usually proprietary. Without the native file and proprietary software, it may be difficult to display the date, time, and other information with the recorded images. For this reason, proprietary file viewers should be included in the export, or otherwise available.

All export formats must maintain aspect ratios consistent with the original recording.

5.6.12.3. Video

As stated above (Section 5.6.12.1), it is important for the system to support the export of bit for bit copies of original video files.

The system should also support the export of video files in an open file format, such as uncompressed, non-proprietary AVI (audio video interleave).

5.6.12.4. Still Image

The system must support the export of single still image files in a standard lossless format (e.g. BMP or TIFF). Formats that use lossy compression (e.g. JPG/JPEG) should not be used unless a lossless format is not available.

5.7. Monitor/Display

For analog video recording systems, monitors capable of operating in an under-scan mode are strongly recommended. This capability permits the viewer to observe the entire field of view being recorded. For digital video recording systems, a digital display is strongly recommended.

6. System Maintenance

CCTV systems should be maintained in a manner that ensures their proper function. Therefore, the following recommendations should be adhered to.

6.1. System Documentation

Institutions should maintain documentation regarding their CCTV systems that includes the following information:

Make and model of all system components, including recorders, cameras, lenses, and multiplexers/switchers. For digital systems, this information should include software and hardware information, including software version. If infrared-sensitive cameras are in use, their location should be documented. An example of a system information sheet is included in Appendix C. A photocopy of the maintenance record should be included.

- Adequate system documentation should be included at the site. This includes system manuals, retention schedule, keys, passwords, and instructions for downloading and outputting recordings.

- Point-of-contact information for system installer and/or system maintenance organization, to include at least two names and telephone numbers.

- Site plan showing all equipment placement (including recorders), as well as field-of-view for each camera. Appendix C includes an example of a site plan.

This information should be verified monthly and made available to responding law enforcement officials upon their arrival at the scene.

6.2. System Validation and Maintenance

Prior to use, systems must be validated to meet the requirements of Section 4. The systems must be capable of acquiring, recording, and producing output images that are of sufficient quality to enable law enforcement officials to identify the people and objects depicted therein. Revalidation of these requirements must occur every time the system is altered.

For example, if additional cameras are added to the system, the resulting video quality could be negatively impacted and should be verified.

A variety of system checks and maintenance are necessary at different times. If system errors are found, steps to correct them should be implemented.

A maintenance log must be maintained to document all system validation activities, checks, and maintenance activities.

Table 4 provides a calendar for these checks and maintenance items that should be recorded on a maintenance log.

Table 4. System Checks and Maintenance Schedule

	Check / Activity	**Procedure**
Daily	Is the system operating?	Play back 30 seconds of recorded video and confirm that all cameras are being recorded.
	Are the cameras aimed properly, in focus, and not obstructed?	Review live images from each camera to ensure this.
	Are the date and time correct?	This is dependent on the system design.
	Is the removable recording media (i.e., tape) properly installed and in the record mode?	Check that the record indicator is active and/or that the tape counter is advancing.
	Is the system secured?	Check physical locks on cabinet and/or doors.
Monthly	Clean camera lenses and housings. (Care must be taken to avoid damage and misalignment.) More frequent cleaning may be necessary depending on environmental conditions.	Follow manufacturer's specifications.
	For systems using removable media (i.e., tape), recording mechanisms should be cleaned.	Follow manufacturer's specifications.
	Check environmental controls (temperature and humidity) to ensure that they meet manufacturer's specifications for all system components.	Follow manufacturer's specifications.
Annually	Complete system preventative maintenance check.	A qualified CCTV technician should perform this check.
	For digital systems using hard drives for storage, a check for bad clusters and other disk errors should be performed.	Refer to manufacturer's instructions and specifications.
	Ensure written policies and procedures regarding system operation are up to date.	Review existing policies and procedures and revise as needed.
	Ensure employee competence in system operations, including alarm-mode response.	Conduct operator training.

	Ensure system output to CD, DVD, or other removable media meets law enforcement needs.	Write sample images from system to removable media and review images on separate computer system.
	Ensure that reusable media is replaced.	A system operator should perform this check.
	Check system configuration and recording settings.	Review resolution, frames/images per second, retention time, number of cameras, etc. is still adequate for recording purposes.

6.3. Maintenance of Recording Media

All recording media has an expected usable life span. Based on that life span, policies should be developed to ensure that media is replaced before this period expires. For example, it is recommended that VHS videotapes be reused no more than 12 times and that they be replaced on an annual basis. The use of extended time-lapse mode may drastically shorten the life span.

For digital recording devices, manufacturer's recommendations for maintenance and the device service-life replacement schedule should be observed. A regular ongoing (automated) inspection of hard drives should be conducted to ensure that the disk(s) is/are functioning properly and that there are no bad sectors or other hardware errors that could result in a loss of data. Other reusable media must be recertified no less frequently than the manufacturer's guarantee period.

Steps must be taken to ensure that media is not mishandled or damaged. This includes keeping media away from magnetic fields, such as those generated by televisions, radios, and speakers. The media should be maintained at room temperature and out of direct sunlight. Media should not be stored in vehicles for an extended period of time.

7. Evidence Handling Procedures

This section addresses procedures to follow when law enforcement response is necessary pursuant to an investigation.

7.1. Documentation for Law Enforcement

The system documentation, as described in Section 6.1, including equipment information, site plan, passwords, contact information, and maintenance log, should be made available to responding law enforcement officials. Any additional pertinent information regarding the recording or the incident itself should be noted, such as incident time, record mode, and discrepancies between actual time and recorder time. Appendix C includes an example of documentation.

7.2. Handling Evidentiary Recordings

Following an incident involving immediate law enforcement response, it is necessary to ensure that the recorded images are secured. Unless the possibility exists that the images may be recorded over, the recording should not be stopped or reviewed until law enforcement officials arrive.

7.2.1. Analog video systems

Upon stopping a recording, the tape should be removed from the recording device and the recording tab immediately removed or shifted to the record-disabled setting. The name of the institution and identity of the person performing this function should be marked on the exterior of the cassette housing, along with the date and time of removal.

Personnel to assist in accessing the tape should be identified and made available prior to the arrival of law enforcement officials.

7.2.2. Digital video systems

The following steps should be followed:

1. Upon stopping a recording, personnel qualified to assist law enforcement in recovering video from the CCTV system should be identified and made available (in person or by telephone) to offer technical assistance.

2. Law enforcement officials will coordinate with appropriate personnel to view and retrieve the best video and/or image(s) prior to the officials' departure from the scene.

When immediate transmission or distribution is necessary from the scene, the video and/or image(s) should be made available by network, e-mail, CD/DVD, or other means. Images should be provided to law enforcement in the TIFF or BMP format. It is not recommended to solely provide JPG images to law enforcement unless absolutely necessary.

If the facility uses a remote location for the storage of recorded images, then the facility will provide video and/or image(s) to an address designated by the law enforcement officials.

3. The facility's security personnel should produce at least two copies of the relevant images and video on CD-R, DVD-R, or other removable media in its original native format, as well as a non-proprietary format.

4. In the event of alarm trigger incidents as described in Section 5.6.9, law enforcement would like all video and relevant data that were recorded five minutes before the alarm trigger, the entire incident, and five minutes after the incident. This is barring any outside circumstances when it is required to save a longer period of time (e.g., casing of the bank).

5. If additional retrieval of video is warranted, law enforcement officials will notify the facility's security personnel to secure the recording device, or retrieve additional video and/or images.

6. When the relevant video, images, and data have been retrieved, each shall be labeled with the name of the institution and identity of the person performing this function, along with the date and time of removal. This information should not be written directly on the media but preferably on a label that is affixed to a protective container, such as a jewel case, sleeve, or clamshell enclosure.

APPENDIX A – CCTV References

Aldridge, J. CCTV Operational Requirements Manual Version 3.0. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 17/94, ISBN 1 85893 335 8. (1994). Available: http://www.homeoffice.gov.uk/pcrg/psdb/publications/or_manual.pdf

Aldridge, J. and Gilbert, C. Performance Testing CCTV Perimeter Surveillance Systems. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 14/95, 1995.

Atkinson, D. J., Pietrasiewicz, V. J., and Junker, K. E. Video Surveillance Equipment Selection and Application Guide, NIJ Guide 201-99. In *Law Enforcement and Corrections Standards and Testing Program* [Online]. (February 2000). Available: http://www.ojp.usdoj.gov/nij/pubs-sum/179545.htm

Brown, B. Crime Reduction: Closed Circuit Television in Town Centres: Three Case Studies. *United Kingdom Home Office Police Research Group - Crime Detection and Prevention Series Paper 68.* (1995). Available: http://www.crimereduction.gov.uk/cctv1.htm

Diffley, C. and Wallace, E. CCTV: Making it Work. Training Practices for CCTV Operators. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 9/98, ISBN: 1 84082 045 4. (1998). Available: http://www.homeoffice.gov.uk/pcrg/psdb/publications/cctv-9_98.pdf

Green, M. W. The Appropriate and Effective Use of Security Technologies in U.S. Schools. In: *A Guide for Practical School Security Applications* [Online]. (September 1999). Available: http://www.ojp.usdoj.gov/nij/pubs-sum/178265.htm

Griffiths, A. CCTV: Making It Work. Time and Date Displays. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 13/98, 1998.

Mather, P. Guidelines for the Handling of Video Tape. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 21/98, 1998.

Nichols, L. J. The Use of CCTV/Video Cameras in Law Enforcement, International Association of Chiefs of Police (IACP). (March 2001). Available: http://www.theiacp.org/documents/pdfs/Publications/UseofCCTV.pdf

Police Scientific Development Branch, Digital Imaging Procedure Version 1.0. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 02/2002. (2002). Available: http://www.homeoffice.gov.uk/pcrg/psdb/publications/digimpro.pdf

Rason, J., Kent, T., Sall, I., Gugenheim, P., and Walker, S. Assessment of the ADVIS, IMPRESS, VIEW Video Enhancement System for the UK Police Service. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 1/2000, 2000.

Scarman Centre National CCTV Evaluation Team, National Evaluation of CCTV: Early findings on scheme implementation – effective practical guide. *United Kingdom Home Office Statistical Bulletin 5/03.* (April 2003). Available: http://www.crimereduction.gov.uk/cctv32.htm

Security Industry Association, 1998-1999 CCTV for Public Safety Report, Security Industry Association, (August 1998). Available: http://www.siaonline.org/response.asp?c=storeproduct_59&r=1024

Tilley, N. Crime Reduction: Understanding Public Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities, *United Kingdom Home Office Police Research Group – Crime Prevention Unit Series Paper No. 42.* (1993). Available: http://www.crimereduction.gov.uk/cctv2.htm

Wallace, E. and Diffley, C. CCTV: Making it Work. Guidance on Recruitment and Selection Practice for CCTV. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 8/98, 1998.

Wallace, E. and Diffley, C. CCTV: Making it Work. CCTV Control Room Ergonomics. Police Scientific Development Branch (PSDB), United Kingdom Home Office, PSDB Publication number 14/98, 1998.

Appendix B: Technical Guidelines for Lighting

In this document, illuminance is measured in Lux. Some older documents and references may refer to the measurement in footcandles (one footcandle is approximately equal to 11Lux).

To provide good-quality camera images, a minimum of 275 to 333Lux of illumination should be provided in the customer areas, office areas, hallways, stairways, and exits where there is camera coverage.

Exterior self-service facilities, such as automated teller machine vestibules or drive-up lanes, should have a minimum of 110Lux of illumination 24-hours daily to ensure good image quality.

Exterior areas, such as sidewalks, entrances, night depository areas, that have camera coverage should have a minimum of 55Lux of illumination.

Parking lots with camera coverage should have a minimum of 11Lux of illumination at ground level.

Supplementary surface lighting may be necessary for adequate illumination for the face of anyone using an automated teller machine or other self-service resource.

Appendix C: System Documentation and Site Plan Examples

System Equipment Information

Recorder make and model _____

Multiplexer make and model _____

Camera/s make and model _____

Are any cameras infrared-sensitive and if so identify _____

Video format (circle) VHS SVHS digital video recorder PC
Other _____

If digital video recorder or PC-based:
Hardware manufacturer _____
Software name and version _____

Is a copy of the most current maintenance/service log attached? (circle) YES NO

Does the system record multiple cameras? (circle) YES NO
If yes, how many? _____

Contact Information

Recording system point of contact _____ Telephone: _____

Institution point of contact _____Telephone: _____

If the system records multiple cameras, note the camera location and angle view. Use the following diagrams as examples.

Include the following additional information in the event of a law enforcement response:

What record mode was the system? (circle) 2 hour, 6 hour, 12 hour, 24 hour, 48 hour, 72 hour,
Other _____ Unknown

Does the recorded date/time accurately represent the time of day? (circle) YES NO

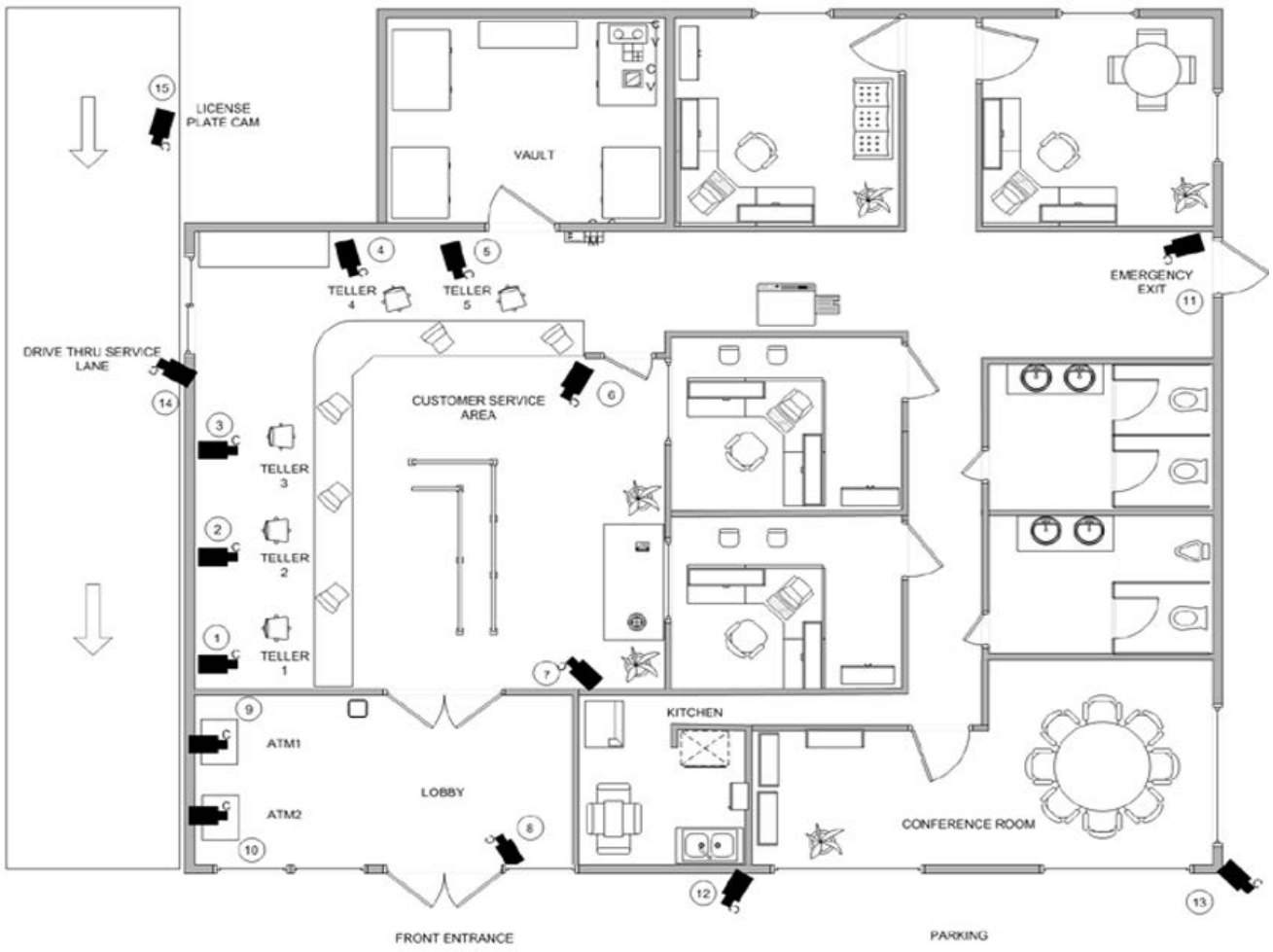
Date and time of incident _____

Date and time of incident on tape _____

Date and time recording removed from equipment_____

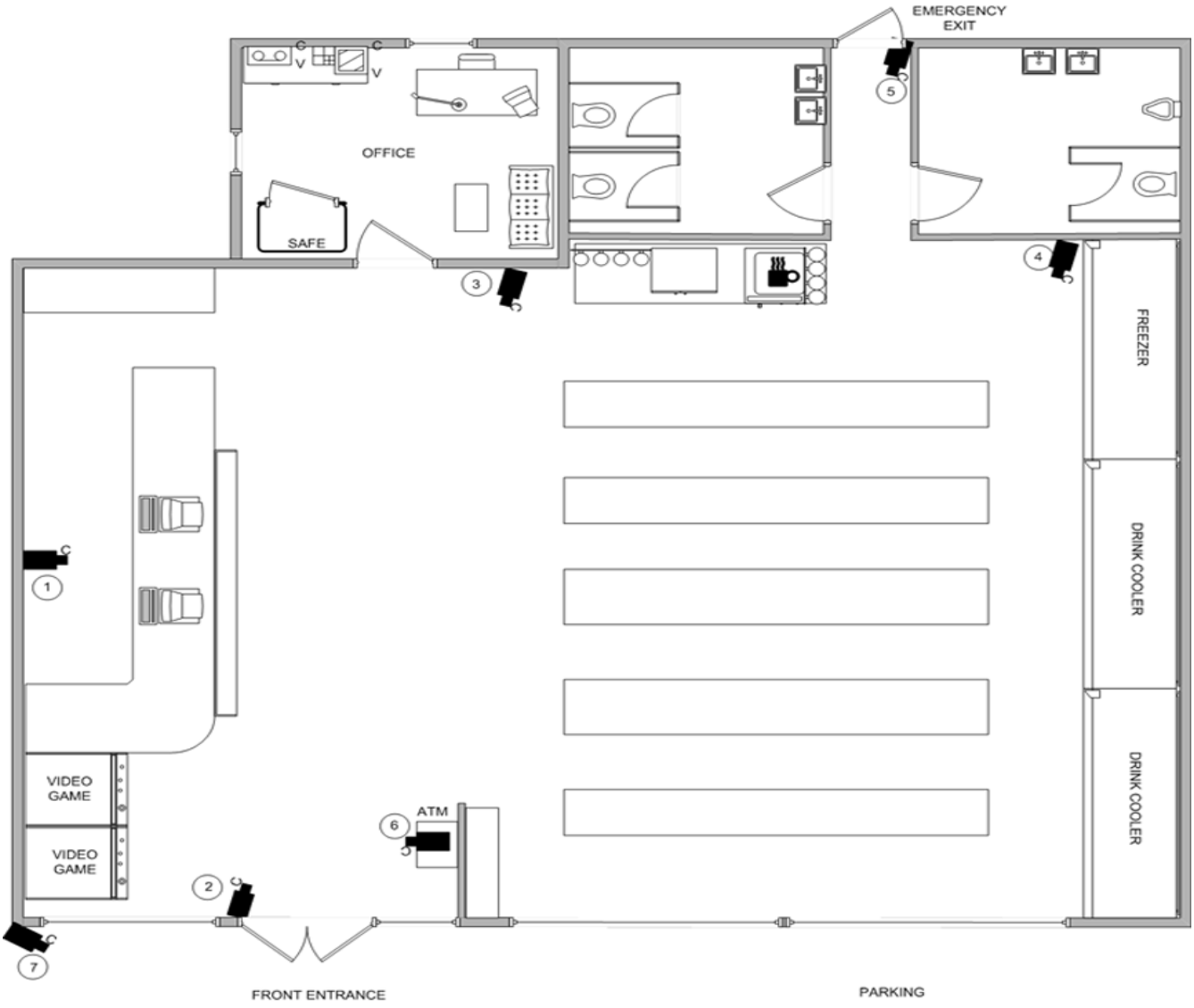
Other Information:_____
_____
_____

EXAMPLE OF SITE PLAN FOR
SMALL BANK



Camera 1: Teller one, facing east
Camera 2: Teller two, facing east
Camera 3: Teller three, facing east
Camera 4: Teller four, facing south
Camera 5: Teller five, facing south
Camera 6: Customer-service area, facing south-west
Camera 7: Customer-service area, facing north-west
Camera 8: Lobby, facing north-west
Camera 9: Lobby automated teller machine one
Camera 10: Lobby automated teller machine two
Camera 11: Emergency exit, facing west
Camera 12: Parking lot, south side of building
Camera 13: Parking lot, south-east corner of building
Camera 14: Drive-through service lane, facing west
Camera 15: Drive-through service lane, facing south

EXAMPLE OF SITE PLAN FOR CONVENIENCE STORE



Camera 1: Clerk and check-out area, facing east
Camera 2: Front door entrance, facing north
Camera 3: Outside of office, facing south
Camera 4: Freezer area, facing south
Camera 5: Emergency exit, facing south
Camera 6: Automated teller machine, facing west
Camera 7: Parking lot, facing south-east

Section 5

Guidelines for Image Processing

Previously called "Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System"

Objective

The purpose of this document is to provide guidelines for the use of digital image processing in the criminal justice system. The objective is to ensure the production of quality forensic imagery for use as evidence in a court of law. This document includes brief descriptions of advantages, disadvantages, and potential limitations of each major process.

SWGIT Position on Image Processing

Traditional photography and its associated image processes have been used in legal matters since 1839[1]. Many of the same processes developed for traditional photography have equivalent counterparts in digital image processing. All of the techniques used in digital image processing have their roots in traditional photography and/or mathematics. This historical precedent helped digital image processing become established and accepted in forensic science.

It is the position of the Scientific Working Group on Imaging Technology (SWGIT) that any changes to an image made through image processing are acceptable in forensic applications provided the following criteria are met:

- The original image is preserved.
- Processing steps are documented when appropriate (see SWGIT document "*Best Practices for Documenting Image Enhancement*") in a manner sufficient to permit a comparably trained person to understand the steps taken, the techniques used, and to extract comparable information from the image.
- The end result is presented as a processed or working copy of the image.
- The recommendations of this document are followed.

Introduction

Processed images are used for many purposes by the forensic science community. They can yield information not readily apparent in the original image, which can assist an expert in drawing a conclusion that might not otherwise be reached.

[1] Photographic Evidence, 2nd Edition, Charles C. Scott, West Publishing Company, St. Paul, MN. 1969, Vol.1, page 2.

This document addresses image processing and related legal considerations in the following three categories:

- Image enhancement
- Image restoration
- Image compression

When using image processing techniques, use caution to avoid the introduction of artifacts that add misleading information to the image or the loss of image detail that could lead to an erroneous interpretation. Any image processing should be applied only to a working copy of the image.

Image Enhancement

Image enhancement is any process intended to improve the visual appearance of an image. Some of the processes below have a direct counterpart in the conventional silver-based photographic laboratory. Others can be accomplished only through digital processing.

Brightness adjustment is used when the image is too bright or too dark. If the image is made too bright, there is a risk of loss of detail in light areas. If the image is made too dark, there is a risk of loss of detail in the dark areas.

Contrast adjustment is used when the image lacks sufficient contrast. If the image contrast is increased too much, there is a risk of loss of detail in both light and dark areas.

Cropping is used to remove that portion of the image that is outside the area of interest.

Dodging and burning have the same effect as brightness adjustment but are used in localized areas.

Color processing includes color space transformations, pseudo coloring, and hue and saturation adjustments. These techniques can be used to modify the color characteristics of objects within an image.

Caution: Application of these techniques can compromise the color fidelity of the image.

Linear filtering techniques (see Figure 1) include sharpening, deblurring, edge enhancement, and deconvolution. They are used to increase the contrast of small detail in an image. If a low degree of enhancement is used, the image will remain an accurate representation of the scene. If a high degree of enhancement is used, the image may no longer be an accurate representation of the overall scene, though still may be useful as an adjunct for interpretation of small details.

Caution: A high degree of enhancement can also increase the visibility of existing noise and artifacts; examples of noise include film grain, snow appearing on a TV screen, or random color dots.

Figure 1. This example illustrates the effects of linear filtering. Left: original image; Middle: blurred image; Right: sharpened image.

Nonlinear contrast adjustments include gamma correction, grayscale transformation, and the use of curves and/or look-up tables. These are an extension of traditional photographic sensitometric techniques and are used to adjust the contrast in selected brightness ranges within the image.

A nonlinear contrast adjustment can be used to bring out details in the shadow areas of an image without affecting the highlight areas.

Caution: A severe adjustment can cause loss of detail, color reversal, and/or the introduction of artifacts, see Figure 2 on the next page.

Figure 2. This example shows nonlinear contrast adjustments. Left: original image; Middle: enhancement of shadow and highlight areas, at the expense of midrange tones; Right: enhancement of midrange tones, at the expense of shadow and highlight areas.

Pattern noise reduction filters identify repeating patterns in the image and allow the user to selectively remove them. This type of filter can be used to remove patterns such as fabric weaves, window screens, security patterns, and halftone dots.

Caution: Overuse of this technique can cause selective removal of relevant image detail.

Random noise reduction techniques include such filters as low pass filtering, Gaussian blurring, median filtering and despeckling. They are used to reduce the contrast of small detail in the image in order to suppress random noise.

Caution: Overuse of this technique can cause loss of relevant detail.

Image Restoration

Image restoration is any process applied to an image that has been degraded by a known cause (e.g., defocus or motion blur) to partially or totally remove the effects of that degradation.

Limitations are imposed on this technique by any noise in the image and by the fact that information that has been totally lost cannot be replaced. Often partial restoration

can be successful even when total restoration is impossible.

Restoration Techniques

Blur removal is a filtering technique designed to partially or completely remove an image blur imposed by a known cause. It differs from the image enhancement filtering processes because the blur removal filter is designed specifically for the process that blurred the particular image under examination. Examples include defocus and motion blur, since these blurring phenomena can be described mathematically. Thus, a specific filter can be designed to compensate for each blur. The degree to which a blur can be successfully removed is limited by noise in the image, the accuracy with which the actual blurring process can be described mathematically, and the fact that information has been totally lost and cannot be replaced. Often partial deblurring can be successful even when total deblurring is impossible.

Grayscale linearization is the adjustment of brightness relationships among the objects in a scene. The purpose of grayscale linearization is to render faithfully the different brightness values in the scene. For example, a monochrome test target having known gray values can be placed in the scene prior to recording the image. Then a grayscale transformation (nonlinear contrast stretch) can be designed to place the different gray values on the test target in their proper relationship. It is commonly assumed that the other objects in the scene will be put in their proper brightness relationship as well. Improper grayscale linearization can render brightness values inaccurately so that objects may appear brighter or darker than they actually appeared when the image was recorded.

Color balancing is the extension of grayscale linearization to a color image. It is the adjustment of the color components of an image. The purpose of color balancing is to render the colors in the scene faithfully. For example, a color test target having known colors can be placed in the scene prior to recording the image. Then a grayscale transformation (nonlinear contrast stretch) can be designed for each color channel (red, green, and blue) in order to place the different colors on the test target in their proper relationship. It is commonly assumed that the color of other objects in the scene will be rendered accurately as well. Improper color balance can render colors inaccurately, causing objects to appear to have the wrong color.

Warping, unlike other image restoration processes, changes the spatial relationships among the objects in an image. It is analogous to printing a photograph on a rubber sheet, then stretching the sheet in different directions and then tacking it down. Warping can be used, for example, to remove perspective from an image or to "unroll" a poster that was wrapped around a pole. Used improperly, it can distort the natural appearance of the objects in a scene.

Geometric restoration is the removal of geometric distortion from an image. Its purpose is to restore the proper spatial relationships among the objects in the scene. It can be used for the removal of geometric distortion, such as that introduced by a curved mirror or a fish-eye lens. It differs from image warping in that the geometric transformation is designed specifically for the process that distorted the particular image under examination. The degree to which geometric distortion can be successfully restored is limited by the accuracy with which the actual distortion process can be

described mathematically and the fact that information that has been totally lost (e.g., hidden behind another object or obscured from the camera) cannot be replaced. Often partial geometric restoration can be successful even when exact geometric restoration is impossible.

Image Compression

Digital images produce a large amount of data to be stored. Image compression techniques reduce the storage requirements by making image data files smaller.

Compression Processes

Lossless compression reduces file size by removing redundant information. Because the redundant information can be retrieved in order to display the image, lossless compression results in no loss of information. Lossless compression does not alter the content of an image when it is decompressed.

Lossy compression achieves greater reduction in file size by removing both redundant and irrelevant information. Because the irrelevant information (as determined by the compression algorithm) cannot be retrieved upon reconstruction of an image for display, compression results in some loss of image content as well as the introduction of artifacts. The degradation occurs each time the image is saved in a lossy file format. Higher compression ratios result in the loss of more information. Normally the degree of compression can be specified. Depending upon the application, lossy compression may render an image less useful.

The Joint Photographic Experts Group developed an image compression standard known as jpeg. This compression algorithm is applied to the image in 8-pixel by 8-pixel blocks. Normally, it is used as a lossy compression scheme where the degree of compression can be specified prior to storing the image. However, jpeg can also be used as a lossless compression scheme. At high compression ratios, jpeg could remove important image detail and introduce blocking artifacts as the block boundaries become visible (see Figure 3*)*. Jpeg is but one of many compression algorithms.

Caution: Compression should be used with care to avoid material degradation of the image. Additionally, the compression settings used by one camera or software program may not be the same as the compression settings used by another camera or software program.

Figure 3. Left: original image; Middle: the result of JPEG compression (compression ratio = 15:1); Right: the result of edge enhancement after compression.

Use of Compression

Many digital cameras store images using jpeg compression, so that some compression is unavoidable. Some digital cameras are capable of storing images in an uncompressed form. The degree of compression should be set low enough that important image content is not lost or obscured by artifacts.

In instances where the primary or original image is already compressed, it should not be further compressed using lossy compression processes; additional data will be lost. Sources of compressed primary images may include electronic booking photographs, some types of digital camera images, and images downloaded from the internet or email. The file format is not an indicator of the compression history for an image. For example, a .tif file may have been previously compressed in a lossy file format (.jpg).

Be aware that the end use of any image may change over time, and the use of lossy compression may become problematic. When an image was compressed, documentation may be necessary in a court of law where there may be a challenge that lossy compression might have introduced artifacts or that relevant information was lost.

Caution: Images intended for analysis should not be compressed using a lossy process.

Frequently Asked Questions (FAQ)

Question: What type of image must not be subjected to the following: image enhancement, compression, or restoration techniques?
Answer: A primary or original image.
Discussion: Because a primary or original image represents the first instance where the image is recorded onto any media, or it is an accurate and complete replica of the primary image, it must not be altered or modified.

Question: In a legal setting, what types of images are discoverable?
Answer: All images may be discoverable.
Discussion: In cases where images are processed, both the original and the processed image, along with associated documentation, may be discoverable.

Question: Who is responsible for testifying about a processed image?
Answer: The person who performed the processing or a person skilled in and knowledgeable about the processing that was used.
Discussion: The person who performed the processing is best qualified to testify about the technique(s) used. However, there may be occasions where the court will require the assistance of additional subject-matter experts. For issues relating to compression, the person who performed the compression can testify about the settings used to compress an image. Questions concerning the actual compression process should be referred to individuals who possess sufficient technical expertise to explain the specific process.

Question: Are there legal ramifications associated with the software used for image processing?
Answer: Yes.
Discussion: Some considerations may include:

- Have the particular functions within the software been accepted by the scientific community?
- Does the software perform as the manufacturer purports?
- Does the software have "plug-ins" that are produced by another manufacturer?
- Is the process repeatable and reliable?
- For image restoration, has the degradation process been accurately modeled?

Question: Where does image processing take place: in the field or in a controlled environment?
Answer: Both.
Discussion: Whereas most image processing takes place in a controlled environment, some image processing, such as image compression, may take place in the field. Image creation itself within a digital camera involves a significant degree of image processing and many modern digital cameras contain significant image processing software that can be controlled by the user.

Question: Who performs image processing?
Answer: Photographers, analysts, and technicians.
Discussion: The person performing the processing must be properly trained. See SWGIT document *"Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System"* and SWGIT/SWGDE document *"Guidelines and Recommendations for Training in Digital and Multimedia Evidence".*

Question: What are file management processes?
Answer: File management processes are the capture, storage, indexing, retrieval, and archiving of image files.
Discussion: Agencies and organizations should establish file management procedures for managing image files for use at a later date.

Question: Does image processing change images?
Answer: Yes.
Discussion: The purpose of image processing is to change the images in a controlled, predictable, and repeatable manner. Image processing does not mean that the original image is overwritten during the process. Forensic image processing should only be performed on working images. See SWGIT document *"Best Practices for Documenting Image Enhancement".*

Question: Is it necessary to document the step(s) used to produce a processed image?
Answer: Yes.
Discussion: The degree to which procedures used in image processing should be documented will depend on the intended end use of the image. Furthermore, the nature of such documentation will depend on the procedures used. See SWGIT document *"Best Practices for Documenting Image Enhancement".*

Guidelines for Digital Image Processing Standard Operating Procedures

The purpose of image processing procedures is to apply processing techniques intended to enhance, restore, and/or compress digital images. Standard operating procedures should be developed and followed. The appendix is a sample standard operating procedure. See also SWGDE/SWGIT document "*Recommended Guidelines for Developing Standard Operating Procedures*".

Equipment

The agency should address the following minimum hardware and software equipment requirements.

Hardware:

- Input/capture device
- Image processing systems
- Output devices
- Storage/archive

Software:

- Image management
- Image processing

Procedures
Agencies should establish specific step-by-step procedures for image processing according to agency requirements using SWGIT guidelines. These procedures should address the following as a minimum:

- Capture
- Processing
- Storage/archive
- Image management
- Security
- Output

Calibration
If necessary, agencies should develop calibration procedures specific to their needs.

Calculations
If necessary, agencies should develop calculation procedures specific to their needs.

Limitations
Agencies should take into consideration agency-specific budget, equipment, management, and accrediting agency requirements.

Safety
Agencies should develop safety procedures specific to their needs.

References
Agencies should maintain its agency-specific documentation, manufacturers' manuals, and SWGIT guidelines.

Training
Agencies should document procedures to ensure sufficient training to afford competence and proficiency with applicable image processing. Refer to the SWGIT "*Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System*" and "*SWGDE/SWGIT Guidelines and Recommendations for Training in Digital and Multimedia Evidence*".

Appendix

SAMPLE Standard Operating Procedures for Latent Print Digital Imaging

Latent Print Units
Laboratory Division

1. Purpose

1.1 This document sets forth Latent Print Units (LPU) specific procedures for latent print digital imaging.

2. Changes and Review

2.1 The Section Chief and Unit Chiefs are the only persons who may authorize changes to this document.

2.2 The appropriate LPU personnel who handle evidence which may be digitally processed must review the LPU Standard Operating Procedure for Latent Print Digital Imaging (SOP-LPDI).

3. Responsibilities

3.1 The Section Chief, Unit Chiefs, Team Supervisors, and Program Managers are responsible for ensuring that LPU personnel adhere to the evidence-handling procedures stated in the LPU Evidence Control Policy.

3.2 LPU personnel are required to handle evidence slated for latent print digital imaging in accordance with the procedures set forth in the LPU Evidence Control Policy.

4. Sending Evidence to the Latent Photography and Digital Imaging Group

4.1 LPU Specialists will determine if latent print digital image processing for enhancement purposes is needed after the appropriate silver based photographic procedures have been performed.

4.1.1 Specialists will initiate a separate Latent Print Digital Imaging Requisition form (LPDIR) for each item of evidence and will ensure all information is accurate.

4.1.2 Specialists will submit the form and appropriately sealed evidence to the Latent Photography and Digital Imaging Group (LPDIG).

5. Evidence Receiving in Latent Photography and Digital Imaging Group

5.1 LPDIG personnel will ensure that the LPDIR form and the evidence are submitted properly, and will sign for receipt.

6. Digital Image Capture

6.1 Upon receipt, the LPDIG Supervisor or designee will assign the submission to a photographer trained in digital imaging.

6.1.1 The assigned photographer will initiate a LPU Latent Print Digital Imaging Processing form (LPDIP).

6.1.2 The assigned photographer will use a digital image capture device to record the image of the latent print(s) in question and save the original image for each latent print using the file name structure to be defined.

6.1.3 The photographer will record the file name(s) assigned to the image(s) on a separate LPDIP form for each latent print. If the evidence is no longer needed, it will be stored in the evidence storage facilities in the LPDIG.

7. Digital Image Processing

7.1 The LPDIG Supervisor and Technology Development and Support Group(TDSG) Supervisors or respective designees will determine which specialist or photographer should perform the processing.

7.2 If the case specialist is not a digitally trained specialist, the specialist/photographer assigned will then contact the case specialist to arrange a time for the processing, so that the case specialist can be present when the processing is performed.

7.3 All processing steps will be recorded in the order they are performed either on a LPDIP form or within the computer program, if the program has that capability.

7.4 Once the case specialist is satisfied that the best possible image has been achieved, the image will be saved with a second file name assigned and recorded on the LPDIP form.

7.5 The case specialist will receive the original of the LPDIR and LPDIP forms along with all appropriate computer printouts for case documentation. A hard copy of both the original and processed images will also be provided for comparison purposes.

7.5.1 If no improvement results from this process and no images will be utilized by the case specialist, the original forms will be returned to the case specialist for case documentation, and a notation on the worksheet must be made that reflects the results of this effort. No image files will be stored when no improvement results.

8. Storage and Archiving of Images

8.1 All images, both original and processed, will be stored temporarily on the hard drive of the imaging station until the examination(s) is completed.

8.2 A backup copy of the images will be created weekly by the LPDIG Supervisor or designee and maintained in a locked cabinet within the LPU LPDIG until the examination(s) is completed.

8.3 Once the examination(s) is completed, the LPDIG Supervisor or designee will record the resultant images on two Digital Video Disks (DVD's) or Compact Disks (CD's) along with any associated case information. One DVD/CD will be designated a working copy and kept with the digital imaging equipment in a locked cabinet. The second DVD/CD will be designated as archival and kept in a locked cabinet within the TDSG.

8.3.1 The LPDIG Supervisor or designee will enter the appropriate DVD/CD serial numbers on both the LPDIR and LPDIP forms, return the originals to the case specialist, and file the duplicate copy of the LPDIP form within the locked cabinet along with the archival DVD/CD.

8.3.2 The DVD/CD's will be filed by the engraved serial number in numerical order in the above-mentioned cabinets. A database will be maintained by the LPDIG Supervisor.

Section 6

Guidelines and Recommendations for Training in Imaging Technology in the Criminal Justice System

Objective

The scope of this document is to provide personnel or laboratories with guidance regarding imaging training in disciplines that are not performing Image Analysis or Video Analysis. Information for personnel or laboratories conducting, Image Analysis and Video Analysis should refer to the SWGDE/SWGIT "*Guidelines & Recommendations for Training in Digital & Multimedia Evidence*."

The consistent and reliable use of silver-based, video, and digital imaging technologies in the criminal justice system requires the competent and appropriate training of personnel. The purpose of this document is to provide guidelines and recommendations for such training.

It should be recognized that some agencies may choose to provide training other than what is recommended in this section. In such circumstances, those agencies should demonstrate and document that the training selected is adequate to meet their anticipated needs.

Introduction

Personnel in the criminal justice system who work with images must be aware of the capabilities and limitations of specific imaging technologies. Those engaged in the production or the use of images should be aware of the procedures commonly followed within the law enforcement community and should strive to meet or exceed these recommendations. In support of these goals, the following recommendations are offered to personnel engaged in the production of images:

- Maintain awareness of new developments.
- Define and employ quality assurance programs to ensure the implementation of valid and reliable procedures for the task.
- Pursue continuing education courses in imaging technology.
- Maintain awareness of legal developments relating to the use of imaging technologies in the criminal justice system.

Definitions of Categories

Several categories of imaging technology training relevant to the criminal justice system as well as the categories of the system users who would benefit from the training are identified and defined as follows:

Categories of Training

- Awareness: Training designed to provide the non-imaging personnel who utilize images (e.g. lawyers, judges, and managers) with a general knowledge of the major elements of a given imaging technology including specific product capabilities.

- Skills and techniques: Training designed to provide competency in specific imaging equipment, as defined by their job requirements.

- Knowledge of processes and relationships: Training designed to provide the individual with an understanding of imaging technology and the ability to apply that technology to various applications as defined by their job requirements.

- Court procedures: witness testimony: Training designed to provide the individual with the ability to present reliable imaging technology based testimony in court.

- Court procedures: case preparation: Training designed to provide the individual with the ability to prepare and review accurate and reliable imaging technology based evidence.

- Continuing education: Training designed to provide the individual with additional and updated training in imaging technologies as defined by their job requirements.

Categories of Users

- Management: Includes personnel who are responsible for setting agency policies and/or making budget decisions

- Command/Supervision: Includes personnel who supervise and/or direct personnel engaged in the use of imaging technology

- Law Enforcement Officer: Includes personnel who use imaging technology as a minor component of their routine duties. If the person is routinely involved in the basic photographic documentation of crime scenes, then this person would fall into the crime scene technician category

- Crime Scene Technician/Investigator: Includes personnel for whom imaging is a major component of their routine duties.

- Photographer/Videographer: Includes personnel for whom imaging is the major component of their routine duties

- Lawyer: Includes prosecutors and defense attorneys

- Judge: Includes personnel who are responsible for the acceptance or rejection of imaging technology-based evidence in court proceedings

- Legal Assistant: Includes personnel who are responsible for preparing materials that will be offered in court proceedings

- Trainer: Includes personnel who are responsible for providing instruction to others in imaging technology-related areas

Recommended Training Levels

The level of training appropriate for any given position should be determined by the particular agency. In some instances, for instance, a managerial position may require only familiarity with the processes involved, while in others, managers who make tactical decisions may need practical proficiency. An examiner would need to demonstrate competency in the area of his or her duties, but a general knowledge of areas that do not directly impinge upon his or her area of expertise. Training should include continuing education to maintain currency.

Topical Areas for Focused Training

The following section delineates specific topical areas in which user groups should receive focused training to effectively fulfill their imaging technology related duties.

Managers, Commanders/Supervisors, Lawyers, and Judges (awareness and issues training)

- Status of imaging technology
    - Legal issues
    - Extent of use and who are the users
    - Industry and market trends
- Description of current technologies
    - Overview of digital imaging
    - Overview of video imaging (analog and digital)
    - Life cycle-cost comparisons and limitations
- Strategic alternatives for the agency
    - Determination of imaging needs
    - Sequence of equipment/software acquisitions
    - Actions to avoid or lessons learned
    - References/information sources

Legal Assistants (basic levels of skill for recording images)

- Working knowledge of the basic fundamentals of photography and/or videography
- Working knowledge of the capabilities and limitations of equipment
- Selection and operation of the appropriate cameras (digital, video, or film) and accessories
- Preparation of court presentations including images

Law Enforcement Officers (first responder)

- Operation of cameras with an understanding of the capabilities and limitations of the equipment assigned as a part of their routine duties
- Selection, framing, and composition of appropriate images
- Procedures for recording quality images in various situations
- Proper collection and preservation of the recording media
- Creation and maintenance of the chain of custody

Crime Scene Technicians

- Knowledge of, and experience in forensic photography techniques, such as
    - Retrieving impression evidence such as fingerprints and/or blood spatter
    - Selecting the appropriate media and equipment based on knowledge of the capabilities and limitations of the various aspects of imaging
    - Solving difficult non-routine imaging problems
- Awareness of image processing options
- Videography techniques
- Knowledge of how to use the most common image processing tools and techniques

Trainers

- Classroom techniques
- Development of lesson plans
- Preparation of audio-visual materials

- Development of student exercises
- Selection of text books and reference materials
- Development of course exams
- Development of proficiency exams
- Development of course evaluation processes

Areas to Consider When Addressing Training Needs
A number of issues should be considered when addressing an agency's training needs. The following section provides guidance for selecting training venues and addressing continuing education and testimony training needs.

On the Job Training
Experience is a critical training tool. Personnel who train under a competent practitioner gain valuable experience, as well as, knowledge and improved skills. However, managers should be aware that there is a potential limitation based on the trainer's knowledge of the state of the art and experience.

Continuing Education
Continuing education should be obtained annually from training conferences, trade shows, professional organizational memberships, professional publications, current literature and specialized courses. This training should address updates and the use of new technologies as it relates to:

- Hardware and equipment
- Software techniques
- Techniques, procedures and methods

Testimony Training
This training should include:

- Lecture-type presentation relevant to court testimony
- Moot court
- Court monitoring

Certifications
If applicable, a relevant test based certification can enhance the credibility of a witness.

Higher Education
The possession and type of a degree may be dictated by the forensic discipline, the accreditation status of the agency, or the requirements of the agency.

Training Documentation
To demonstrate compliance with training:

- Develop a written training program.
- Provide a training syllabus.
- Document performance.
- Establish a formal means of recognition of successful completion of the training such as a certificate, letter, or memorandum.

The retention of training documentation is left to the discretion of the agency.

Selecting a Training Provider

Course	**Instructor**	**Equipment**
Is a course outline provided?	What is the background and training of the instructor?	Does the training provider supply equipment for the training or must the students provide their own?
Is the course outline followed?	Is the training up to date? How has the instructor maintained proficiency in the field?	Is the course equipment offered by the provider sufficient to meet the agency's course objectives?
Does the course description include reference texts and other materials?	Can the instructor provide references?	Who provides the facilities, the agency or the training provider?
Does the trainer provide course evaluation forms, and are past evaluations available for review?	Is the training affiliated with professional, technical, or educational organizations?	Who provides the audio-visual equipment?
Is a course manual provided?	What is the instructor-to-student ratio?	Are course supplies provided by the training provider?
Does the provider offer certificates of completion?	What field expertise does the instructor have in the topical area?	
Can the course be customized to meet agency-specific needs?		
Does the class involve any testing?		
Are continuing education units offered?		
Can the training program travel or must the students travel to the instructor?		
For whom is the course intended?		
Course objectives		
Prerequisites		
Current courses		

Competency and Proficiency

Competency testing is designed to verify that an individual is able to conduct a specific task prior to its use in independent casework. Agency policy and user category determine which skills are required for competency.

Proficiency testing is the continual evaluation of agency personnel in the performance of tasks relating to their discipline.

Competency Testing

Competency testing can be conducted either at the end of training or in a modular format throughout the course of training.

- Required levels of skill and knowledge for a job category should be identified by the agency.
- A curriculum should be designed by the agency to provide the skills and information necessary for the agency's personnel to attain competency in those skills.

Proficiency Testing

Annual discipline specific proficiency testing is a means to confirm that a trained user is qualified to continue performing their assigned duties.

- This should be documented and confirmed with annual proficiency testing in the relevant subject matter.
- Discipline and job specific topics should be included in proficiency tests.
- There should be a mechanism for remediation if proficiency is not demonstrated.

Section 7

Best Practices for Forensic Video Analysis

***Previously released as "Recommendations and Guidelines for the Use of Forensic Video Processing in the Criminal Justice System and "Definitions, Recommendations and Guidelines for the Use of Forensic Video Processing in the Criminal* Justice System"**

OBJECTIVE

The objective of this document is to provide guidance regarding appropriate practices for performing a variety of processing and analytical tasks involving video submitted for examination.

SWGIT POSITION ON FORENSIC VIDEO ANALYSIS

Forensic Video Analysis (FVA) is a forensic science. In 2002, the International Association for Identification (IAI) formally recognized Forensic Video as a valid sub-specialty within the scientific discipline of Forensic Imaging (IAI Resolution 2002-12).

INTRODUCTION

Forensic Video Analysis is the scientific examination, comparison, and/or evaluation of video in legal matters.

With an increased prevalence and awareness of Closed Circuit Television (CCTV) surveillance, there are additional investigative opportunities. For example, in 1970, when Sterling Hall at the University of Wisconsin was bombed, there were no CCTV recordings in the area. Twenty-five years later, in 1995, investigators reviewed hundreds of video recordings related to the Oklahoma City bombing. Just six years later, in 2001, thousands of video recordings were examined by federal, state, and local agencies in relation to the terrorist attacks of 9/11. In 2005, the Metropolitan Police Service in the United Kingdom (New Scotland Yard) seized over 55,000 videotapes, hard drives, compact disks, digital video recorders, and other media in support of the investigation of the July bombings in London.

FORENSIC VIDEO ANALYSIS – GENERAL TASKS

The process of FVA can involve several different tasks, regardless of the type of video analysis performed. These tasks fall into **three** categories: Technical Preparation, Examination, and Interpretation. The general principles and procedures used in these tasks are the same regardless of the format or media in which the images are recorded. This includes both analog and digital media.

Technical preparation is the performance of tasks in advance of examination, interpretation, or output. There are a multitude of technical decisions within the various tasks. Technical preparation will affect further stages of FVA. Tasks may include the following; instrument calibration, visual inspections, media characterization, write protection, organization of files, and playback optimization.

Examination is the application of image science expertise to extract information from video. Examples may include the following; demultiplexing, decoding digital video and/or images, duplication, capture, reconstruction, format conversion, timeline sequence reconstruction, and standards conversion. Image and video enhancement, frame averaging, video stabilization, and other video processing activities intended to improve the visual appearance of features in a video are also examination tasks.

Interpretation in Video Analysis is the application of specific subject matter expertise to draw conclusions about video recordings or the content of those recordings. An example of the former is video authentication. The latter may include determining that an article of clothing appears different in a video than it does under normal lighting conditions due to the properties of the recording process (e.g. an Infrared (IR) negative image effect on natural fibers). Content-based interpretations may also include comparison analysis of such things as clothing or vehicles. If such a content-based interpretation leads to an identification, then it falls within the discipline of Image Analysis. For further information on Image Analysis, refer to SWGIT document "*Best Practices for Forensic Image Analysis*".

Note: Technical Preparation, Examination, and Interpretation are tasks, not job descriptions or roles. An individual may perform part of one task or a combination of multiple tasks within the organizational structure of any given activity. Each of these tasks requires its own training and qualifications. Proper methods and practices are necessary in order to get the most out of video evidence.

BEST PRACTICES

The following are guidelines that describe the SWGIT recommended best practices for forensic video analysis.

Evidence Management

Agencies should have documented procedures for the handling, transportation, and storage of evidence. Agencies should have chain of custody procedures in place and should follow these procedures.

Quality Control and Quality Assurance

Quality control and quality assurance policies and procedures should be implemented and documented. Technical and administrative peer reviews are integral components of quality control.

Security

There should be procedures in place to maintain the security of the working data, all notes, and other such analysis related materials to provide the level of security and privacy needed by the organization. For example, archived case related materials should be stored in a manner that limits access. The degree of access will be agency specific.

Infrastructure

Agencies should have sufficient space, equipment and facilities to adequately support the required quality and volume of work.

Work Management
Forensic Video Analysis is a labor intensive process. An upper limit on caseload should be established for every category of tasks.

Documentation
Agencies should establish standards for information included in, and the format for, reporting results.

Training, Competency, and Proficiency
Forensic Video Analysts and/or examiners are encouraged to review SWGIT "*Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System*", "*SWGIT/SWGDE Guidelines and Recommendations for Training in Digital and Multimedia Evidence*" and "*SWGIT/SWGDE Proficiency Test Program Guidelines*".

Analysts should have certification in their knowledge domain and associated forensic discipline, when such certification is appropriate and available. Note however, that the existence of an external professional certification program does not imply that it is necessary, sufficient, or appropriate.

Analysts should demonstrate competency in their discipline prior to being assigned unsupervised case work responsibilities. Analysts should remain proficient through continuing education, training, and peer review of examinations. Agencies should document competency, proficiency and continuing education for each analyst.

The analyst should demonstrate:

- An understanding of the scope of work and how it will be applied in the forensic environment;
- subject matter knowledge and competence;
- working knowledge of image and/or video processing and evaluation techniques;
- working knowledge of applications and tools utilized in the specific agency;
- working knowledge of SWGIT guidelines for capturing, storing, and processing image/video, including issues relating to topics such as data integrity and compression artifacts;
- understanding of legal precedent for the use of specific image and/or video processing techniques;
- knowledge of appropriate case work documentation.

Standard Operation Procedures (SOPs)
There should be Standard Operating Procedures (SOPs) in place for the tasks being performed. These SOPs should be agency specific, reflect the work flow, and be general enough to permit flexibility for the required tasks.

FORENSIC VIDEO ANALYSIS – WORK FLOW

The following describes a generalized sequence of actions involved in the analysis of video evidence and recommendations for their performance. This is not a training manual, nor a step-by-step methodology. These recommendations represent specific considerations to be addressed by the examiner. The exact sequence will be dependent upon the evidence submitted and the required examinations.

Chain of Custody

Throughout the entire FVA process chain of custody must be maintained as per agency policy.

Submission Review

A submission form should be completed for every case the examiner receives, regardless of what type of examination or service the requestor is seeking. ***See Appendix A for an example***.

Ensure examiner safety is maintained by determining whether biohazards such as blood or body fluids are present or other special handling is required.

Ensure that no other prior examination is required such as latent print or trace evidence.

At all times precautions should be taken to ensure video evidence is protected from external factors that may cause damage to the media or to the recorded signal contained on the media. (e.g. magnetic fields, static electric charges, electrical hazards)

Physical Inspection

Document the physical condition of the evidence. Physical inspection may include the following determinations:

- Physical damage to media or housing
- Contaminants (dirt, grease)
- Media characteristics (manufacturer, size, format)
- Device settings (hard drive jumper settings, device switch positions)
- Write protect status
- Existing labels or identifiers

If the media is an obvious copy, such as marked on the label as a duplicate, contact the requestor to determine if the original is available.

Any deficiency should be documented and resolved if possible before beginning any forensic analysis (e.g. splicing a broken or damaged tape, restoration into a new cassette housing).

Evidence Marking

Evidence needs to be marked per agency policy. Markings could include labelling with initials, ID number, case number or any other identifying information.

The ideal method for marking CDs and DVDs is with a non-solvent based felt-tip permanent marker designed to mark optical media.

Notations should be made in the clear inner ring as no data information is recorded in that area. Any identifying information (such as serial numbers) should be documented. Inappropriate marking or labelling methods may affect playback and could potentially damage the evidence.

- Never use a ballpoint pen, pencil or other sharp writing instrument when marking CDs and DVDs
- Do not use markers that contain solvents
- Do not use adhesive labels

Write Protection

Video recording media must be treated in such a manner as to be write protected in order to prevent modification of the media content.

For tape based media, record tabs should be removed, or slid to the write-protect position.

When possible, playback and file access from optical media should be performed with units incapable of record operations (e.g. CD ROM and DVD ROM drives). This may not be possible for media that has not been finalized.

A write blocking method, whether hardware or software, should be utilized for any media whenever possible.

For other forms of media storage, the manufacturer's recommendations regarding write protection should be followed.

Virus Scan

Virus scanning should be performed on any submitted media containing file based digital video recordings. Virus scanning is necessary to both ensure the integrity of the evidential video data, and to protect against malfunction and/or corruption to video processing hardware and/or software systems. The specific methods and software applications used for virus scanning, and remedial actions if a virus is found, will be determined by individual agencies and will be documented within an agency's SOPs.

Equipment Selection and Playback Optimization

Playback optimization and equipment selection is the process of determining the most suitable equipment and settings for analyzing the output video signal. This includes time base correctors (TBC), playback devices (including field-based VCRs), monitors, capture cards, multiplexers, vectorscopes, waveform monitors, and write blockers.

NOTE: Examiners should be aware that audio may be present within video recordings.

In order to ensure the best possible playback and viewing conditions of tape based evidence as it passes through the video processing chain, each piece of equipment and connections between equipment should be optimized. This will allow for the best evidence to be preserved, examined and further analyzed.

Key components of the video chain may be assessed using test patterns. For example, test patterns assist in the detection of noise and allow for adjustments to be made. A regular maintenance and cleaning schedule will assist in equipment reliability.

For tape based media

Prior to inserting videotape evidence into a playback device, ensure the equipment is functioning properly by inserting a non-evidentiary test tape of known signal and image quality. When playback of the evidentiary tape is less than optimal or signal dropouts occur, and the analyst suspects player idiosyncrasies 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 and/or camcorder unit. For example, head misalignment on the original recorder may produce a tape in which video playback is degraded or not viewable when played back on any unit other than the original recording device. Tracking adjustment may be necessary to optimize playback of the original video.

Analog based media usually requires visual examination of the individual recorded fields.

NTSC, PAL, and SECAM standards require appropriate equipment for viewing, conversion, and playback purposes to accommodate varying frame rates, aspect ratios and lines per frame.

Care should be taken to avoid extended playing or pausing of tape based media to prevent damage or degradation of the original video.

For file based digital video recordings

The minimum specifications provided by the relevant manufacturers to ensure proper playback, display resolution, and overall quality should be utilized when playing back file based digital video recordings. This applies to the particular video workstation hardware (e.g. processor, hard drive, memory, graphics card) and software (e.g. operating system, proprietary video player).

Digital video files and software that are recorded on removable media (e.g. CD-R, flash memory card) should be copied to the video workstation for playback, if possible.

For Digital CCTV (DCCTV), if possible obtain the pertinent video information in the native file format with the appropriate player. The analyst should be aware that different methods of playback and extraction (including universal players) may yield different results. When reviewing digital video using the proprietary software, the player or on-screen display (OSD) may affect the representation of the video. An incorrect display aspect ratio will not accurately depict the dimensions of the

actual recorded video. For example, objects that should have been recorded as circles may be depicted as ovals instead.

In some instances the original recording hardware, or equipment of the same make and model, may be necessary for playback.

In order to maintain image quality, the highest available signal path should be chosen for the devices in the FVA chain (e.g. s-video over composite).

Cable optimization can minimize electromagnetic interference, which can produce static or noise. Cable lengths should be as short as possible. Arrange any excess cable in an "S" or figure eight shape, avoiding loops and coils. Kinks or cables bent at sharp angles can damage cable connectors or the terminals of equipment.

Keep power cords away from audio and video cables if possible. Even shielded cables can be affected by power cords, which can cause electromagnetic interference and signal degradation. If cables must cross over power cords, these should cross at right angles.

Generation Determination

If during playback optimization there are indications that the submitted media is a copy, contact the submitter to obtain the original if it exists. Indications of an analog copy may include multiple head switching points viewed on an underscan monitor or an analog recording of a digital CCTV source. For digital media, a file playable in a universal player may be an indication that transcoding of the native file format has occurred.

Media Review

The submitted media for analysis should be reviewed. Information regarding recording method, time/date of incident, and problems in playback or viewing of the recording should be verified. Any observed discrepancies with the information documented in the submitted request should be noted.

A preliminary determination should be made with respect to the feasibility of the requested task (e.g. enhancement, comparison, duplication). If the analyst determines any additional tasks are necessary, these should be noted.

When identifying the area of interest for analysis, the following should be considered:

- There may be relevant information outside the area of interest requested by the submitter
- Details about the incident not directly related to the subject may be present. These include;
    - Images which could verify the time and/or place of the incident such as; clocks, signs, scoreboards
    - Potential witnesses or bystanders

Creation of a Work Copy and Verification

A working copy of the pertinent area of the recording should be created. This copy should be made to ensure the preservation of video data in the event of accidental corruption, erasure, or other unexpected damage or degradation to the original recording media. Examples of working copies are; copying of digital files from optical media to another medium (e.g. hard drive) and magnetic tape to digital files (uncompressed/lossless). The working copy should be digitally and/or visually verified as to content and quality.

For duplication purposes, a master copy should be created and all subsequent copies be made from this master. Where analog is concerned, this copy should be of the highest quality possible (VHS to VHS copying should be avoided whenever possible due to loss of quality).

Processing, Enhancement, and Examination

Video that has been processed should be documented. This documentation should include the order in which the processes were applied to ensure the integrity and the reproducibility of the results. Specific information and additional SWGIT recommendations related to video/image related enhancements may be found in the SWGIT document "*Best Practices for Documenting Image Enhancement*."

The following alphabetical list provides a brief discussion of various processing, enhancement, and examination techniques utilized in FVA, and specific recommendations for their use. Many of these techniques can be applied over an entire image (globally) or over a specific area (locally).

Brightness/Contrast

The specific settings for brightness and contrast filters should be set so that the level of detail for the area of interest is not adversely affected. Steps should be taken to ensure that clipping does not occur in the area of interest within the image. In a global brightness adjustment, areas of the image that are not pertinent may in fact be made less visible in order to optimize the pertinent area.

Color Correction

A known standard, such as MacBeth or SMPTE standardized charts, should be used when the most precise color correction is necessary. The chart should be captured under the same conditions, position and location as the original video and color balanced to a neutral tone. This color balance can be based on a visual display on a calibrated color monitor or by using the values displayed for this neutral toned object in the info palette of an image processing program.

Cropping/Resizing

Cropping/Resizing must not result in a misleading and/or inaccurate representation.

Deinterlacing

CCTV recordings may require deinterlacing to achieve the best image possible. This should be performed before any other process. Deinterlacing may be necessary in circumstances where display of the original interlaced signal results in

obscured or degraded image detail. For example, a VHS CCTV recording may contain noise only in the odd field of the video signal, due to a damaged or dirty record head on the recording VCR. Another example is motion between individual fields, as shown in Figures 1 and 2. In these cases, normal playback of the interlaced video may obscure image details in the recording. Therefore, deinterlacing the video signal and creating a processed version from a single field may result in clearer video images.

Figure 1. Interlaced Image

Figure 2. Deinterlaced Image

Demonstrative Comparison

Demonstrative Comparison occurs when multiple images are placed side-by-side for the purpose of visual comparison. This consists solely of preparing the composite exhibit. If the analyst indicates points of similarity or dissimilarity this represents an opinion about the content of the images; subject matter expertise and the principles of Image Analysis thus apply.

Ensure that all the displayed images have the correct aspect ratio and that significant features are approximately the same size.

To the degree practical, displayed images should depict the same composition including such features as camera to subject geometry (perspective), lighting, color rendition, focus, etc.

Analysis of the content of video images for the purpose of rendering a conclusion regarding the depicted subject(s) is beyond the scope of this document. This may include photogrammetric analysis or photographic comparison. For further information refer to SWGIT document "*Best Practices for Forensic Image Analysis*".

Demultiplexing

Demultiplexing may be accomplished through hardware or software tools.

Hardware based

Hardware based demultiplexing may allow for the decoding of date, time, and other camera information.

Hardware based demultiplexing can result in cropping and/or softening of the images. Also, the verification of dropped and/or incorrectly sorted frames may not be possible.

If available, the same make and model of multiplexer/demultiplexer used in producing the original recording should also be used for hardware demultiplexing. Third party multi-format hardware demultiplexers may also be used; however, there may be a variation in the results.

Optimal hardware configuration includes a monitor before the demultiplexing as well as a review monitor. This allows for simultaneous input and output monitoring.

Playback speed should be adjusted to run at an appropriate time-lapse rate in order to minimize the potential of the multiplexer skipping or dropping frames.

Figure 3.
Figure 3 shows a three-camera multiplexed combined signal and Camera 1 demultiplexed.

Software based
Software based demultiplexing may allow the analyst to verify that frames were correctly sorted and none were dropped.

This method typically uses image content to separate multiplexed cameras. Time and date information is often not displayed.

Pay particular attention to Pan-Tilt-Zoom (PTZ) cameras, and cameras with drastic lighting and/or scene changes, as they may cause difficulty for software based demultiplexing programs.

Noise Reduction
The best method to reduce noise will depend on the type of noise present in a given image or video. Frame averaging and single frame noise reduction techniques may be effective for different types of image noise.

Frame averaging is most often useful when there are multiple frames and no movement of the camera or the subject of interest.

Any single frame noise reduction technique will always be a trade off between reducing the noise and blurring or eliminating detail.

Sometimes no noise reduction is the best choice when enhancing an image in order to maintain fine details and textures.

Sharpening/Deblurring

Sharpening techniques can be useful to enhance edge detail. Since the fine detail of an image lies in the high frequencies, video analysts may want to boost the high frequencies of an image in an attempt to better visualize these details.

Some noise also exists in high frequencies. Any attempt to boost the details contained in the high frequencies of an image will also boost the high frequency noise. This amplification of noise is the major limitation in any sharpening technique applied to images and video.

Over sharpening an image, besides boosting the noise, may also result in an unnatural look to the enhanced image. Some sharpening processes may change the average brightness and/or contrast of an image.

VCR circuitry can contain a sharpening element. Care should be taken that this effect is willfully activated or deactivated and the consequences of it are understood.

Image restoration techniques, such as deblurring, can be used to reduce the motion, lens, and Gaussian blur.

A deblurring technique is not the same as a sharpening technique. However, if no deblurring tool is available, a sharpening tool may be effective.

Speed Adjustment

Speed adjustment of forensic video is typically performed for the following reasons:

- To convert the playback speed of time lapsed video recordings to a real-time rate.
- To slow the playback speed of video to a less-than-real-time rate ("slow motion").

This is often done to facilitate the viewing of images and action details occurring in the original recording.

Speed adjustments are made by varying the playback frame rate, and may be accomplished through hardware (e.g. time-lapse VCR) or video-processing software (e.g. motion effects).

Timeline Sequencing

Timeline sequencing can be an effective way to show subject movement through a scene or a series of events. Every pertinent image should be included in the timeline displayed or verified time/date information and/or frame numbers. Scene content may also be useful in verifying the proper sequence of recorded images. Examples of scene content may include movement of vehicles or people. Images used in timeline sequencing may come from multiple cameras at one location or multiple locations. Proper documentation when performing any of these methods is essential.

Video Stabilization

Video Stabilization is typically performed at the field level, and may be either an automatic or manual process. This is usually performed prior to attempting noise reduction using inter-frame adding or averaging operations.

Figure 4.

Figure 4 shows an original sequence of images captured with a handheld VHS-C camcorder. The vehicle is moving within the frames as the result of camera jitter and vehicle movement. To correct for this, an area of interest is defined within an image that subsequent video frames will be aligned with.

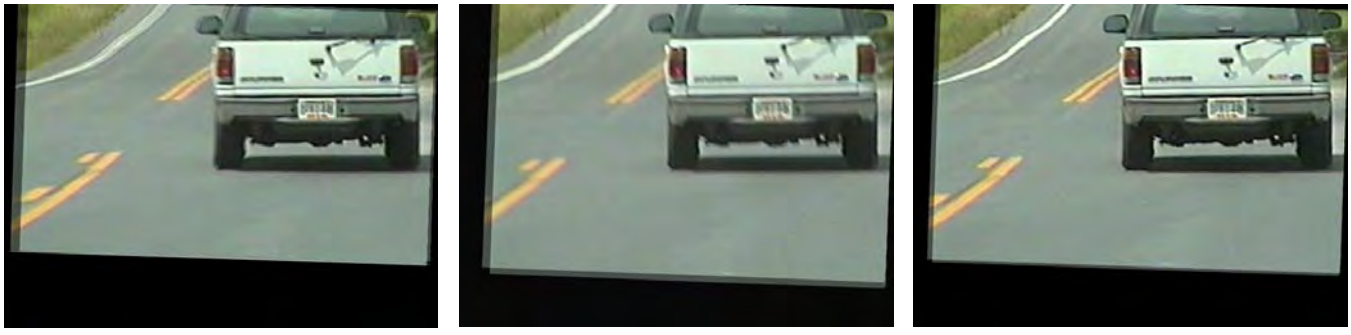


Figure 5.

Figure 5 shows the processed video sequence. The vehicle has been stabilized, by aligning the frames to the previously selected area of interest. Notice that the frames are being moved (horizontally and vertically) and rotated to align them.

Output
Results can be output to media, such as videotape, prints, write once optical media (e.g. DVD, CD), hard drive, etc., for return to the requestor. Media should be write protected, when possible. Rewritable optical media (e.g.DVD-RW, CD-RW) should not be used.

Any notations added to the final image results, such as agency logos, text, case information, or examiner markings, should not obscure the pertinent area.

The type of output images (video, stills, or a combination) is dependent upon what best illustrates the content, quality, and events to be depicted in the final product. When deciding what to output, consider the intended use and the quality of the images available as well as the needs of the requestor for playback and courtroom presentation.

If adjustments for pixel aspect ratio are required for printing, in most cases, they should be done after all image processing and enhancement is performed. Prior to output, ensure the pixel aspect ratio is correct for the chosen media. If the aspect ratio is not correct, the output results may not be proportionate (width to height) and will not be an accurate representation of the original image.

Durability, longevity and quality of prints produced should be considered. Whenever possible, the printer manufacturer's recommendation for ink, paper, storage, maintenance, and settings should be followed. The most important aspect of printing is that the printed still image files remain a true and accurate representation of the original event.

When outputting to digital media, be aware that several factors can reduce output quality. These include:

- High compression rates
- Long record times
- Poor quality equipment and media
- Incorrect settings

Verification
Any output should be verified to check that all content was transferred successfully and that the quality of the output accurately reflects the results of the examination and/or analysis.

The analyst should be aware that there may be compatibility issues between the output produced and the playback device. Ideally, output should be verified on multiple systems to ensure optimal playback compatibility.

After verification, the original media and all processed output should be properly labeled, sealed and packaged according to your agency's SOPs.

Appendix A – Video Submission Form

SUBMISSION OF VIDEO EVIDENCE

Date		Agency Case #		
Submitter Name				
Agency				
Offense		Phone #	Cell #	
VICTIM (or SUBJECT)		**RACE**	**SEX**	**DOB**
1				
2				
SUSPECT		**RACE**	**SEX**	**DOB**
1				
2				

Brief Details of Case (Attach Report if Necessary)

_____
_____
_____
_____

Examinations Requested

_____
_____
_____
_____

CCTV System Information

Digital Video Recorder Make, Model, Serial Number _____

PC Based Stand Alone Networked (Circle One)

Playback software name and version_____

Software provided with evidence YES or NO (Circle One)

System and/or Software Password _____

System Settings:
Image Quality (i.e. high, medium, low) _____
Frames per second (fps)/pictures per second(pps) _____
Image/Frame recorded size (e.g. 320 x 240) _____
Can it be determined if any cameras are alarm or motion triggered?_____
Number of hard drives, storage capacity of each _____
System firmware version _____

Other available system settings (e.g. event log)_____

Analog Video Recorder Make, Model, Serial Number_____

VHS SVHS Other _____ (Circle One)

What record mode was the system? (Circle One) 2 hour, 6 hour, 12 hour, 24 hour, 48 hour
72 hour, Other _____ Unknown

Multiplexer YES or NO Make and Model _____

Basic Information

Does the recorded date/time accurately represent the time of day? (circle) YES or NO

Date/Time displayed _____

Actual date/time _____

# of Camera/s _____ Active # of cameras

Camera make and model _____

Are any cameras infrared-sensitive and if so identify _____

Is audio being recorded? _____

Is a copy of the most current maintenance/service log attached? (circle) YES or NO

Other Information: _____
_____

Scene Contact Information

Scene Address _____

Hours of operation_____

Scene point of contact _____Telephone: _____

CCTV system point of contact _____ Telephone: _____

Please provide a sketch of the scene indicating camera position and placement.

Submitted By _____ **Print Name**_____
Signature

13) Images from separate incidents should be clearly delineated by a change of storage media or by proper documentation.

14) As soon as practical, media should be downloaded to an approved storage medium. Refer to SWGIT document Section 13, "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*".

Step 3: Use of Portable Computers/Storage Devices (Optional)

1) Connect camera or removable media to the device according to manufacturer's specifications.

2) When using a computer, create and name a file folder on the computer's hard drive to receive original image files. The camera or software may require unique file folder names for each download. Care should be taken not to overwrite existing image files from previously downloaded media. Some cameras reset their file counters whenever media is changed.

3) Prepare subdirectories for receiving downloaded images from camera or media. Create and name a subdirectory, using unique naming convention, in sequential order.

4) Copy all original files to appropriate subdirectory.

5) Verify that all images have been copied into the correct subdirectory.

6) Take necessary precautions and steps to preclude accidental deletion of files.

7) Removable media should not be erased in the field; however, if it becomes necessary redundant copies should be made and Agency SOP's should be followed.

Section 8

General Guidelines for Capturing Latent Impressions Using a Digital Camera

Introduction

The purpose of this document is to describe the proper documentation of latent print evidence by qualified personnel when using a digital camera.

The procedures described in this document are made in accordance with current SWGFAST guidance, see SWGFAST document "*Standard for Friction Ridge Digital Imaging (Latent/Tenprint)*"[1], as well as National Institute of Standards and Technology (NIST) standard, "*NIST Special Publication 500-271 ANSI/NIST-ITL-2007*"[2], both documents specify 1000 pixels per inch (ppi) at 1:1 as the minimum nominal resolution for latent print evidence.

Equipment

It is recommended that a professional digital camera kit consist of, at a minimum, the following items:

- Professional digital single lens reflex (SLR) camera
- Fixed focal length macro lenses
- Lens filters
- Dedicated electronic flash capable of off-camera operation
- Remote shutter release
- Sturdy tripod capable of various angles and positions
- Variety of light sources (e.g. flood lights, flashlights, Alternate Light Source [ALS])
- Digital storage media (format the media in the camera prior to each use)
- Graduated scaling devices (e.g. millimeters)
- Photographic log/notes

[1] www.swgfast.org
[2] http://fingerprint.nist.gov/standard

Optional Equipment

- Portable computer with appropriate software for downloading and viewing images at the scene
- Appropriate cables and connections (e.g. USB, Firewire)
- Card readers (e.g. Secured Digital [SD], Compact Flash [CF])
- Independent portable storage devices

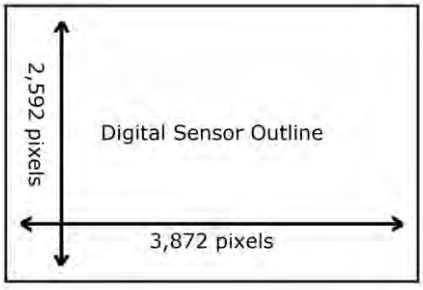
Procedure

Step 1: Prior to Initial Use

1) Determine the maximum field of view in which a minimum of 1000 ppi may be achieved.
    a. Refer to the effective pixel dimensions of the camera's sensor as stated by the manufacturer (e.g. 3872x2592 pixels).

    b. Divide each dimension by 1000 ppi which, in this example equals 3.872 inches x 2.592 inches. This makes the maximum field of view approximately 3¾ inches x 2½ inches. To convert inches to millimeters, multiply inches by 25.4. To achieve maximum detail, it is best practice to fill the frame with the impression.

    c. Not all camera viewfinders cover 100% of the capture area. Take a test image of scales across the vertical and horizontal axis to determine coverage of viewfinder.



2) Review Standard Operating Procedures (SOPs) detailing how the equipment is to be used.

Step 2: Camera Set Up and Use

1) Verify camera settings that include but are not limited to time/date stamps, image file format and image size. It is recommended to capture using no compression or lossless compression (e.g. RAW or TIFF). Refer to SWGIT document Section 19, "*Issues Relating to Digital Image Compression and File Formats*".

2) Prepare photographic log or worksheet per agency policy.

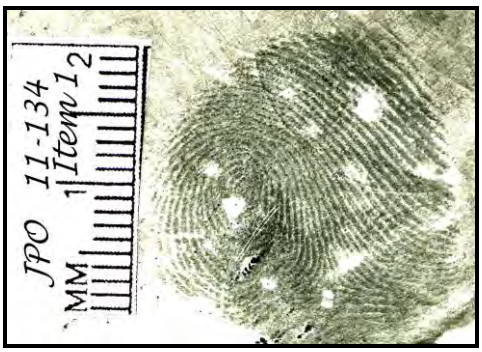
3) When appropriate (e.g. crime scene), capture overall view of impression area without a scale using proper lighting.

4) Capture overall view of impression area with a scale, using proper lighting.

5) Mount camera on tripod or copy stand with camera at a 90-degree angle to the impression. Caution should be taken when using a magnetic level. Avoid contact or proximity of magnetic fields with storage media and camera because these fields may erase stored images and data and interfere with image capture.

6) Light impression appropriately.

7) Place scale on the same plane and as close as possible to impression without obscuring detail. Do not exceed the maximum field of view established in *Step 1*. The scale may contain the following information based on agency procedures:
   a) Case number or unique identifier
   b) Date
   c) Initials
   d) Source
   e) Process used
   f) Location/orientation



8) Select appropriate camera settings based on the previous equipment testing. **Note:** Manual mode or aperture priority is recommended.

9) Capture impression for optimum quality, evaluate image and then bracket exposures as needed.

10) If images are unacceptable, re-photograph.

11) Repeat steps 8 through 11 for each lighting position used for each impression.

12) After the evidence is processed for impressions, follow steps 3 through 11 as appropriate for all latent prints developed.

13) Images from separate incidents should be clearly delineated by a change of storage media or by proper documentation.

14) As soon as practical, media should be downloaded to an approved storage medium. Refer to SWGIT document Section 13, "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*".

Step 3: Use of Portable Computers/Storage Devices (Optional)

1) Connect camera or removable media to the device according to manufacturer's specifications.

2) When using a computer, create and name a file folder on the computer's hard drive to receive original image files. The camera or software may require unique file folder names for each download. Care should be taken not to overwrite existing image files from previously downloaded media. Some cameras reset their file counters whenever media is changed.

3) Prepare subdirectories for receiving downloaded images from camera or media. Create and name a subdirectory, using unique naming convention, in sequential order.

4) Copy all original files to appropriate subdirectory.

5) Verify that all images have been copied into the correct subdirectory.

6) Take necessary precautions and steps to preclude accidental deletion of files.

7) Removable media should not be erased in the field; however, if it becomes necessary redundant copies should be made and Agency SOP's should be followed.

Section 9

General Guidelines for Photographing Footwear and Tire Impressions

***Previously released as " General Guidelines for Photographing Tire Impressions" and "General Guidelines for Photographing Footwear Impressions" ***

Introduction

The purpose of this document is to describe the proper method of photographing footwear and tire impression evidence by qualified personnel.

Recommended Equipment Includes:

- Professional camera, minimum 35mm or digital SLR with a minimum eight (8) megapixel native resolution, capable of interchangeable lenses, manual override for exposure and focus
- Detachable flash with a six (6) foot extension cord or a flash with remote capabilities to allow for side lighting
- Professional quality lens capable of filling the frame with the impression and having minimal distortion (see *Technical Note* below)
- Remote shutter release
- Sturdy tripod mount capable of adjustable angles and positions
- Artificial light sources *(*e.g., floodlights, flashlights)
- Level/Angle finder
- Suitable storage media
- Flat rigid scales
- Measuring tape (Tire Impression)
- Photographic log
- Reflector
- Device for blocking ambient light

Procedure for Impression Photography[1]

A typical standard operating procedure should include the following:

1) Locate visible impressions to be photographed.

2) Prepare photographic log or worksheet as per agency policy.

3) Select suitable film or digital media.

4) Once the overall, midrange and close-up views of the area have been documented without scales and markers, photograph the overall and midrange views of the area with identifying markers and scales using appropriate lighting.

5) To document details of the impression for examination, photograph close-up views of the impression with identifiers and scales using appropriate lighting. Each image must fill the frame with the impression and scales:

   a) Mount camera on a tripod with the focal plane parallel to the impression.

   b) Manually focus on the bottom of the impression and close aperture to optimize depth of field (e.g. generally two stops below the largest f-stop or smallest aperture opening).

      Note: The scale should be at the same level plane as the impression.

   c) Set camera to the highest resolution using uncompressed or lossless compression. (e.g. RAW or TIFF).

   d) (Footwear only) In addition to close-up photographs of the entire impression, take multiple overlapping exposures mapping the entire impression. Light each overlapping section of the impression to bring out maximum detail. Separate close-up images of the heel and toe box area should be taken. Each image will contain an identifier and scale.

   e) (Tires only) Take multiple overlapping exposures of the entire impression. Light each overlapping section of the impression to bring out maximum detail. For a long tire impression, a series of overlapping photographs of 12 inches each should be taken. For continuity and orientation purposes, a tape measure should be positioned flat and extended along the side of the entire length of the impression. Each image will contain an identifier and scale in addition to the tape measure.

   f) Multiple exposures using various settings/bracketing and lighting techniques may be required. A minimum of three images should be taken with oblique

[1] Reference SWGTREAD Guide for the Forensic Documentation and Photography of Footwear and Tire Impressions at the Crime Scene

lighting at least 100 degree increments around the entire footwear impression. Height of the light source should be sufficient to capture the detail in the bottom of the impression. Distance of the light source should be established to ensure even lighting. If the impression is in a brightly lit area, such as an area directly lit by the sun, it may be necessary to shade the impression.

g) If the impression is processed (e.g. with fingerprint powder or chemicals), re-photograph after each process.

Technical Note: Lens Distortion

When capturing images for comparative analysis, it is important to minimize distortion. Professional quality fixed focal length (normal) lenses have significantly less optical distortion. The issues related to using variable focal length (zoom) lenses are highly complex. Due to their construction, they commonly produce distortions depending on the focal length. Wide angle settings can amplify these distortions and will affect a forensic examination. In most cases, distortions can be minimized when the focal length is set toward the middle range of the lens. Care should be taken when using variable focal length lenses.

Figure 1 demonstrates this point. In this example, both images were taken with the same camera and a variable focal length lens. The sole of the shoe has a circular pattern in the heel. The image on the left was set for a 50 mm focal length. The image on the right was set for an 18 mm focal length. Notice the circular area on the right is elongated.

Figure 1. 50 mm

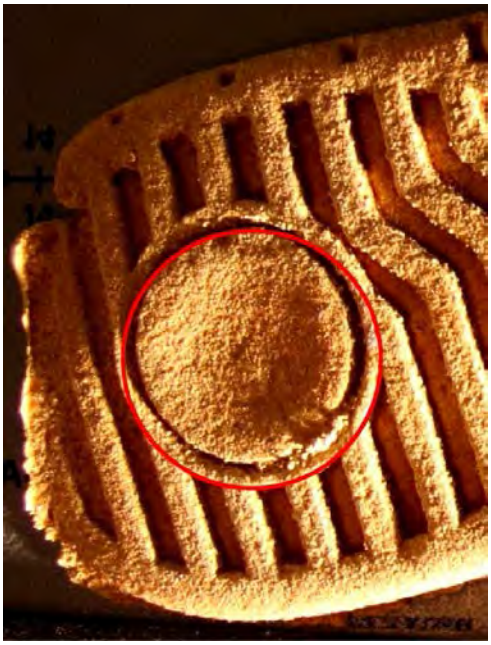


Figure 1. 18 mm

In addition to the design of the lens, some camera manufacturers address distortion through firmware and software updates. Because of the complexity of this issue, the simplest way to determine if your equipment is performing properly is to test it. Your specific setup can be tested using the following method:

- Ensure the camera has the latest version of firmware
- Mount camera on a tripod or copy stand
- Using a leveling device, ensure that the camera's sensor plane is parallel to the target to prevent keystone effect
- Lay down a sheet of graph paper or target grid
- Fill the frame with the target
- Square the lines in the viewfinder
- Using consistent camera settings and lighting, make an exposure at each focal length graduation and note the value
- Repeat this process though the range of the lens graduations
- From the resulting images, identify the focal length where no visible distortion occurs. Figures 2, 3 and 4 below demonstrate what you should be looking for.

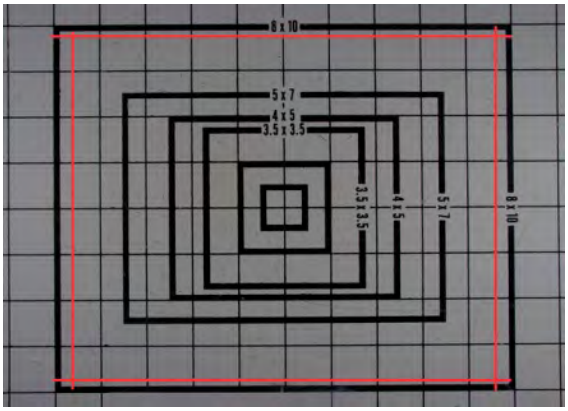


Figure 2. Minimal Distortion

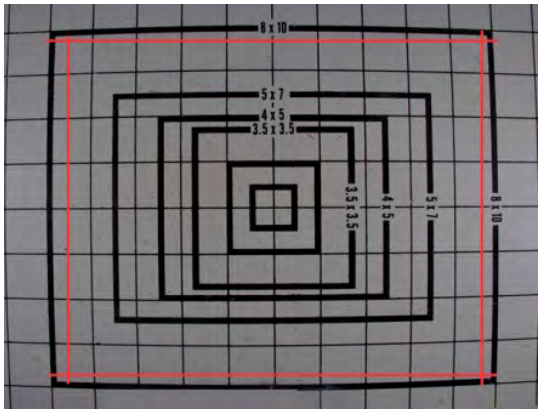


Figure 3. Barrel Distortion

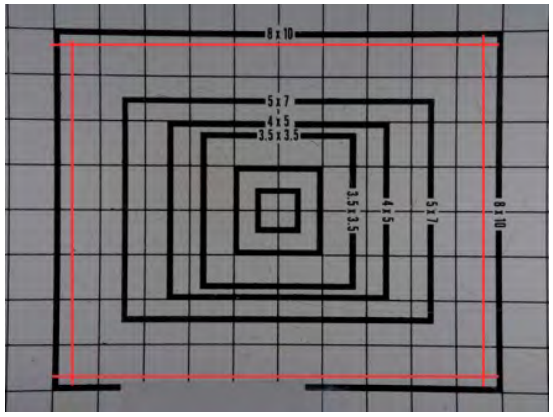


Figure 4. Pincushion Distortion

Section 10

General Guidelines for Photographing Footwear Impressions

Introduction

The purpose of this document is to describe the proper method of photographing footwear evidence by qualified personnel.

Recommended Equipment

- Professional camera, minimum 35mm or digital SLR with a minimum eight (8) megapixel native resolution, with interchangeable lenses, manual override for exposure and focus.
- Detachable flash with a six (6) foot extension cord or a flash with remote capabilities to allow for side lighting.
- Macro lens capable of filling the frame with the footwear impression
- Remoter shutter release
- Sturdy tripod mount capable of various angles and positions
- Artificial light sources (e.g., floodlights, flashlights)
- Level/Angle finder
- Suitable B&W and color negative film or digital storage media
- Flat rigid scales
- Photographic log
- Reflector
- Device for blocking ambient light

Procedure for Footwear Impression Photography[1]

A typical standard operating procedure should include the following:

1. Locate the visible impressions to be photographed.

[1]Reference SWGTREAD Guide for the Forensic Documentation and Photography of Footwear and Tire Impressions at the Crime Scene

2. Prepare photographic log or worksheet as per agency policy.

3. Select suitable film or digital storage media.

4. Once the overall, midrange and close-up views of the area have been documented without scales and markers, photograph the overall and midrange views of the area with identifying markers and scales using appropriate lighting.

5. To document details of the impression for examination, photograph close-up views of the impression with identifiers and scales using appropriate lighting. Each image must fill the frame with the impression and scales:

    a) Mount the camera on a tripod with the focal plane parallel to the impression.

    b) Manually focus on the bottom of the impression and close aperture to maximize depth of field (e.g. set aperture to f16 or f22).

    c) If using digital camera, set camera to the highest resolution and uncompressed or with lossless compression (e.g. RAW or TIFF).

    d) In addition to the close-up photographs of the entire impression, take multiple overlapping exposures mapping the entire footwear impression.

        - If the impression is in a brightly lit area, such as an area directly lit by the sun, it may be necessary to shade the impression.

        - Light each overlapping section of the impression to bring out maximum detail. Separate close-up images of the heel and toe box area should be taken.

    e) Multiple exposures using various settings/bracketing and lighting techniques may be required. A minimum of three images should be taken with oblique lighting at least 100 degree increments around the entire footwear impression. Height of the light source should be sufficient to capture the detail in the bottom of the impression. Distance of the light source should be established to ensure even lighting. If the impression is in a brightly lit area, such as an area directly lit by the sun, it may be necessary to shade the impression.

    f) If impression is processed (e.g. with fingerprint powder or chemicals), re-photograph after each process

Section 11

Best Practices for Documenting Image Enhancement

INTRODUCTION

A fundamental goal of this and other Scientific Working Group on Imaging Technology documents is to ensure the production of quality forensic imagery for use as evidence in a court of law. The specific purpose of this document is to describe best practices for documenting image enhancement used in the criminal justice system and to provide laboratory personnel with instruction regarding the level of documentation that is appropriate when performing a variety of enhancement operations on still images, regardless of the tools and devices used to perform the enhancement.

Accurate documentation is necessary to satisfy the legal requirements for introducing forensic images as evidence in a court of law and to allow other professionals to understand the enhancement and produce comparable results.

The general principles and procedures used are the same regardless of the format or media in which the images are recorded. Therefore, in this document the word *image* refers to any image recorded on any media (e.g., conventional photographic, electronic, magnetic, or optical media, etc.).

Note: The Best Practices described below are predicated on the assumption that an original file/image that has been subjected to processing be preserverd.

IMAGE ENHANCEMENT POSITION

Image enhancement has been used in forensic applications since the 1840s and is an accepted practice in forensic science, regardless of whether it is performed in a traditional wet chemistry darkroom or in a laboratory equipped only with electronic devices, such as computers, scanners, and/or video capture systems.

IMAGE CATEGORIES

The degree to which procedures used in image enhancement should be documented will depend on the intended end use of the image. Furthermore, the nature of such documentation will depend on the procedures used.

The Scientific Working Group on Imaging Technology recognizes two fundamental end uses for images encountered in the legal system.

Category 1

Category One images are used to demonstrate what the photographer or recording device witnessed but are not analyzed by subject matter experts. These can include, but are not limited, to the following:

- General crime scene or investigative images

- Surveillance images
- Autopsy images
- Documentation of items of evidence in a laboratory
- Arrest photographs, such as mug shots

Category 2
Subject matter experts use Category Two images for scientific analysis. These can include, but are not limited, to the following:

- Latent prints
- Questioned documents
- Impression evidence
- Patterned evidence
- Category 1 images to be subjected to analysis

ENHANCEMENT TECHNIQUES

Basic
Basic image enhancement techniques are those used to improve the overall appearance of the image. When one visually compares an original image to that same image after basic enhancement, a trained professional should be able to produce comparable results even in the absence of documentation of specific parameterization or software settings. These techniques can be applied over an entire image and in localized areas in an image. They include, but are not limited to, the following:

- Brightness and contrast adjustment, including dodging and burning
- Resizing (file interpolation)
- Cropping
- Positive to negative inversion
- Image rotation/inversion
- Conversion to grayscale
- White balance
- Color balancing and/or color correction
- Basic image sharpening and blurring (pixel averaging)

- De-interlacing

There can, of course, be both simple and complex ways of doing certain task. For example, there may be many ways to create grayscale representations of color images ("conversion to grayscale"). When complex techniques are used, they should no longer be considered "basic".

Advanced
While advanced image enhancement techniques may also be applied to improve the overall appearance, they are often also used to extract specific information contained in the image. These techniques which are not easily approximated by a trained professional without documentation of specific parameterization or software settings. The techniques include, but are not limited, to the following:

- Frame averaging
- Fourier Analysis (including the use of FFT)
- Deblur
- Noise reduction
- Image restoration
- Color channel selection and subtraction
- Perspective control and/or geometric correction
- Advanced sharpening tools, such as unsharp mask

DOCUMENTATION – What is needed

Category 1 Images
When enhancing Category One images, one need only document the techniques with a standard operating procedure that describes the typical enhancement processes. If an original image previously treated as a Category One image is to be subjected to scientific analysis, it becomes a Category Two image.

Category 2 Images
The use and sequence of any enhancement techniques in Category Two images should be documented in every case.

Documenting image enhancement steps should be sufficient to permit a comparably trained person to understand the steps taken, the techniques used, and to extract comparable information from the image. Documenting every change in every pixel value is discouraged because it adds nothing of value to the analysis.

Exploratory enhancement operations not incorporated in the final image do not need to be documented. Test prints and/or intermediate images resulting from a variety of techniques not incorporated into the final image should be discarded.

Minimum requirements for documentation of advanced techniques include identifying the software application and/or techniques as well as the settings and parameters used. Automated processes, such as running user-defined macros, require only documenting usage if the process is defined in the agency documentation.

DOCUMENTATION – How to do it

Documentation can be recorded in a variety of ways including hand-written notes, electronic recording, or through the use of automated logging tools, or incorporated into the final report.

The following examples are intended to represent the documentation level appropriate for Category Two images. Following these recommendations will help fulfill the requirements for the admissibility of images in a court of law. In addition to the examples below, a sample SOP which includes the use of automated logging is provided in the appendix.

Examples:

Brightness and contrast and/or contrast adjustment

I printed the Q5 image using Kodabromide II grade 4 RC paper. The tread area was burned into increase detail.

Unsharp mask (strength, distance, threshold)

In software application X, version N, I used unsharp mask at strength = 100%, with distance = 1.5 pixels, and threshold of 3 levels.

Multiple image averaging (number of images used, which images used, individual image weights)

I averaged 4 images (Q1_01.tif; Q1_02.tif; Q1_03.tif; and Q1_04.tif) with equal weighting

Fourier Analysis (Fast Fourier Transform – FFT) (Identify region of interest, and edits performed on spectrum, such as spike cut, spike boost, low pass filter and high pass filter)

Selected the region of interest to include the vehicle, performed a forward FFT operation, edited the spectrum, using spike cut on the repetitive signal, then performed the inverse Fourier transform.

Noise reduction (Type, such as despeckle, Gaussian blur)

I reduced noise in the image by applying an IIR Gaussian blur.

Color channel selection and removal

I removed the red channel by deleting it.

Perspective control and/or geometric correction (scale, rotation or degree, perspective, skew)

I rotated the image 90 degrees clockwise.

User-defined macro (macro name)

In Adobe Photoshop Version 7.0, I used Action Video Process 1 (defined in agency documentation).

Appendix
SAMPLE
STANDARD OPERATING PROCEDURE

Title: Latent Print Image Processing **Approval Date** _____

_____
Reviewer Signature

_____ _____
Technical Leader Signature **Forensic Services Director Signature**

Purpose: To establish a list of actions to enhance latent print images requested by latent print analysts.

Procedures:

1. Log into the agency-approved software application for processing latent prints.

2. Select the case containing the images to be processed.

3. On the menu bar, click Image, Enhance. The program will make a copy (working image) of the original image and import the copy and the enhanced image history into the agency-approved enhancement software application.

4. Process the working image using enhancement techniques. All processes applied to the working image are recorded using the enhanced image history tool. Approved processing techniques for use on working images are those that have direct counterparts in traditional darkrooms including brightness and contrast adjustment, dodging and burning, and color balancing. The tools include Brightness/Contrast, Levels, Curves, Color Balance, Hue/Saturation, and Invert. Using Mode, Channels, and Fast Fourier Transform filters (FFT) are acceptable. The following tools are prohibited: Rubber Stamp, Airbrush, Paintbrush, Paint Bucket, Eraser, and Blur.

5. After the working image is processed and the processes are recorded, save the changes to the processed working image. Import the processed working image back into the latent print processing application.

6. The operator may now process additional images, export a processed image for printing, or exit the application.

Safety Considerations: None.

Limitations: Based on existing equipment and technology.

Quality Control: Perform appropriate equipment maintenance to ensure proper capacity and quality performance.

Literature References: User Manuals.

Section 12

Best Practices for Forensic Image Analysis

OBJECTIVE

The objective of this document is to provide personnel with guidance regarding practices appropriate when performing a variety of analytic tasks involving images, regardless of the knowledge domain that is the subject of analysis.

SWGIT POSITION ON FORENSIC IMAGE ANALYSIS

Forensic image analysis is a forensic science. It has been practiced since the early days of photography, dating at least to 1851 when Marcus A. Root conducted the first documented example of Forensic Image Authentication. Through microscopic examination, Root revealed that the color daguerrotype "process" promoted by Reverend Levi Hill was actually the product of hand coloring, not a breakthrough in photographic science (Davis, Photography, Brown & Benchmark, 1995). In addition to being an accepted scientific practice in the forensic community, image analysis is also recognized in other disciplines including medicine, intelligence, geology, astronomy, agriculture, and others.

INTRODUCTION

Forensic Image Analysis is the application of image science and domain expertise to interpret the content of an image and/or the image itself in legal matters. Major subdisciplines of Forensic Image Analysis with law enforcement applications include: Photogrammetry, Photographic Comparison, Content Analysis, and Image Authentication.

The process of Forensic Image Analysis can involve several different tasks, regardless of the type of image analysis performed. These tasks fall into three categories: Interpretation, Examination, and Technical Preparation. These tasks are described below. The general principles and procedures used in these tasks are the same regardless of the format or media in which the images are recorded. Therefore, in this document the word "image" refers to any image recorded on any media (e.g., film, electronic, magnetic, or optical media, etc.).

FORENSIC IMAGE ANALYSIS – GENERAL TASKS

Interpretation

Interpretation, as used here, is the application of specific subject matter expertise to draw conclusions about subjects or objects depicted in images. Examples include a podiatrist drawing conclusions about foot shape from an image, a shoeprint expert drawing conclusions about the provenance of a shoe, or a military expert drawing conclusions about force distribution from remote sensing data.

Examination

Examination is the application of image science expertise to the extraction of information from images, the characterization of image features, and the interpretation of image structure. Examples include watermark detection, steganalysis, extraction of Photo Response Non-Uniformity signature and image alteration evaluation, as well as the development of case-specific image exploration strategies. Image enhancement, image restoration, and other image processing activities intended to improve the visual appearance of features in an image are examination tasks.

Technical Preparation

Technical preparation is the performance of tasks such as preparation of evidence or images for examination, interpretation, or output. Note that there is a wide gamut of technical decision making within the various responsibilities covered by technical preparation actions. Some responsibilities may involve minimal technical decision making, such as feeding paper into a preset sheet fed scanner that has been previously calibrated. Some responsibilities may involve a great deal of technical decision making, such as determining appropriate color balance, sampling during acquisition, or output resolution.

Note: Interpretation, Examination, and Technical Preparation are tasks, not job descriptions or roles. An individual may perform part of one task or a combination of multiple tasks within the organizational structure of any given activity. Each of these tasks requires its own training and qualification.

FORENSIC IMAGE ANALYSIS – SPECIFIC AREAS OF ANALYSIS

Photogrammetry

"Photogrammetry is the art, science, and technology of obtaining reliable information about physical objects and the environment through the processes of recording, measuring, and interpreting photographic images and patterns of electromagnetic radiant energy and other phenomena." [from "The Manual of Photogrammetry, 4th Edition, 1980, ASPRS]. In forensic applications, photogrammetry (sometimes called "mensuration") most commonly is used to extract dimensional information from images, such as the height of subjects depicted in surveillance images and accident scene reconstruction. Other forensic photogrammetric applications include visibility and spectral analyses.

Figure 1 illustrates an example of a photogrammetric analysis conducted to determine the height of a subject depicted in a bank robbery surveillance photograph.

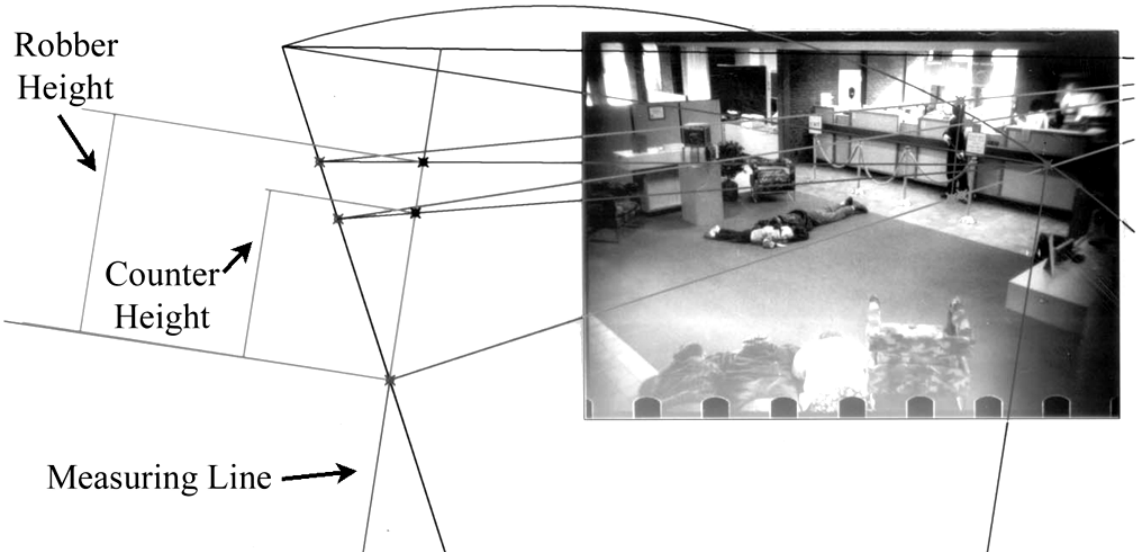


Figure 1.

Photographic Comparisons

Photographic comparison is an assessment of the correspondence between features in images and known objects for the purpose of rendering an expert opinion regarding identification or elimination (as opposed to a demonstrative exhibit). Examples of photographic comparisons include, but are not limited to:

- A facial comparison between an unknown subject depicted in a surveillance image with an identified suspect; (see www.FISWG.org for more information)
- The comparison of objects such as vehicles depicted in surveillance images with those recovered in an investigation;
- The comparison of a questioned image with a known camera to determine if the image was captured using that camera.

Photographic comparisons are frequently referred to as "side-by-side" comparisons since they usually involve a comparison of class and individualizing characteristics in imagery. The scientific basis and technical processes involved in photographic comparisons are comparable to those used in other forensic disciplines such as fingerprint analysis. ACE-V (Analysis, Comparison, Evaluation – Verification) is a common protocol used to perform photographic comparisions. Statistical analysis can be used as a component of the evaluation stage of ACE-V, but is not required.

Figure 2 illustrates demonstrative exhibits from a facial comparison exam, in which ACE-V was used to individualize the subject as the same person in both images.

Figure 2.

Figure 3 illustrates a demonstrative exhibit from a clothing comparison examination, in which ACE-V was used to individualize the camouflage jacket as the same one in both images.

Figure 3.

Content Analysis

Content analysis, within the context of forensic image analysis, is the drawing of conclusions about an image. Targets for content analysis include, but are not limited to:

- the subjects/objects within an image;
- the conditions under which, or the process by which, the image was captured or created;
- the physical aspects of the scene (e.g., lighting or composition); and/or
- the provenance of the image.

Examples include vehicle license plate number identification, patterned injury analysis, correlation of injuries inflicted in an image sequence with autopsy results, determination of the presence of computer-generated imagery in an alleged "snuff" film, and determination of the type of camera used to record a specific image.

Image Authentication

Image Authentication is verification that the information content of the analyzed material is an accurate rendition of the original data by some defined criteria. These criteria usually involve the interpretability of the data, and not simple format changes that do not alter the meaning or content of the data.
Examples include:

- Determining the degradation of a transmitted image;
- Determining whether a video is an original recording or an edited version;
- Evaluating the degree of information loss in an image saved using lossy compression.
- Determining whether an image contains feature-based modifications such as the addition or removal of elements in the image (e.g., adding bruises to a face).

BEST PRACTICES

The following are guidelines that describe the SWGIT recommended best practices for the performance of forensic image analysis.

Evidence Management

Agencies should have documented procedures for the handling, transportation, and storage of evidence. Agencies should have chain of custody procedures in place and should follow these procedures.

Quality Control and Quality Assurance

Quality control and quality assurance policies and procedures should be implemented and documented. Technical and Administrative peer reviews are integral components of quality control.

Security

There should be procedures in place to maintain the security of the working data, all notes, and other such analysis-related materials to provide the level of security and privacy needed by the organization. For example, archived case-related materials should be stored in a manner that limits access. The degree of access will be agency-specific.

Infrastructure

Agencies should have sufficient space, equipment and facilities to adequately support the required quality and volume of work.

Work Management

Because forensic image analysis is a labor-intensive process, an upper limit on caseload should be established for every category of tasks.

Documentation

The practitioner should have available documentation that describes and justifies the use of any method involved in the analysis. Such documentation can include peer-reviewed journal articles, scientific conference proceedings, reference books, internal white papers, or the results of empirical studies.

The application of analytic techniques in a given case should be recorded to the degree that a similarly trained professional would reach a comparable analytical conclusion.

Agencies should establish standards for information included in, and the format for, reporting results.

Training, Competency, and Proficiency

Practitioners of Image Analysis should follow SWGIT-SWGDE Guidelines and Recommendations for Training in Digital & Multimedia Evidence and SWGDE/SWGIT Proficiency Test Program Guidelines.

Analysts should have certification in their knowledge domain and associated forensic discipline, when such certification is appropriate and available. Note, however, that the mere existence of a certification program does not imply that it is necessary, sufficient, or appropriate.

Analysts should demonstrate competency in their discipline prior to being assigned unsupervised case work responsibilities. In addition, analysts should demonstrate proficiency and maintain continuing education activities. Agencies should document competency, proficiency and continuing education of each analyst.

The practitioner should demonstrate:

- understanding of the scope of work and how it will be applied in the forensic environment;
- subject matter knowledge and competence;
- working knowledge of the potential image processing and evaluation techniques;
- working knowledge of applications and tools utilized in the specific agency;
- working knowledge of SWGIT guidelines for capturing, storing, and processing of imagery, including issues relating to topics such as data integrity and compression artifacts;
- understanding of legal precedent for the use of specific image processing techniques;
- knowledge of the techniques necessary to document the conclusions.

Standard Operating Procedures (SOPs)

There should be Standard Operating Procedures (SOPs) for the tasks being performed. These SOPs should reflect the work flow and be general enough to permit flexibility for the required tasks.

Work Flow

The following describes a generalized sequence of actions involved in the analysis of an image and recommendations for their performance. The exact sequence will be agency specific.

1. Review of request for analysis.
    a. The agency must confirm that it performs the requested analysis.
    b. The agency must ensure the requestor has submitted all items needed to support the requested analysis or examination. Note: In some cases, it may be necessary for the agency to obtain additional items or information before an analysis can be completed.
    c. The agency must confirm that it has the necessary equipment, materials, and resources needed to conduct the requested analysis.
    d. The agency must assign the analysis request to the appropriate personnel.

2. Acquisition of imagery.
    This is the implementation of the acquisition strategy determined in the initial assessment. It produces the image for the steps that follow. Often, analysis or examination may be performed on objects directly or on analog images without the need for digitization. The primary or original image should be archived in a manner that permits verification. The image acquisition step is where the integrity of the primary or original data is initially established. Most often, subsequent steps are performed utilizing working copies, but in all cases, the integrity of the primary or original image(s) must be maintained.

a. If possible, the original or primary image, or a bit-for-bit duplicate, should be available for analysis.
b. Triage imagery
    i. The practitioner must determine if the submitted material is suitable for analysis.
    ii. The practitioner must determine if all of the submitted material, or only a subset of the material, is to be subjected to analysis.

3. Production of Working Copies.
   Produce working copies of images to be subjected to analysis. This may require digitization from negatives, prints, or conversion from other media.

4. Processing of Images to be Analyzed.
   (**Note:** Guidance relating to forensic image processing [FIP] and case-specific documentation requirements for FIP can be found in the following SWGIT documents: "Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System" and "Best Practices for Documenting Image Enhancement").

    a. Design an image processing strategy. This is the application of domain knowledge to choose which processes to apply to the image to extract the information necessary for drawing a conclusion. The strategy should be justifiable. No single processing strategy is appropriate for all cases. This should be reflected in the organizational SOPs.
    b. Identify the appropriate tools to implement the strategy. There should be some references/documentation that the selected tools are capable of implementing the strategy.
    c. Implement the designed image processing strategy.
    d. Assess results. Determine that the image processing strategy yielded results suitable for analysis.
        i. If the results are suitable for analysis, then proceed to the analysis (5). Otherwise, repeat process of designing an image processing strategy until suitable results are achieved.

    Note: Exploratory strategies that are not incorporated into the final work flow pathway need not be documented in case notes. Agencies may wish to document this fact in their SOPs.

5. Analyze processed data.
    a. Determine if criteria necessary for reaching a conclusion are present in the processed image.
        i. Specific criteria for reaching a conclusion should be identified and documented.
        ii. In some cases, the criteria will reflect the subjective experience of the practitioner. Such conclusions should be confirmed through appropriate technical review.
    b. Reach conclusion.

6. Report Conclusions.
    a. Some conclusions (e.g. photogrammetric analysis) can be reported in terms of statistical criteria. In contrast, many conclusions are derived from the observations of a trained examiner. The basis for, and uncertainty of, any conclusion should be reflected in the reporting.

    b. When a statistical basis for a conclusion can be made, the conclusion should be quantitatively reported. It may be possible to provide bounds on probabilities based on incomplete knowledge. See Appendix A.

    c. When statistical criteria do not exist, the conclusion should be reported in terms of the kind of features discerned. The ACE-V protocol is one way of doing this. Another way of doing this is to use a graded scale. An example of such a graded scale is provided in Appendix B.

    d. The report format and contents should follow agency standards.

Work Flow Examples

Photogrammetric Analysis Example

A local police agency asks the state crime lab to determine the height of the individual depicted robbing the convenience store in a surveillance video tape. The police have two suspects of different heights and would like the crime lab to determine if either can be excluded on this basis.

Following the workflow delineated above, the agency proceeds:

1. The agency reviews the request and:
    a. determines that they perform this type of analysis,
    b. determines that all necessary items to support the requested exam have been submitted,
    c. determines that they have the necessary equipment, materials, and resources needed to conduct the requested analysis, and
    d. they assign the analysis request to an analyst.

2. The analyst acquires the necessary imagery.
    a. The analyst observes that the videotape has no markings that would indicate that it is a copy, then verifies that it is an original using available video processing equipment.
    b. The practitioner reviews the video sequence of interest and locates images suitable for photogrammetric analysis.

3. The analyst digitizes still images from the analog video sequence for use in the analysis as working copies.

4. Standard image processing techniques such as brightness and contrast adjustments and deinterlacing are applied to the working images.

5. The analyst imports the images into a photogrammetric application and conducts an analysis. This analysis results in a calculated value for the robber's height, as well as a determination of the accuracy and precision of this result. The analyst compares these results with the reported heights of the two suspects and eliminates one of the suspects on this basis.

6. The analyst writes the report. Per the crime lab's SOPs, the report includes a review of the materials received, the request, the methods used, the results obtained, an estimate of accuracy and precision, the basis for the conclusion, and the conclusion.

Photographic Comparison Example

An FBI field office investigating a report of child abuse recovers a compact disc containing digital image files that appear to depict the suspect's left hand upon a victim. A second compact disc is received containing digital image files of a known suspect's left hand. An FBI image analysis unit is requested to perform a photographic comparison of the questioned and known hands to determine if the hands belong to the same individual.

Following the work flow described above, the unit proceeds:

1. The agency reviews the request and:
    a. determines that they perform this type of analysis,
    b. determines that all necessary items to support the requested exam have been submitted,
    c. determines that they have the necessary equipment, materials, and resources needed to conduct the requested analysis, and
    d. they assign the analysis request to an analyst.

2. The analyst acquires the necessary imagery.
    a. The analyst calls the investigating agency and determines that copies of the original images have been received. The authentication was performed by the investigating agency.
    b. The practitioner reviews the imagery and selects several images for further analysis.

3. The analyst makes copies of the selected imagery for use as working copies, and safely stores the received data.

4. Image processing techniques such as brightness and contrast adjustments, unsharp masking, and multi-pixel averaging are performed. The use of these techniques are documented per the unit's SOP.

5. The resulting images are analyzed and it is determined that compression artifacts present in the questioned images prevent unambiguous identification of individualizing features on the hand. The class characteristics of the questioned and known hands, however, are observed to be similar. Therefore, the analyst

concludes that similarities exist which allow the inclusion of the suspect, but do not permit the identification or elimination of the suspect.

6. The analyst writes the report. Per the unit's SOPs, the report includes a review of the materials received, the request, the methods used, the results obtained, the basis for the conclusion, and the conclusion.

Content Analysis Example

A four-year-old child is admitted to the hospital, complaining of fever. Emergency room (ER) physicians note a confluent red rash over the victim's trunk and groin. The child begins having seizures, stops breathing, and dies. Resuscitation efforts fail. The local physician signs the death certificate as "death due to scarlet fever." The coroner is not informed of the death, and the body is cremated. Three weeks after cremation, a family member makes the accusation that the child had been dipped in boiling water. The ER physician had taken digital snapshots of the rash as a teaching tool.

The county medical examiner's office is asked to evaluate the imagery to determine if the injuries are consistent with scarlatina or child abuse.

Following the work flow described above, the medical examiner's office proceeds:

1. The agency reviews the request and:
   a. determines that they perform this type of analysis,
   b. determines that all necessary items to support the requested exam have been submitted,
   c. determines that they have the necessary equipment, materials, and resources needed to conduct the requested analysis, and
   d. assigns the analysis request to a medical examiner (ME).

2. The ME acquires the necessary imagery.
   a. The ME calls the hospital and subpoenas the child's records.
   b. The ME confirms that the imagery is a copy of the digital snapshots taken by the ER doctor.
   c. The ME reviews the documents and imagery and selects several images for further analysis.

3. The ME makes working copies of the selected imagery, and safely stores the received data.

4. No image processing is required.

5. The selected images are analyzed and it is determined that the pattern of injury on the body, the location on the body, and the texture of the rash, is incompatible with immersion in boiling water. Examination of the medical records reveals a positive blood culture for *Streptococcus pyogenes*. In addition, a rapid test for influenza A was performed and was positive. Therefore, the ME concludes that the skin lesion was due to scarlatina resulting from a *S. pyogenes* superinfection secondary to influenza A.

6. The ME writes the report. Per the Medical Examiner's Office's SOPs, the reasoning behind the conclusions and the results are detailed.

APPENDIX A

Reporting Conclusions through Quantitative Means (Commentary and Example)

Classic photogrammetric evaluation is amenable to estimation of error, either through the propagation of error involved in the calculations or in comparison with fiducials that may be present in an image. The reader is referred to standard photogrammetric and numerical methods texts for the former. In many images that require measurement, there are objects of known dimension. These may be used to provide estimates of error. Both common kinds of error (imprecision and bias) should be estimated if possible, and if not possible, the limitations of the method should be mentioned in the final report.

Example: Evaluation of hostage photograph. A government agency has obtained a photograph of a middle-aged male hostage. They wish an estimate of the time since capture based on the assumption that the man has not been allowed to shave. The analyst is instructed to measure the hairs on the chin of the hostage and estimate the time since last shave. The hostage photograph is taken with the hostage holding a newspaper below his chin, and the date is estimated to be in mid-May. In addition, the victim is wearing a known brand shirt, with buttons of minimal manufactured tolerance. The button diameter is 12mm (+/- 0.0001 mm).

Photogrammetric measurement of 6 buttons reveals an average measured diameter of 12.01 mm (+/- 0.02 mm). Measurement of 100 hairs on the chin reveals an average length of 3.2 mm (+/- 0.3mm) for pigmented hairs and 7.2 mm (+/- 0.5 mm) for nonpigmented hairs.

The photogrammetric error is thus of an order of magnitude less than the error of the hair, and can be discounted. The published average growth rate for beard hair is 0.47mm/day for pigmented hair (+/- 0.2mm) and 1.12 mm/day for white hair. The May date allows negligible adjustment for seasonal hair growth variation (which may be up to 60%). White hair growth data is discarded because of great interpersonal variation.

The estimate of beard growth is thus 3.2/0.47 = 6.8 days, with an estimated error of sqrt[(0.3/3.2)*(0.3/3.2) + (0.2/.42)*(0.2/.42)]*6.8 or 3.3 days.

The estimate is thus that the hostage had been kept for 6.8 +/- 3.3 days, ignoring the (sizeable) seasonal variation and (possibly sizeable) nutritional effects. Both the error and the ignored sources of error are noted in the final report.

APPENDIX B
Reporting Conclusions Through the Use of a Graded Scale (Commentary and Example)

When a statistical basis for the conclusion can be made, the conclusion should be reported in terms of probability. When statistical criteria do not exist, the conclusion may be reported in terms of the kind of features discerned and their correspondence or disagreement. One way of doing this is through the use of a graded scale such as the following:

- Grade 0: Exclusion.
- Grade 1: Correspondence of class characteristics only.
- Grade 2: Correspondence of class characteristics and pseudorandom characteristics for which the underlying probability distribution is unknown.
- Grade 3: Correspondence of class characteristics and acquired/random characteristics which can be considered unique within a selected population.

It may be possible to provide bounds on probabilities based on incomplete knowledge. If the examiner decides to provide such a bound, then a statement of probabilities can be made as commentary, with explicit description of the underlying assumptions. For example, consider a piece of clothing with a given fabric pattern. An estimate of a certain percentage could be made that the cloth has a given orientation for one panel and another percentage for another panel. If the assumption is made (and stated), or if investigation of the manufacturing process allows determination that the orientations are independent, then it is possible to calculate a total probability by multiplying the individual probabilities. Thus, if panel A is at most 40% likely to have a given orientation, and panel B is at most 40% likely to have a given orientation, then an upper bound of 16% of the clothing thus made will have that particular combination of panel orientations. For the most part, however, these kinds of data are not available to investigators, and the limit of examination will be a grade-based conclusion.

Section 13

Best Practices for Maintaining the Integrity of Digital Images and Digital Video

Introduction

Integrity ensures that the information presented is complete and unaltered from the time of acquisition until its final disposition. Files which are copied from storage and processed result in new files. These files must also have their integrity maintained.

Integrity differs significantly from authentication. Authentication is the process of substantiating that the content is an accurate representation of what it purports to be. For example, authentication of a digital image of a gun on a table could be authenticated by a person at the scene stating the picture fairly and accurately represents the gun on the table. The integrity of the image can be established by methods covered in this document. For further information on image authentication, see SWGIT document *"Best Practices for Image Authentication"*.

This document is designed to cover the issues that can affect the integrity of digital media files. Extraction of digital media files from devices is not covered in this document.

Integrity of a digital image or video file is best demonstrated through a combination of methods. This document will discuss specific methods and provide examples of how those methods can be applied. Maintaining integrity requires both documentation and security of the files throughout the workflow. A standard operating procedure (SOP) should describe the workflow.

MAINTAINING AND DEMONSTRATING INTEGRITY

When working with digital image and video files, one needs to maintain integrity of the files and also demonstrate that the steps taken were effective. Maintaining integrity requires security of the files during transport and storage. Demonstrating integrity uses methods to show that the file has not changed.

When a digital image or video file is obtained, a reference is created for future demonstration of integrity. The reference can be accomplished in a variety of ways. The file is then transported to a storage device or location. When it is removed from storage for use, the integrity is demonstrated by the method used to create the reference.

Figure 1 shows a generic workflow of methods for maintaining, referencing and demonstrating integrity. The arrows and the boxes indicate where security measures need to be implemented to protect file integrity. The circles indicate methods used to demonstrate integrity has been maintained.

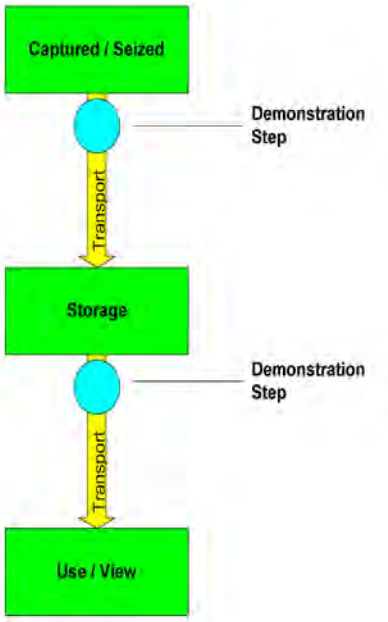


Figure 1 - Overall Maintainance with Demonstration Steps

METHODS FOR MAINTAINING INTEGRITY

The following is a list of some of the more common methods of maintaining integrity and is not exhaustive.

- Written Documentation: SOP documenting the steps required to properly maintain security. This documentation may include chain of custody, if required by agency policy.

- Physical Security / Environment: Mechanical or physical systems for preventing unauthorized access to data or loss of data, e.g. door locks, security guards, personal control, fire suppression systems, isolated computer systems.

- Redundant Physical Copies: Duplicates of files kept in an alternate location to prevent loss of files in the case of disaster.

- Logical Security (WAN / LAN): Operating system or software-based devices to prevent access to files, e.g. password protection, firewalls.

- Third-Party Escrowing: This requires transferring files to third parties, which relinquishes control. Although it may be appropriate under certain circumstances, the agency must have a viable method for demonstrating integrity that is independent of the vendor, and an appropriate contract that clarifies the vendor's obligations should be in place before any files are transferred.

METHODS FOR DEMONSTRATING INTEGRITY

The following is a list of some of the more common methods of demonstrating integrity and is not exhaustive.

- Hashing Function: An established mathematical calculation that generates a numerical value based on input data. This numerical value is referred to as the hash or hash value. Hashing computes a number using a complex formula and is very sensitive to changes in the input values.

- Visual Verification: The process of confirming the accuracy of an image through visual inspection.

- Digital Signature: This process is used along with a hash process. The resulting hash is encrypted with a specific private key. File integrity can be verified using the hash value and the source of the signature is validated using the public key. The advantage of a digital signature is that the source of a digital file can be attributed to an individual.

- Written Documentation: Notes/narrative written by the operator at various steps to document the workflow.

- Checksums / Cyclical Redundancy Check (CRC): Checksums are often used in file transfer to verify that the data transfer was successful. Some checksums are as powerful as hashes. It is recommended that those checksums which are not, be used in concert with other methods (such as hashing or visual verification) to the degree possible.

- Encryption: This process modifies the content of the files and does not in and of itself demonstrate that the file has not been altered. Encryption can be used in concert with other methods.

- Watermarks: This process modifies the content of the files and can persist as a part of the file. This method is not recommended.

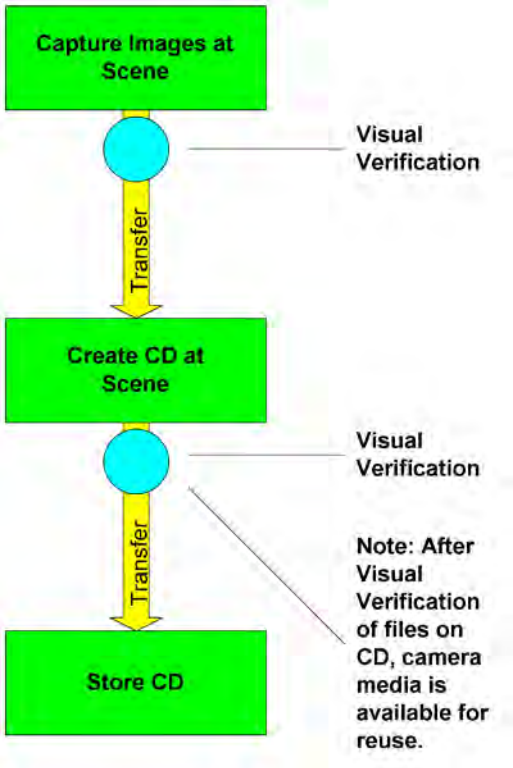
- Proprietary Methods: Methods offered for sale or license where a vendor controls the source code may not be independently verifiable. Likewise, it may not be possible to validate the methodology independently. Therefore, this method is not recommended.

EXAMPLE WORKFLOWS

The following is a list of specific workflow examples. The list is not exhaustive as each situation requires tailoring a specific process that should be outlined in an organization's SOPs.

Example #1

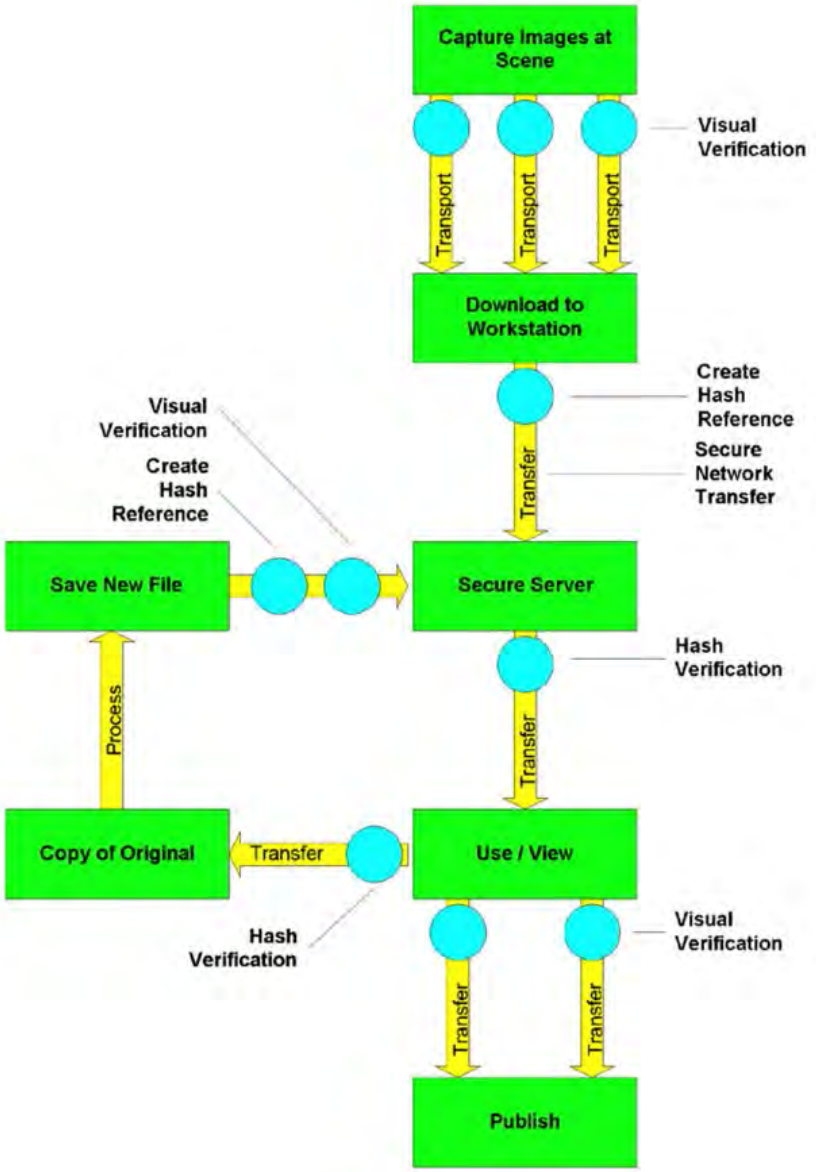
A series of digital still pictures are taken at a scene and are visually verified on the camera. The memory card is removed and placed in a self-contained CD writer, which creates two read-only copies of the pictures on CDs. The CDs are labeled with the photographer's name, the date, case number, and signature. Until the files are stored, they are in the hands of the photographer. The files on the CDs are visually verified, and then the CDs are stored in separate secure locations. At that point the memory cards are wiped and reused. In preparation for court, one CD is removed from storage; the signature on the CD is verified, and the files are visually verified. Then prints are prepared for court.



Example #2

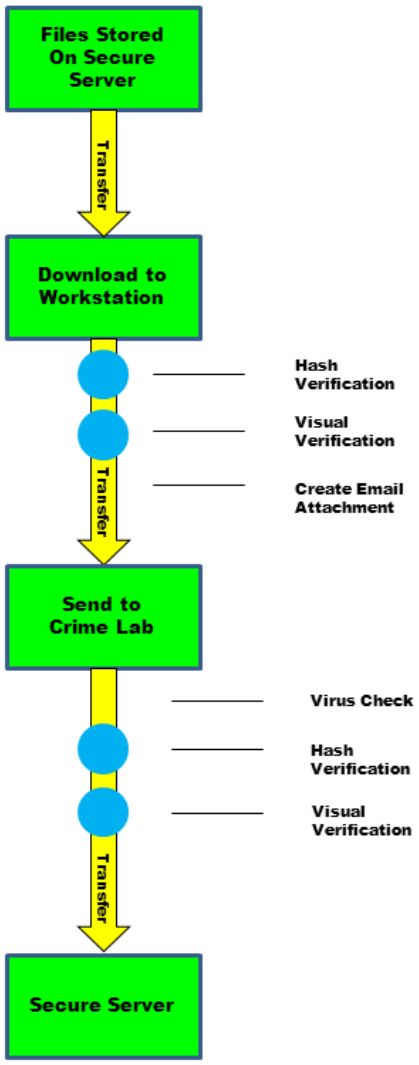
A series of digital still pictures are taken using multiple flash cards at a scene and are visually verified on the camera. Each flash card is sealed in an envelope with the name of the photographer, case number, case details, and the signature of the photographer. The flash cards are transported to another site and the person transporting them provides physical security. They are logged in at the other secure facility and placed in a locked box. Another worker removes the cards and signs the log. The files are downloaded from the memory cards to a workstation and a hash reference is created. The data is transferred to a secure network server. The hash numbers are then verified.

Later the photographer creates working copies of the files from the server, checks the hash references, and visually verifies them. The files are printed for court and some are used for further processing. The processing results in new files which are saved at the processing workstation. Visual and hash references are created. The processed files and hash references are then saved to the secure network server.



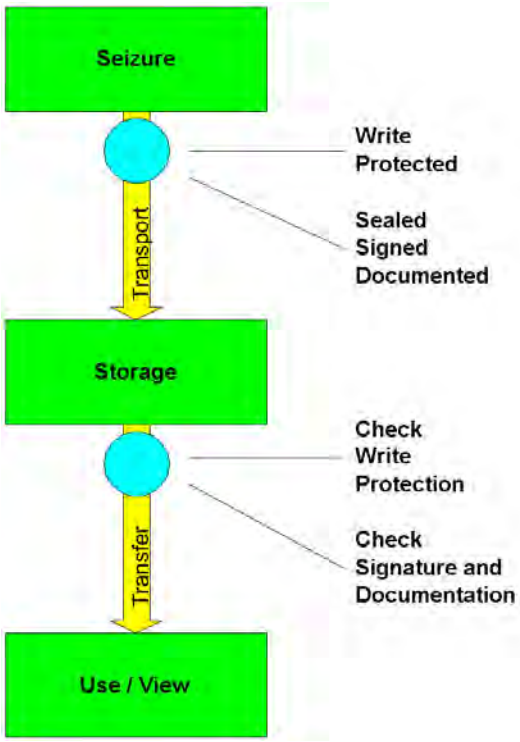
Example #3

A processed file is sent to the crime lab via electronic transfer (e.g. E-mail, FTP, etc.) for analysis. The submitting agency prepares an evidence submission form or equivalent with appropriate case information, hash value and analysis request. The sender verifies the hash reference and forwards the file to the forensic laboratory as an E-mail attachment. The forensic laboratory receives the E-mail, enters case information into the laboratory information management system, detaches the file, runs an anti-virus program, verifies the hash value and stores the file on a secure server pending analysis. The laboratory sends a response acknowledging receipt.



Example #4

In the course of an investigation, a digital video camera is seized. The Mini DV tape is removed and the write protection tab is engaged. The cassette is placed in an evidence envelope and sealed and then an entry on an inventory log is completed. The envelope is transported to and stored in a physically protected facility. When the material is removed for use or viewing, the write protect, signature, and inventory information is verified.



Section 14

Best Practices for Image Authentication

OBJECTIVE

The objective of this document is to provide personnel with guidance regarding practices appropriate when performing image authentication as part of image analysis.

INTRODUCTION

Forensic Image Authentication is the application of image science and domain expertise to discern if a questioned image or video is an accurate representation of the original data by some defined criteria. Image Authentication is a subtask of Image Analysis, and general best practice issues are discussed in SWGIT document "*Best Practices for Forensic Image Analysis*". This document addresses issues specific to Image Authentication. Questions involved in authentication include issues of image manipulation, image creation, and consistency with prior knowledge about the circumstances depicted.

Image Authentication must not be confused with the requirement to authenticate evidence as a precondition to admissibility in court. Likewise, authenticity differs significantly from integrity. Integrity ensures that the information presented is complete and unaltered from the time of acquisition until its final disposition. For example, the use of a hash function can verify that a copy of a digital image file is identical to the file from which it was copied, but it cannot demonstrate the veracity of the scene depicted in the image. For further information on digital image integrity, refer to SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*".

The process of Image Authentication can involve several tasks. These tasks include, but are not limited to, evaluation of image structure and content. Image structure issues include discovery of artifacts consistent with image manipulation or degradation, metadata analysis, and indications of provenance (issues involving the time, place and manner of image creation). Image content issues include continuity issues, evidence of manipulation, evidence of staging, and anachronism (a person or thing which is chronologically out of place). General principles and procedures for such evaluations are described below.

Image authentication may involve the evaluation of a number of technical issues as discussed below; the image analyst should demonstrate a command of them. Training and proficiency are discussed in the SWGDE/SWGIT document "*Guidelines & Recommendations for Training in Digital & Multimedia Evidence*".

GENERAL CONSIDERATIONS

Provenance

In the absence of a witness who can testify to the origin of a questioned image or video, it may be possible for an examiner to authenticate such data by identifying its origin (provenance).

Metadata Analysis

Digital image files contain both pixel data and information about the structure and content of the file itself; the latter is referred to as metadata. Metadata may contain some of the following information:

- Camera make/model/serial number
- Date/time of creation
- Camera settings
- Resolution and image size
- GPS coordinates/elevation
- Processing/Image History
- Original file name
- File structure
- Lens information
- Flash information

Metadata may be useful in identifying the source and processing history of the file, but can be limited, absent or altered. Metadata retrieval can be dependent on the software used to read it. For instance, certain software may not be able to read all the metadata that is recorded in the file. Metadata may be readable in software designed to read metadata, some image editing software or the same make and model camera used to photograph the original image.

***Note**: Converting a file to a different file format may alter or delete metadata on the converted file.*

Photo Response Non-Uniformity (PRNU)

PRNU is the variation in the sensitivity to light of the individual camera sensor elements. This variation creates a unique pattern specific to the sensor. A correlation can be made between two patterns to identify a source to an image. PRNU patterns can also be used to correlate two images to each other, without a known source.

Detection of Manipulation

For the purposes of this document, manipulation is defined as the modification of image features by direct alteration of image content. Detection of manipulation may involve analysis of textures within the image, shading and shadow, color balance, palette, lighting, quality of light, perspective, focus, and resolution.

Common manipulation techniques amenable to analysis involve primarily alteration and compositing. Alteration is the changing of image features through the use of artistic means. Figure 1 provides an example.

Figure 1. Left is original image. Image on right has been altered to remove weapon from the table.

Compositing (also known as cut-and-paste) is the combination of elements of two or more images to form one image. Figure 2 provides an example.

These techniques are sometimes incorrectly referred to as morphing. Morphing is the automated transformation of components of one image into those of another involving a sequence of intermediate images demonstrating incremental change.

Figure 2. Top image has been created by altering bottom left image and compositing it with the bottom right image.

While it is technically feasible to manipulate an image, particularly a single still image, in a manner that is not detectable by subsequent analysis using currently available tools and techniques, such manipulations involve a number of practical issues. These issues include, but are not limited to:

- Access to the image;
- The skill level of the artist necessary to perform the manipulation;
- The time necessary to create the manipulation;
- The availability of software and hardware necessary to perform the manipulation;
- The level of fine detail in the image; and
- The complexity of the image content, such as physical interaction of people with one another and the environment.

For instance, changing the color of a fountain pen in an image may be easy for an unskilled artist to achieve, but it would be a much greater artistic and technical challenge to alter an image of a nude adult to appear to be a young child. Accordingly, the complex manipulations necessary in the latter case might be easier to detect compared to a simple color change.

The presence of a manipulation does not necessarily mean that the events depicted in an image did not occur or that the individuals depicted are not real or were not there at the time. There are multiple examples in known child pornography images in which the face of an adult has been altered to obscure identity. Likewise, there are other real child pornography images in which parts of the background have been obscured to prevent observers from determining information such as the location or date of the image.

Detection of Image Creation
This is the creation of image content entirely through artistic means. One example is the creation of virtual humans using 3D modeling software (e.g. "computer-generated" or "CG" humans). Detection of such creation involves the discovery of unrealistic components and features within the image, including subsurface scattering of light in the skin, depth of field, textures, movement and physics.

Detection of Staging
Staging is the physical alteration of the scene prior to image acquisition. Detecting this may require coordination with scene investigators, correlation of image features with the real features at the scene, or comparison with other images of the scene or subject.

Continuity Issues
Continuity involves temporal inconsistencies in moving images, or inconsistencies of content within the scene in a still image. Examples include "cut edits" in a video sequence and anachronism. Anachronism is image content incongruous for the date represented in the image. Similar analysis is done to detect incongruities of place and situation. Provenance issues involve the time, place, and manner of image creation. For instance, a photograph purporting to be an original of Abraham Lincoln recorded on modern film would be suspect.

Image Processing

Image processing is often not necessary for image authentication. For instance, a picture supposed to be taken in Paris that shows the Washington monument in the background will be suspect by inspection. Detection of incongruous textural features, however, may require substantial image processing. Image Processing is discussed in SWGIT document *"Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System"*.

Report

Image authentication conclusions can rarely, if ever, be reported in terms of a numerical probability. It is sometimes possible to definitively detect manipulation or rule out authenticity. It is further possible to determine positive evidence for authenticity according to a set of criteria. Those criteria should be delineated in the report.

SPECIFIC CONSIDERATIONS

In today's forensic context, the application of the general authentication considerations for certain tasks warrants further discussion.

Child Pornography

There has been a heightened public awareness of the exploitation of children and of child pornography, leading to an increased case load for many agencies.

A common assertion regarding purported child pornography is that the image does not depict the actual abuse of a child. Instead, there may be multiple claims:

- The image is that of an adult that has been manipulated to appear to be that of a child;
- A non-sexually explicit photograph of a child has been altered to appear to be a sexually explicit photograph; or
- The image was created through artistic means without the exploitation of real children (e.g. "computer generated" children).

The best way to authenticate child pornography is to identify the victims in the image. Investigators do this through the use of known victim databases and direct contact with victims and people who know the victims. If authentication cannot be done in this manner, then further forensic analysis may be necessary.

Detection of Manipulation

Common manipulations encountered by the analyst include cut-and-paste and removal or reduction of secondary sexual characteristics using so-called "airbrushing" and "cloning" tools, among others. Artifacts of such manipulation may include inconsistencies in lighting and shadows, inconsistencies and discontinuities in color and texture, differing resolutions within an image, changes in compression and noise artifacts, and repetition of textures and features. Subject matter experts may be able to observe such artifacts directly through visual inspection or by utilizing image processing techniques.

Detection of Image Creation

It is increasingly practical to render virtual people, but some aspects of the human body remain a challenge for artists. Unrealistic features may be observed in:

- Skin tones & textures
- Skeletal structure
- Flesh & muscle movement
- Body-to-object contact
- Skin-to-skin contact
- Skin creases
- Hair
- Ears
- Eyes
- Reaction of subjects/objects to gravity and physics.

Continuity Issues

Human beings move in a manner that is generally continuous and fluid. A recording of this movement in a sequence of images should reflect this continuity. Lapses in continuity of motion may indicate image manipulation or fabrication.

Provenance may be important. Many images encountered in child pornography are part of a series of images depicting the same individuals and/or scene. When a single image can be demonstrated to be part of a series (including video), the existence of the series supports its authenticity because of the difficulty of creating consistent, undetectable manipulations. Additionally, Photo Response Non-Uniformity and metadata may link an image to a specific camera; metadata may also link the image to date/time, or author/creator.

The relationship between historical print media and computer imagery is of particular importance in the evaluation of child pornography. There were times and places in which child pornography was legal. These images were frequently published in magazines dedicated to child pornography. This era was prior to the advent of commercially available consumer-level digital image processing. This has specific implications:

- During this period, it was practical and cost-effective to create pornography using real children in real sexual acts.

- The technology of the period did not allow sophisticated digital image manipulation.

The practical implication of this for modern investigation is that when images dating from that period are encountered, their provenance argues for authenticity.

Child Pornography Case Workflow Example

A workflow example is included below:

A local police agency submits 20 digital images depicting child pornography. The request is to determine if the individuals and events depicted in the imagery are real or the result of manipulation or fabrication.

Following the workflow delineated in SWGIT's "*Best Practices for Forensic Image Analysis"* the agency proceeds:

1. The agency reviews the request and:
   a. determines that they do this type of analysis,
   b. determines that all necessary items to support the requested exam have been submitted,
   c. determines that they have the necessary expertise, materials, and resources to perform the analysis, and
   d. the analysis is assigned to an analyst.

2. The analyst obtains the imagery. The analyst contacts the investigating agency and verifies that the images are of the best quality available.

3. The analyst triages the images.
   a. The images are viewed to see if the subject is a known victim. The subject has not previously been noted, and is considered a new victim.
   b. The images are prioritized to establish the order in which they will be analyzed. The analyst also evaluates the images as a group for comparison with respect to continuity and similar issues.

4. Initial image processing is determined to be unnecessary in this case.

5. The images are examined to determine if there is evidence of manipulation. The agency maintains a list of features that are evaluated for such determination. A checklist of these features is used to streamline the note-taking process. Noting a feature that bears further inspection in one image, the analyst uses image processing to enhance the feature of interest. Upon this inspection, the feature is found to represent artifacts explainable as the result of the photographic process. The examiner notes this and continues with the examination.

6. Having found no unexplainable artifacts, consideration is given to the number of images depicting the same individual and/or location, as well as the level of detail. This image set consists of highly detailed views of the same victim in a number of poses taken in what appears to be one location. This is considered strong support of authenticity.

7. The analyst writes the report.

Execution Videos

In the current geopolitical and technological environment, videos purporting to depict the execution of individuals are common. In some cases, determining the authenticity of these videos is operationally important.

A common assertion regarding purported execution videos is that the images do not depict an actual execution.

The best way to authenticate an execution video is to examine the presumed victim. If this is not possible, forensic image analysis may be necessary. In contrast to child pornography, in which image manipulation and continuity are of primary importance, the evaluation of execution videos often involves the detection of staging and computer-generated special effects.

Detection of Manipulation

Cases have been observed in which documentation (e.g., a newspaper) is composited into the video to falsify the date. Instances have also been observed in which blood, wounds, and smoke have been artistically inserted.

In addition to the inconsistencies noted in the discussion of child pornography, artifacts seen in fake execution videos include the geometric artifacts of the modeling of special effects, such as globular smoke, reflecting the underlying geometric model used for the special effect.

Detection of Image Creation

Execution videos that are completely generated without the involvement of real people have yet to be demonstrated as forensically important. The same questions of realism that were discussed for child pornography would pertain.

Detection of Staging

Indicators of staging include inconsistencies on the scene, unusual objects or arrangements of objects in the scene, and unnatural body movement or position. For example, in a staged hanging the examination of the folds in the clothing might reveal an underlying scaffolding holding the body erect. This would suggest that the individual had been killed earlier and the execution was staged on a corpse. There have been cases in which a corpse was posed to make it appear that the subject was still alive for the purposes of extortion.

Subject matter expertise is often critical when looking for staging – it may be important to have extensive knowledge of uniforms, weapons, anatomy, physiology, or other disciplines in order to reach an accurate conclusion. In some staged executions, blood substitutes such as colored syrup or water do not display appropriate viscosity or bloodstain pattern behavior. In 2005, the news media reported on a picture of a purported American hostage accompanied by death threats, which turned out to be a posed scene using a toy action figure.

Detection of staging was accomplished through recognition of the action figure, the lack of standard insignia and ID on the uniform, inauthentic appearance of a toy weapon, and the presence of WWII-vintage hand grenades on the victim's vest (an anachronism).

Continuity Issues

The basic principles of continuity assessment apply, as described previously. In the case of execution videos, a common finding is the presence of multiple "takes," in which the scene is replayed for varying camera angles and perspectives. In a well-known case evaluated by multiple offices, frame-by-frame evaluation revealed that a gunshot entrance wound changed location on the body slightly over time. Analysis of optical flow or visual discontinuities may reveal editing.

Consultation with specialists in the analysis of other media, such as audio, may be appropriate.

The Conspiracy Theory Defense

A common issue at trial is that someone has changed a scene or surveillance photograph for the purpose of misrepresentation. While, by definition, it is not possible to prove a negative (one cannot prove that there are no unicorns, only that no one has ever proven they exist), it is possible to demonstrate that it is unlikely. The previous discussions focused more on searching for evidence of manipulation, while this task is oriented more towards providing a measure of the difficulty in achieving an indiscernible manipulation.

It should be noted that crime scene photographers can assist in the process of refuting charges of scene alteration by taking photographs of the same objects or parts of a scene from more than one angle. As noted elsewhere, the process of creating multiple altered images of the same person, object, or scene is more difficult than creating a single altered image. This is due to the fact that the three dimensional properties of people and objects, as well as the manner in which they interact with a scene's lighting, are complex and difficult to recreate artificially in a consistent fashion in multiple images. Having multiple image of the same object from different viewpoints would thus undercut claims that an object was inserted into an image after the fact. Likewise, having multiple images which show the same empty location from multiple viewpoints can contradict arguments that an object had been digitally removed from a crime scene image.

Given that an analysis for a supposed modification provides no positive evidence for it, important considerations for a negative conclusion include:

- The artifacts that would likely be produced and the techniques necessary to remove them;
- The practical limitations of the algorithmic technique supposedly employed;
- The time and expertise necessary to achieve the supposed modification, given the opportunity; and

- The resources (hardware, software, training) that would be required and their availability at the time of the supposed modification.

To illustrate with an example, consider an allegation of prisoner abuse recorded by video taken by a participant. The video had been downloaded onto a laptop computer which had been in his possession for two days. The defense claimed that the owner of the laptop computer had inserted images of the defendant into the video. Analysis of the video revealed no evidence of manipulation. Computer forensic analysis revealed that no software had been added or removed from the computer during the time period in question. Further, the laptop computer contained only a common media player and editing software that allowed editing clips. Modification of individual frames was not possible using this software. Therefore, modification of the sort claimed by the defense would not have been possible with the resources and time available.

Section 15

Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System

INTRODUCTION

It is essential that agencies store their digital and multimedia evidence[1] (DME) in such a way and under conditions that will permit access when it is needed. Archiving is the process of storing data in a manner suitable for long-term availability and retrieval. The archiving process is more than just the preservation of physical media. In cases where archiving is desired, this should be planned for from the moment the DME is generated, processed or seized.

This document is intended to familiarize the reader with issues surrounding archiving DME and suggests best practices for establishing and maintaining an archiving program. This document is not intended to cover the archiving of administrative documents or public records but may prove useful in the archiving of non-evidentiary images, video, and related files.

Why Archiving is Needed

Archiving is needed to ensure that stored DME is available for future use. The techniques employed should be chosen to ensure that data can be located, accessed and used. DME is sometimes required to be stored for long periods of time per statutory requirement and/or departmental policies and regulations.

What Should be Archived

DME that you are legally permitted to possess and that may be required for future access should be archived. Keep in mind that it may be necessary to retain original software and hardware, or to transfer data from one type of media to another, in order to access archived DME in the future.

ARCHIVE CREATION

Archive SOP's

Departments should ensure that a written archive standard operating procedure exists and is implemented. (This SOP does *not* have to be a stand-alone document.) The SOP should take into consideration the department's long term goals, planning and needs. New technologies, court precedents and changing circumstances may dictate an SOP change. Previous versions of SOPs should be maintained as reference.

Physical Plant

Physical plant concerns are multi-faceted. One of the biggest issues is environmental factors that can have an adverse effect to the archive. Some of these factors include temperature and humidity control, electrical surge protection, fire suppression, natural disaster preparation and electro-magnetic field mitigation. The use of a secondary off-site storage facility is encouraged to provide a backup to the primary archive facility.

Security

To ensure the integrity of the archive, security policies and procedures must be addressed by the agency. Security policies should address issues such as physical and electronic access tracking, limitation of access, virus detection and data suitability. In the event of an archive containing DME requiring a chain of custody, this issue should be addressed as part of agency policy and procedures.

Hardware / Software

As technology progresses, and hardware and software are upgraded or changed, it is possible the original hardware and software used to create/access the DME may need to be retained in functional condition to ensure accessibility. This is especially true in the case of proprietary systems.

Media

In the field of imaging technology, photographic plates, films, and photographic prints have been shown to be appropriate media for archiving purposes, provided they are developed and stored according to industry standards. Videotape has also demonstrated the ability to be stored for long periods of time without degradation when stored correctly. There are many types of media to which DME data can be written for the purposes of archiving. These include optical media (including CDs and DVDs), magnetic tape, and servers which may or may not include Redundant Arrays of Independent Disks (RAIDs). Serious consideration should be given to the type of media chosen for this purpose.

Many law enforcement agencies have chosen to use optical media as an interim solution for the storage of DME. Concerns about the actual versus theoretical lifespan of optical media have been raised. The lifespan of optical media begins at the time of manufacture, not at the time it is first placed into service. While optical media has been shown through common experience to be sufficient for short to moderate-term storage, it is inadequate for archiving. However, optical media used for any length of storage should be specifically designed for archival purposes and multiple copies should be maintained. Re-writable optical media should never be used for archiving as it has the shortest lifespan. Steps should be taken to ensure the serviceability of the optical media used by periodically testing and refreshing as required. (In the refreshment process, data from the original media is copied onto new media.) When media is refreshed multiple copies still need to be maintained. This process should continue until the DME is placed onto a different type of media, as technology advances, or the data is to be purged.

Some types of magnetic tape have been shown to be a reliable option in the long-term storage of data provided the media is refreshed as required per manufacturers' guidelines. At the time the archive is being planned and the use of magnetic tape archiving equipment has been determined, consideration should be given to the utilization of a magnetic tape format that is designed specifically for long term archiving purposes. Many of these devices make use of hardware and/or software compression in their storage of data. Compression concerns are addressed elsewhere in this document.

RAIDs can be implemented using different configurations, which have varying levels of redundancy and fault tolerance. For example RAID Level 0 provides for no redundancy or fault tolerance, whereas other levels of RAID provide for excellent redundancy and fault tolerance. When RAIDs are used, agencies should determine their long-term needs and resources and choose the appropriate RAID configuration for their archives.

Media Preservation

The advantages and limitations of storage media, such as the unknown lifetime of optical disks, print fading, hard drive volatility and other manufacturer research data should be understood and incorporated into the archival structure. Utilize media recommended for long term storage when archiving data; in cases where servers are used, it may be necessary to have a backup solution. Media should be handled and stored in a manner consistent with the manufacturers' recommendations.

Data Transmission

When creating an archive consider the individual file size to be archived and the bandwidth available on the network in which the archive is established. Large or numerous files being transferred across a network may influence network performance. If the archive is not a dedicated system then the transfer rate of the network may be adversely affected.

Data Management

The integrity of the DME to be archived should be verified both before and after the creation of the archive[2]. Archived DME should be readily accessible via cataloging and indexing. The metadata[3] can be very useful for facilitating broad and accurate searches of the archive. Therefore, metadata should be archived with the data. Storage facilities should be adequate in size for the data to be maintained as well as allow for growth. (DME files can be very large in size and as technology increases file sizes will increase dramatically.)

Data Compression

Generally speaking there are two ways to approach the compression of data within the archive; hardware compression and software compression. When compression is used, it is imperative that the hardware and/or software used to decompress the data be archived.

Compression can be either lossless or lossy in nature[4]. Where practicable, it is recommended that data contained within the archives not be compressed. While lossy compression may not render an image unusable, such compression schemes are not recommended. (This is *not* to say that DME that was originally created in a compressed format cannot or should not be archived.) File type and content should be considered when determining the amount and degree of compression to be used.

When SOPs call for the conversion of proprietary formats to open source formats, it is advisable to use uncompressed formats when possible. If a compressed open source format is selected, lossless compression is highly recommended. As described above, less compression is best if the file must be compressed.

Archive Maintenance

As new versions of hardware and software are released, backwards compatibility is not always ensured. Newer versions of software and hardware will not always be able to access the older data. It is necessary over time to ensure that the newer versions of software and hardware will be able to access the older data. Archivists should be aware that software providers occasionally cease support for their proprietary file formats. Long term retrieval capabilities require that *both* original hardware and software be archived.

Hardware and Media

Maintenance of physical devices and/or media may require preventative maintenance on a periodic basis per manufacturers and industry recommendations. This maintenance should be planned for at the time the archive is developed. Hardware and media should be periodically checked and/or tested for operability and serviceability. If it is found that the hardware or media is no longer serviceable, or obsolescence is foreseen, steps should be taken to migrate all data to a proven, stable storage solution as soon as possible. If failures are detected, the possibility of batch failures should be investigated.

Software

Because certain file formats or proprietary software may become unusable as technology progresses this software should be archived as necessary to ensure accessibility of DME created by the software.

Reverse Compatibility and Interoperability

Reverse compatibility is the ability of newer versions of software and/or firmware to access older file versions. Interoperability is the ability to access data across platforms or applications. These issues should be considered when upgrades to hardware and/or software are planned.

It should be noted that upgrades to the computer operating system may cause installed programs to operate erratically or not at all. When upgrading, it is recommended that the new operating system be tested on a similar type of computer system prior to implementation into the archive system. It is recommended that when the operating system is upgraded, previous versions be archived.

DATA MIGRATION

From time to time, it becomes necessary to move data from one type of media to another or to newer media of the same type.

Media Obsolescence and Lifespan

As technology progresses, media storage will evolve. Older versions of media may no longer be readable or supported and will become obsolete. To ensure uninterrupted archive capabilities, it may be necessary to migrate the DME to current media. Additionally, no media has been shown to be completely permanent. A schedule should be implemented to periodically re-write DME to new media based on industry standards and/or an understanding of the limitations of media.[5]

File Formats

Proprietary formats are formats that are primarily supported by the company producing them. These formats may not be supported as new applications become available and as technology improves. When possible, DME should be retained in its original format *and* in a non-proprietary format. Additionally, the original accompanying proprietary software should be retained for future accessibility as addressed above.

ARCHIVE RETENTION PERIODS

Legal / Departmental Retention Requirements

The type of DME and its retention periods may be dependent upon statutory requirements and/or departmental policies. These may be different but the longer time will take precedence. Some mechanism should exist to identify this time period and should be included in departmental SOP.

Purging

Legal requirements, storage space issues and departmental policy may dictate a purge (complete destruction) of archived DME. The method(s) used should be adequate to ensure that the purge of the data and/or media is accomplished. Proper means of verification should be incorporated into the methodology and documentation of the purge and include the method(s) used and when it was accomplished.

DISCIPLINE SPECIFIC ISSUES

Some disciplines may have unique requirements or special circumstances related to archiving and should be considered at the time the archive is planned. File size, proprietary file types, specialized software, metadata, interoperability and bandwidth are all factors that need to be considered. Close collaboration between discipline subject matter experts, administrative personnel, and information technologists is required to insure appropriate archival methods are implemented.

ADDITIONAL REFERENCES

United States. National Archives. http://www.archives.gov/preservation/
(Includes: Storage and Conservation concerns and Technical Information)

United States. Library of Congress. Nov. 22, 2005: *Collections, Care and Conservation.* http://www.loc.gov/preserv/pubscare.html
(Includes: Photographs, Magnetic Media, Recorded Sound and Film)

United States. NIST. April 15, 2004. Information Technology: *Care and Handling of CDs and DVDs – A guide for librarians and archivists*. ISBN 1-932326-04-9. http://www.itl.nist.gov/div895/carefordisc/

[1] Analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein. *See SWGDE and SWGIT Digital & Multimedia Evidence Glossary*
[2] See SWGIT *Best Practices for Maintaining the Integrity of Digital Images and Digital Video*
[3] Metadata is information about the associated file or data. *See SWGDE and SWGIT Digital & Multimedia Evidence Glossary*
[4] Compression of a file is the process of making the file smaller in size. Some compression schemes result in the loss of data while others do not. *See SWGDE and SWGIT Digital & Multimedia Evidence Glossary*
[5] United States. NIST. April 15, 2004. Information Technology: *Care and Handling of CDs and DVDs – A guide for librarians and archivists*. ISBN 1-932326-04-9

Section 16

Best Practices for Forensic Photographic Comparison

OBJECTIVE

The objective of this document is to provide personnel with guidance regarding practices appropriate when performing photographic comparison as part of image analysis.

SWGIT POSITION ON FORENSIC PHOTOGRAPHIC COMPARISON

Photographic comparison is an intrinsic component of many scientific and technical disciplines. Such disciplines and industries include astronomy, geology, geography, medical specialties such as radiology and pathology, intelligence and surveillance, manufacturing quality assurance, and insurance. Forensic photographic comparison is recognized as scientifically valid within the forensic science community. The first publicly prominent Forensic Photographic Comparison examinations took place as part of the Warren Commission investigation into the assassination of President Kennedy. Photographic comparisons in this investigation were used to help establish the rifle as being Oswald's as well as to establish that the "Backyard Photos" were taken with Oswald's camera.

INTRODUCTION

Photographic Comparison is an assessment of the correspondence between features in images and known objects or images for the purpose of rendering an expert opinion regarding identification or elimination (as opposed to a demonstrative exhibit). Photographic Comparison is a subtask of Image Analysis, and general best practices issues are discussed in SWGIT document "*Best Practices for Forensic Image Analysis*". This document addresses issues specific to Photographic Comparison.

SCOPE OF FORENSIC PHOTOGRAPHIC COMPARISON

Forensic Photographic Comparison examinations may be conducted on virtually any item, subject, or image. Practitioners of Forensic Photographic Comparisons in the field of Image Analysis should have expertise in image science, an understanding of the principles of individualization, and knowledge relevant to the specific subject under examination. Practitioners should be able to demonstrate sufficient knowledge of the subject matter to support their conclusions.

Several other forensic disciplines rely extensively upon photographic comparison techniques as a part of their procedures, such as footwear and tire impression analysis, latent print analysis, questioned document analysis, trace evidence analysis, and tool mark analysis. These subject matter experts use photographic comparison as a tool within the context of their domain expertise. This document is geared toward those comparison examinations typically performed by Image Analysis examiners outside the scope of these other disciplines.

This includes, but is not limited to:

- Facial and body comparisons;
- Object comparisons, such as clothing, vehicles, weapons, luggage, structures;
- Comparisons of a questioned image with a known camera to determine if the image was captured using that camera. For further information on camera identification, see SWGIT document "*Best Practices for Image Authentication*".

VALIDITY

The basis for conclusions reached through photographic comparison lies in the detection of correspondence or discordance of subject features. In some cases, a statistical model may exist, or a model can be developed which will provide a formal, probabilistic basis for a conclusion. In other cases, statistical models may not be practical.

The absence of a statistical model does not necessarily preclude formulating a sound conclusion. In such cases, expert experience is critical for the recognition of features and their significance. These experts must be able to explicitly state the underlying assumptions, observations and chain of reasoning behind their conclusions in order to demonstrate that validity.

CRITICAL ASPECTS OF FORENSIC PHOTOGRAPHIC COMPARISON

There are a number of critical practices, processes, and factors used to ensure and demonstrate validity in forensic photographic comparison. The relative importance of any one of these may vary among cases. Regardless of the protocol used in conducting photographic comparisons, the methodology used should be documented.

Class vs. Individual Characteristics

The concept of class vs. individual characteristics is fundamental to forensic photographic comparison. Class characteristics are used to subdivide things into groups or classes. Individual characteristics allow one to differentiate objects within a class from one another. Individual characteristics may be used to uniquely characterize an object. They arise from such events as random natural processes, manufacturing processes, intentional alteration, and wear-and-tear.

The ability to identify an individual person or object requires a correspondence of individual characteristics. The number of such characteristics necessary for such an identification is a function of the subject matter, the quality and quantity of details in the images, and the expertise of the analyst; no arbitrary number of characteristics is required. A correspondence of class characteristics may be useful for establishing candidate subjects. Likewise, a discordance of class characteristics can be used to eliminate potential subjects.

ACE-V

A commonly accepted protocol applied to photographic comparisons is ACE-V (Analysis, Comparison, Evaluation – Verification). Not all photographic comparisons invoke this protocol. It is commonly invoked in footwear impression and fingerprint examinations, but it is uncommon in medical image evaluation and in photogeology. Some practitioners use a formalism referred to as "ACE-VR", which adds a "Report" phase. Other practitioners, such

as physicians, do not use ACE-V but instead use conceptually similar approaches appropriate for their discipline.

The Analysis stage involves a thorough assessment of the properties and attributes of the features contained in the images under examination. While the features involved are objectively determined, the cognitive assessment of these features is an inherently subjective process. This includes determining which features are class or individual characteristics as well as issues of image formation, such as resolution, lighting, focus, and camera-to-subject geometry.

In the Comparison stage, an assessment is made of the correspondence/discordance of the characteristics identified in the Analysis stage.

In the Evaluation stage, a tentative conclusion is reached and the correspondences/discordances are tested against it. All discordances are evaluated to determine if they reflect true differences between the subjects.

Three types of discordance may be observed:

(1) *Explainable differences*. Discordances may result from the imaging process or conditions in the scene.

(2) *Unexplainable differences.* Discordances exist, but are of unknown source and significance and may or may not lead to an elimination.

(3) *Exclusionary differences.* Discordances that reflect a true difference between the objects under comparison. Such a difference establishes an elimination.

If no exclusionary differences exist, the quantity and quality of corresponding features are used to determine the level of correspondence and the results are documented. As a result of this evaluation the final conclusion is formed. The discussion of statistical vs. cognitive evaluation below applies to this stage.

In the Verification stage, the results of the examination are evaluated through independent review by a comparably trained individual.

Recognition of Imaging Artifacts

In order to accurately interpret the content of an image under examination, it is imperative that the examiner not mistake artifacts of the imaging process as reflective of physical properties of the subject depicted. For example, a watermark on a passport photograph should not be misinterpreted as a tattoo on the subject depicted. Likewise, resolution, compression, optical defects, sensor defects, lighting conditions, atmospheric conditions, and motion, among others, may introduce barriers to correct interpretation. It is for this reason that SWGIT strongly recommends image science expertise, in addition to subject matter and individualization expertise, be applied to forensic photographic comparison.

Statistical vs. Cognitive Evaluation

In some cases, statistical models have been developed for photographic comparisons. When available, these models can be of great use. In other cases one may conceive of a statistical basis for individualization but one has not yet been developed. For others,

development of a statistical basis may not be possible or may not be practical.

Cognitive Evaluation is the drawing of conclusions from visualized features. It involves testing hypotheses against known circumstances and observed features to find the best fitting hypothesis. Part of this is perceptual analysis, consisting of the comprehension and recognition of significant features by a trained eye and the cognitive ability to not only see, but recognize what one observes and relate those observations to circumstances. A trained eye is not merely the recognition and memorization of lists of features, but represents a complex cognitive analytical process.

Another feature of cognitive evaluation is to place those observations within a method of inference. Very few real-life inferences involve statistical models. Many involve what is called "abductive inference," commonly described as "inference to the best explanation." In this method of inference numerous hypotheses are tested against known circumstances and that hypothesis which is most consistent with the circumstances and without contradiction by the circumstances is proposed as the most likely explanation. While early work by C.S. Peirce focused on the use of abduction in hypothesis formation, later work has focused on its use for confirmation. While abductive inference by definition is not to "certainty", it may asymptotically approach certainty in terms of confirmation.

Visual evaluation of an image by an individual with domain expertise often involves an intrinsically cognitive evaluation. Recognition of features in an image by subject matter experts may not have a statistical component. For instance, the identification of the make and model of a vehicle depicted in a surveillance image is not a statistical process. Likewise, comparison of antemortem and postmortem dental x-rays for the purposes of identification does not involve a statistical analysis but involves cognitive evaluation. In contrast, statistical models of clothing manufacture can provide a numerical probability of individualization.

Expertise and Experience

Before conducting forensic photographic examinations, individuals should have expertise in a number of areas. The most critical of these are image science, subject matter expertise, and the science of individualization.

Image science expertise is necessary to understand the creation and evaluation of artifacts of the imaging process. Subject matter expertise is necessary to understand the significance of features. Understanding individualization is necessary to assess the utility of the features for comparison leading to identification or elimination. This diversity may require both formal and practical cross-training among multiple disciplines or it may require the involvement of multiple individuals with a variety of expertise.

Expertise may be developed in response to the needs of a specific case. For instance, a comparison involving an item of clothing may require research into the manufacturing process.

Training, Competency, and Proficiency

Training should provide a basic level of competence. The translation of training into practice requires real-world experience under supervision by qualified personnel. The value of such experience must not be underestimated. A fundamental feature of image comparison is the cognitive ability to visually recognize important image features. This skill comes from experience. Training, competency, and proficiency for image analysis are discussed more fully in SWGIT document "*Best Practices for Forensic Image Analysis*"

Infrastructure for Forensic Photographic Comparison

Competent photographic comparison requires adequate technological and physical support, ranging from hardware and software to environments adequate for proper visualization.

A steady workload facilitates the development of experience. Agencies are encouraged to ensure that their image analysis experts are given a case load that is manageable, yet sufficient to maintain proficiency.

Managers should recognize that working a single case involves many factors beyond the processing of images for comparison and noting of similarities and dissimilarities. In addition to administrative and quality requirements, there may also be the need for additional research, testing, and consultation in order to achieve a conclusion. Failure to allocate sufficient time per case to the examiner may also eventually lead to error and incomplete examination.

BEST PRACTICES

Note: Although the paragraphs below refer primarily to the comparison of images, the principles also apply to the comparison of images and physical objects.

Bias

It is the duty of the examiner to eliminate the effects of bias when conducting examinations. Eliminating the effects of bias can be accomplished through awareness, training and quality assurance measures.

Selection of Images for Comparison

If the submitted images include more than one depiction of the questioned and known objects, then the practitioner should screen them to determine which images will be useful for analysis. Once selected, images are then processed as necessary.

Comparison Process

Photographic comparisons commonly involve an examination and evaluation of features observed in a submitted image compared to features of a known subject. This process may require image processing to enhance features for comparison.

Reconstruction

Often it is necessary to determine that issues of image creation, lighting, and composition do not create artifacts that affect the comparison. Reconstruction of the circumstances of the questioned image acquisition may be necessary.

This reconstruction may consist of photographing the object under comparable conditions as seen in the questioned image or otherwise duplicating them by real or virtual means.

Figure 1. This figure demonstrates differences in the appearance of an object when the camera has a different spectral response. (Left) Color photograph. (Center) Video still from black and white camera with IR blocked out. (Right) Video still from black and white camera with IR allowed to pass.

Levels of Findings

In those cases where a statistical basis for decision making exists, the level of finding should reflect the appropriate probability. The underlying assumptions, particularly simplifying assumptions, for the statistical model should be reported.

In those cases without a statistical basis, a clear indication of the strength of the conclusion should be given; this will necessarily be a descriptive statement and not a numerical probability. Most agencies employ a scale of reporting with a certain identification at one end, certain elimination at the other, no conclusion in the middle, and some number of intermediate steps. In addition, there may be some indication of the suitability of the sample for comparison, particularly if it precludes a finding.

As illustration, three scales currently used by agencies are given below (it should be noted that this chart is not an all encompassing list of conclusions) :

<table>
<tr><td colspan="4">Continuum of Conclusions Examples For Photographic Comparative Analysis</td></tr>
<tr><td rowspan="10"> 
</td><td>Identification</td><td>Identification</td><td>Identification</td></tr>
<tr><td rowspan="3">Similar</td><td></td><td>Powerful support same</td></tr>
<tr><td rowspan="2">Similarities noted</td><td>Strong support same</td></tr>
<tr><td rowspan="2">No conclusion, but with similarities</td><td>Moderate support same</td></tr>
<tr><td rowspan="3">Neither/Nor – with explanation</td><td>Limited support same</td></tr>
<tr><td>No conclusion</td><td>Inconclusive</td></tr>
<tr><td>Limited support different</td></tr>
<tr><td rowspan="3">No conclusion, but with dissimilarities</td><td rowspan="3"></td><td>Moderate support different</td></tr>
<tr><td>Strong support different</td></tr>
<tr><td>Dissimilar</td><td>Powerful support different</td></tr>
<tr><td>Elimination</td><td>Elimination</td><td>Elimination</td></tr>
<tr><td></td><td>No comparison Possible</td><td>Not suitable – with explanation</td><td>No comparison Possible</td></tr>
</table>

It should be noted that the criteria for a full identification are a function of image quality and the clarity, relative weight (often subjective) and number of individual characteristics. No arbitrary number of individual characteristics is necessary to effect an identification.

Photogrammetry and Forensic Photographic Comparison

Images subject to photographic comparison may not include a scale or other means of directly defining the size of the questioned object. In many of these cases the issue of comparison does not depend upon the scale. In such cases a conclusion can be made in the absence of an explicit determination of the size. For example, the determination of the make and model of a car does not require a determination of the exact wheelbase. In other cases, the relative or approximate size is sufficient. For example, a corresponding number of buttons on a shirt when compared to shirts of the same design could be used to

demonstrate a similarity in size, but cannot provide a quantitative estimation.
In other cases, it may be necessary to demonstrate a comparable size through either direct or indirect measurement. This can be accomplished by photogrammetry. See SWGIT document "*Best Practices for Forensic Image Analysis*".

Care must be taken in deriving 3-dimensional measurements from 2-dimensional imagery. Differences in imaging conditions can lead to differences in measurements despite the fact that the identical feature is being measured in both images. Likewise, the subject of examination could change over time. For instance, a person could gain weight. These differences are explainable, but must be recognized and accounted for.

Photographic Documentation as a part of Comparison/Analysis

In some cases it may be necessary to photograph a partial reconstruction or model to demonstrate corresponding features or differences between the questioned and known objects. Some factors to take into consideration are: lighting, camera to subject geometry, spectral sensitivity of the camera sensor or film, optical properties of the questioned object and other objects in the scene, deformation of the subject (e.g. folds in clothing), viewing conditions (including effects of weather), and optical distortions in the lens and camera enclosure. **See Figure 1** for an example in which spectral sensitivity was documented.

EVIDENCE MANAGEMENT

Items subject to photographic comparison may also be analyzed by other forensic science disciplines. Laboratory management should be aware of the possibility of photographic examinations and its placement in the overall analytic work flow. The sequence of examination is critical for photographic comparison examinations because other examinations may render the object unsuitable for comparison. For example, removal of fabric from clothing for DNA analysis can destroy visually significant features. Identification marks placed on shoes during footwear impression examinations can also adversely affect the comparison.

Similarly, the improper handling of an object during photographic comparison may contaminate or alter it, and adversely affect the outcome of subsequent examinations. For example, latent fingerprints may be destroyed.

QUALITY CONTROL/QUALITY ASSURANCE

A photographic comparison laboratory is not a drug chemistry laboratory with the same methodologies and instrumentation. Therefore, the concepts of drug chemistry standards and controls do not always directly apply. While criteria should be developed to assure appropriate processing and evaluation of images, arbitrary quality control methodologies may not have a meaningful direct application and may not be appropriate. For instance, requiring a daily log indicating if a microscope light turns on does not serve a particularly useful calibration purpose in standard histologic evaluation. If an examiner sits down at his or her microscope and notices the light does not turn on, he or she can simply change the bulb. In contrast, there may be instruments, such as densitometers or displays used for colorimetric evaluation, where traditional calibration is appropriate.

Section 17

Digital Imaging Technology Issues for the Courts

INTRODUCTION

Digital photography and imaging technology has its background in technology from the 1940s. The first camera designed to create photographs represented by a digital file was developed in the 1960s. Just as color film was a normal progression of the technological evolution from black and white film, electronic/digital imaging is a normal progression of the technological evolution from silver-halide based film.[1] Today, digital imaging technology is regularly encountered in the courts around the world. The goal of this document is to discuss the proper use of digital imaging technology through the dissemination of information to judges and attorneys. This document is designed to present the relevant issues in plain language to maximize the effectiveness of the courts when dealing with this technology.[2]

This document will provide the reader with citations to case law and scientific and technical research articles dealing with digital imaging technology used within the criminal justice system.

This document will also address some of the common myths and misconceptions associated with digital imaging technologies used in the criminal justice system. For additional information readers should become familiar with the basics of digital imaging technology. Information on these basics can be found in several documents released by SWGIT.

DEBUNKING MYTHS AND MISCONCEPTIONS

One of the most challenging issues facing the legal community in dealing with digital imaging technology is separating fact from fiction. "Expert" advice is readily available, but may be inconsistent, impractical, and biased. Despite the misinformation to the contrary, digital imaging technology in the hands of a competent, properly trained practitioner, is appropriate for use in a forensic setting and produces results that are admissible in judicial and similar fact-finding proceedings.

MYTH: "Film is better than digital because film cannot be altered or manipulated."

FACT: Both film and film-based images can be manipulated. Traditional film and photographs have been manipulated for over 100 years, and the integration of film and digital technologies allows the production of manipulated negatives that can be indistinguishable from the results of traditional film photography. Fortunately, in most cases, manipulation is detectable by those trained to do so. Ultimately, it is the integrity and abilities of the practitioner, established processes, and accepted practices that make film and digital equally valuable in the courtroom.

MYTH: "Because digital images can be manipulated, they should not be admissible."

FACT: The integrity of digital images can be assured. There are methods that demonstrate digital file integrity including hashing functions, visual verification, digital signatures, written documentation, and checksums/cyclical redundancy checks.[3] Additionally, experts may be capable of determining whether a digital image, film photograph, or film negative has been altered. When evidence is produced suggesting an alteration, experts can be used in an attempt to confirm or refute the assertion.[4]

MYTH: "Digitally enhanced images should not be admissible."

FACT: Digitally enhanced images that reveal features that exist in the image but not immediately apparent through visual examination have historically been found to be valid and admissible evidence in courtroom proceedings. Case law supports the admissibility of digitally enhanced images. Both *Frye* and *Daubert* challenges to the use of this technology have been resolved in favor of admission of digitally enhanced images. A digital image or film photograph that has been altered or enhanced that produces an output that does not accurately and fairly depict what was captured does present admissibility issues. For example, if a blue car is the subject of a photograph and the image is changed to make the car appear red, such an image would certainly be subject to objection and explanation. On the other hand, an image that has been enhanced to reveal a fingerprint on a patterned background by removing the background pattern should be admissible because the nature of what the image depicts (a fingerprint) has not been changed. In this respect, one does well to remember that under rules of evidence an "original" of the data (which is what is created when a digital photograph is captured) is not restricted to the data itself, but "any printout or output readable by sight, shown to reflect the data accurately." Federal Rule of Evidence 1001(3).

***MYTH*:** "When images are digitally enhanced they must be reproducible, and these reproductions must be "*bit-for-bit*" copies of each other."

FACT: Digitally-enhanced images must be reproducible; however, when images are enhanced the bit values change. Two persons using the same techniques, producing images visually indistinguishable from each other, will get different bit values. This is an expected and normal occurrence that should not affect the admissibility of the image. Reproducibility is judged by obtaining visually comparable results, not identical bit values.

MYTH: "Film always has higher resolution (detail) than digital."

FACT: As digital imaging technology advances, output quality approaches and sometimes surpasses that achieved by traditional photography. Output quality depends upon a number of factors including the camera's optics, sensor or film, method of printing or display, and photographic technique. Any of these can limit the quality of the final product and a digital camera's sensor resolution is often not the limiting factor. In addition, the highest possible resolution is not

always necessary to accurately and fairly depict what has been captured with film or a digital camera. Film photographers, for example, do not always find it necessary to use the type of film that has the highest resolution.

MYTH: "Digital cameras do not accurately represent color."

FACT: Digital cameras are neither more nor less accurate in depicting color than film cameras. No imaging technology can exactly reproduce the human visual system. The color rendition of an image is dependent on a number of factors. Although the method used in processing color differs between film and digital imaging technologies, both are capable of producing accurate results.

MYTH: "Localized adjustments such as dodge and burn should never be used in the digital enhancement of images."

FACT: Localized adjustments are appropriate under many circumstances. The dodge and burn technique is one that has its roots in traditional darkroom technology. When the technique is applied appropriately, it can greatly improve the visibility and usefulness of evidence. This processing technique *can* be documented by the practitioner.[5]

MYTH: "Digital enhancement of a fingerprint image can accidentally morph the fingerprint of one person into that of another."

***FACT*:** When digital image enhancement is performed according to accepted guidelines and standards, it is not possible to change one person's fingerprint into another's. The end result of properly enhancing any image is an increase in the visibility of characteristics of interest within the image. Research completed at Indiana University Purdue University Indianapolis (IUPUI), Mathematical Sciences Department, found that the possibility of such an occurrence to be one in 10-to-the-80^{th} power (1 followed by 80 zeroes). This number is approximately equal to the number of atoms in the universe.[6]

MYTH: "All digital images must be electronically authenticated to be admissible."

***FACT*:** A digital image (as well as a film photograph) can be authenticated through testimony or other evidence that the image is a fair and accurate representation of what it purports to depict; electronic authentication is not required. Image integrity must not be confused with the requirement to authenticate evidence as a precondition for admissibility in court.[2,4] Courtroom authentication of an image substantiates that the image is a fair and accurate representation of what it purports to be, whereas integrity verification is the process of confirming that the image presented is complete and unaltered since time of acquisition. The integrity of digital images can be verified through a number of means, some of which are not electronic.

MYTH: "Image files should be left on the camera's removable flash media and the flash media must be available in court as a condition precedent to admissibility of the image."

FACT: Most removable flash media is designed as temporary storage. Flash media cards that are stored for long periods of time are prone to data corruption that leads to loss of images. Excessive heat or cold, shock, and other improper handling and storage techniques can all put flash media at peril of losing data.

MYTH: "Any copy (duplicate) of a digital image made from the camera's media is not an original."

FACT: When the contents of a camera's media is copied to a hard drive, CD, or DVD by a method which accurately reproduces the data on the camera's media, a duplicate of that data is created. Federal Rule of Evidence 1001 (4). Furthermore, "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Federal Rule of Evidence 1003. This legal result is the same as what has happened digitally; the process of correctly copying the data from the camera's media to another media creates identical data. Copying the data from one media to another is analogous to producing multiple original prints from a negative.

MYTH: "Compression of digital images or video is always bad."

FACT: Compression can be appropriate depending on the intended use of the image or video. Compression should be used with care to avoid material degradation of the image. The use of compression, if over applied, can degrade the quality of the image, but it does not change the subject of the image into a different one.[7]

MYTH: "Compressed images, such as those captured in JPEG format, are not suitable for comparative or analytical purposes."

FACT: It is preferable to capture images that are intended for comparative or analytical purposes using uncompressed formats; however, lossy compressed formats like JPEG may be used if the examiner determines sufficient detail is present in the image for such analysis.

MYTH: "All digital images must be treated as evidence and tracked with a chain of custody."

FACT: Many digital images do not require a chain of custody. Whether a chain of custody is established for a digital file is determined by the reason for which the file has been created or is being maintained and will vary between jurisdictions. For example, seized evidence almost always requires a chain of custody. Images produced or enhanced in a laboratory setting do not always require a chain of custody.[2]

MYTH: "All digital imaging equipment must be calibrated to be used in a forensic setting."

FACT: The requirement for calibration of equipment is determined by individual agencies and manufacturers, based on the type of equipment and their function. The need for calibration generally exists in equipment that performs quantitative or numerical analysis. When required, visual comparison of digital images can suffice as calibration of digital imaging equipment.

MYTH: "Potential jurors understand how digital imaging is used in a forensic setting."

FACT: Due to the technical and potentially labor intensive nature of forensic imaging, most outside the discipline do not understand the difference between forensic image processing and artistic editing of images. Laypersons exposed to mass media depictions of forensic science such as novels, dramatic cinema, and television programming may not have an accurate understanding of the science and its limitations. The media has a tendency to highlight forensic tools and techniques that pique the audience's interest while often disregarding realism in their application and the time frames required to obtain results. For example, Richard Catalani, writer for the television drama *CSI: Crime Scene Investigation*s writes, "*CSI*, admittedly, tends to focus on the more interesting and novel forensic techniques, and not on more realistic, tedious, labor-intensive searches, when no one finds the needle in the haystack."[8]

MYTH: "An expert is required to lay a foundation for any digital images introduced in court."

FACT: When images that have been subjected to processing to reveal information are being offered in court, a subject matter expert will usually be required to explain the process used. On the other hand, when traditional darkroom type adjustments are applied these are easily understood without the need for an expert. For example, an enlargement or brightening.

MYTH: "Watermarking does not change the original image."

FACT: Watermarking is a potentially irreversible process of embedding information into a digital signal. It modifies the content of the files and can persist as a part of the file. This process may change the image content as it was captured by the camera. Watermarking may occur at the time of recording, at the time the video or images are exported from the system, or during post-processing. Watermarking is not recommended.

MYTH: "For the purposes of CCTV recordings, one type of compression is always superior to another."

FACT: CCTV recordings should not be rated solely on the type of compression used, but on the quality and suitability of the entire system. In addition to the type of compression used, other factors within the system affect the quality of CCTV recordings. These include, but are not limited to: lighting, frame size, frame rate, camera quality/optics/placement, environmental factors, and method of collection/output.

MYTH: "The use of cell phone or other electronic devices that have integrated cameras are perfectly acceptable for crime scene documentation."

FACT: Although cell phones and other electronic devices have integrated cameras, the technology has not advanced to the quality necessary for proper crime scene or other forensic purposes. Cellular telephone and other personal electronic devices with digital cameras should not be used unless their use is an operational necessity.

MYTH: "For video to be of evidentiary value, there is a minimum recorded frame rate required."

FACT: NTSC is a common video standard in the US that specifies a frame rate of 29.97 frames per second, referred to as real time. In an effort to reduce hardware requirements (e.g. storage) video is often recorded at a lower frame rate. Lower frame rates may reduce the likelihood of determining activities within a scene but do not negate the value of the video. The evidentiary weight of video should be determined on a case by case basis.

MYTH: "Images should never have their metadata modified or removed as this will invalidate them for forensic use."

FACT: While it is best practice to maintain digital image files in an unaltered state from time of capture, separation of image content from metadata may not invalidate them for forensic use. In the majority of cases, the visual interpretation of an image is not affected by conditions of capture reflected in the metadata. In some cases the presence of metadata is necessary for the analysis of the image.

CASE LAW

Many cases exist in various courts throughout the United States and other countries where digital imaging technology has been challenged and successfully admitted into evidence. This section of the document is designed to provide the reader with case law citations in which issues of admissibility have been addressed.

This list is intended as a starting point for researching such case law.

ISSUE: Fair and Accurate Representation of the Scene

CASE: *Almond v. State*, 553 S.E.2d 803, 805 (Ga. 2001)

ISSUE: Digital Manipulation vs. Processing

CASE: *English v. State, 422 S.E.2d 924 (Ga. Ct. App. 1992)*
CASE: *US v. Mosley, 35 F.3d 573 (9th Cir 1994)*
CASE: *Nooner v. State, 907 S.W. 2d 677 (Ark. 1995)*
CASE: *Washington v. Hayden, 950 P.2d 1024 (Wash. App. 1998)*
CASE: *US v. Beeler, 62 F. Supp. 2d. 136 (D.Me 1999)*
CASE: *Dolan v. State, 743 So. 2d 544 (Fla. App. 1999)*
CASE: *State v. Hartman, 93 Ohio St.3d 274 (Ohio 2001)*
CASE: *Rodd v. Raritan Radiologic Associates, PA et al., 860 A.2d 1003 (N.J. Super. 2004)*
CASE: *Kennedy v. State, 853 So. 2d 571 (Fla. App. 2003)*
CASE: *Hartman v. Bagley, 333 F.Supp. 2d 632 (N.D. Ohio 2004)*
CASE: *State v. Swinton, 847 A.2d 921 (Conn. 2004)*

ISSUE: Video

CASE: *Commonwealth of Pa. v. Auker, 681 A. 2d 1305 (Pa. 1996)*
CASE: *US v. Beeler, 62 F. Supp. 2d. 136 (D.Me 1999)*
CASE: *Dolan v. State, 743 So. 2d 544 (Fla. App. 1999)*

Canadian Case Law

CASE: *R v Mohan (1994)2S.C.R.9*
CASE: *R v Nikolovski (1996) 3 S.C.R. 1197*
CASE: *R v C (P.T.)–(2000) B.C.J.No 446;*
CASE: *R. v. Cooper(2000) B.C.S.C 342;*
CASE: *R v Kucerova(2001) B.C.J. No 358;*
CASE: *R v Mackay(2002)SKQB 316;*
CASE: *R v Penny(2002)N.J. No.70;*
CASE: *R v Pasqua(2008) A.J. No. 184 or ABQB 128.*

United Kingdom Case Law

CASE: R v W & ANTHONY BEST (2006)
CASE: R.v. Birch et al (1992)

SCIENCE AND TECHNICAL PUBLICATIONS

In addition to the cited legal cases, the following references might prove useful to the reader.

Hak JD, Jonathan W., *The Admissibility of Digital Evidence in Criminal Prosecutions*, DOJ- Alberta Canada, 2003
http://www.khodges.com/digitalphoto/hak.pdf

Conviction Through Enhanced Fingerprint Identification, Re-printed in "The Print" 10(2) February 1994, pp1-2
http://www.scafo.org/library/100201.html

Barakat JD., Brian and Miller JD., Bronwyn, *Authentication of Digital Photographs Under the "Pictorial Testimony" Theory: A Response to Critics*, Florida Bar Journal July 2004, pp38
http://www.floridabar.org/DIVCOM/JN/JNJournal01.nsf/76d28aa8f2ee03e185256aa9005d8d9a/1703e6eec2b2a74385256ec100751bda?OpenDocument&Highlight=0,barakat*

Berg, Erik C., *Legal Ramifications of Digital Imaging in Law Enforcement*, Forensic Science Communications October 2000 Volume:2 Number:4, United State Department of Justice, Federal Bureau of Investigation, Washington DC
http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/berg.htm

Nagosky, David P., *The Admissibility of Digital Photographs in Criminal Cases*, FBI Law Enforcement Bulletin, December 2005 Volume:74 Number:12, United State Department of Justice, Federal Bureau of Investigation, Washington DC
http://www.fbi.gov/publications/leb/2005/dec2005/dec05leb.htm

United Kingdom House of Lords, Science and Technology Committee 5th Report, 1997-1998, *Digital Images as Evidence*.
http://www.publications.parliament.uk/pa/ld199798/ldselect/ldsctech/064v/st0501.htm

United Kingdom. Home Office Scientific Development Branch Digital Imaging Procedure. Version 2.1 November 2007. Publication Number 58-07. Crown Copyright 2007, ISBN: 978-1-84726-559-3
http://science.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web).pdf?view=Standard&pubID=555512

Kashi, Joe, Authenticating Digital Photographs as Evidence: A Practice Approach Using JPEG Metadata, June 2006 Law Practice Today, American Bar Association
http://www.abanet.org/lpm/lpt/articles/tch06061.shtml#bio#bio

Robinson, Edward M. *Crime Scene Photography*, Academic Press, Elsevier, Burlington MA (2007)

Davies, Adrian and Fennessy, Phil. *Digital Imaging for Photographers, 4th ed.*, Focal Press, Elsevier, Burlington MA, (2001)

[1] IAI Resolution 97-9
[2] SWGIT Section 1 *Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System*
[3] SWGIT Section 13 *Best Practices for Maintaining the Integrity of Digital Images and Digital Video*
[4] SWGIT Section 14 *Best Practices for Image Authentication*
[5] SWGIT Section 11 *Best Practices for Documenting Image Enhancement*
[6] Li, Fang. "*Probability of False Positive with an Innocent Image Processing Routine*", Journal of Forensic Identification, V:58, I:5, (2008) Pg:551-561.
[7] SWGIT Section 5 *Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System*
[8] Yale Law Journal, http://yalelawjournal.org/2006/02/catalani.html

Section 18

Best Practices for Automated Image Processing

Objective

The objective of this document is to provide personnel with guidance regarding the use of automated image processing.

Introduction

It is common in the evaluation and processing of forensic imagery to use integrated software applications/libraries, hardware, or both that can have automated functions. These automated functions, called "components" in this document, may reduce complex operations to a single "button-push". This can increase productivity and reliability within an organization, but the use of these applications can encourage the naïve user to perform tasks without adequate knowledge of the underlying principles and their impact on the resulting output image. This can lead to inappropriate application of certain algorithms and the use of automated methods when manual processing would be more suitable. It is the responsibility of the practitioner to know how automated methods in their equipment and laboratories work, to know that they work and to know when to use them.

Scope of this document

Automated processes can be found in hardware as well as software. In digital cameras, a great deal of automated image processing can occur, and many of these operations may be under the control of the user. Image processing within a camera performed as part of image acquisition that is not under user control should be considered simply part of nominal camera function. User-controlled in-camera image processing constitutes image processing just as if it was done on a computer and image processing guidelines apply. (See SWGIT document "*Guidelines for Image Processing*") This document provides guidelines for the use of automated processes regardless of platform or application.

The Practitioner Must Know How The Application Works

Many software applications and systems provide access to a large suite of components, many of which are not useful to a particular laboratory or for a specific examination. The practitioner must demonstrate knowledge and competency of those components used but does not need to demonstrate it for those components that he/she does not use.

The practitioner must understand the basic principles of the component and the effects of changing settings within the software application. It is important to understand what artifacts are likely to be produced using any particular component of a software application and how to recognize and interpret them. The user must be able to recognize when a component is not functioning correctly and what steps, if any, can be taken to mitigate this.

Practitioners should attempt to obtain adequate documentation on the principles and implementation of the components in the application used in the laboratory. In some cases, such as open source software, the implementation may be well documented and the source code is available. In other cases, sufficient documentation may be provided by the manufacturer. It may not be necessary for documentation to contain explicit implementation or mathematical details, but it should provide enough information for the practitioner to understand the principles and use. If such documentation is not provided by a manufacturer, then the component should be used with caution. If sufficient understanding of the principles underlying the component cannot be obtained, then the component should not be used. It may be necessary for the practitioner to obtain formal training in the theory or application of the algorithms implemented within components above and beyond manufacturer documentation and vendor-based user-focused courses.

Different software applications may provide the same labeled function using different algorithms or implementations with different numbers and types of settings that can affect the result of applying that function. If the practitioner uses multiple applications, he/she should be aware of these differences and their functional significance.

The Practitioner Must Know That The Application Works

The use of a particular software application must be validated for its intended purpose. Likewise, periodic verification should ensure that the components function properly. If validation or verification fails, then practitioners should know what mitigating steps to take.

Many software applications and integrated systems offer periodic upgrades and updates. While these are often desirable, they are not necessary if the current version performs adequately and meets the needs of the laboratory.

When upgrades or updates are incorporated, the agency must determine and document whether this constitutes a major or minor modification. If deemed "major", then it is recommended that the application or system be re-validated. If deemed "minor", then simple verification is appropriate.

The Practitioner Must Know When To Use An Application

The practitioner must know when it is appropriate and not appropriate to use a given component. Even within an appropriate class of images, a given component may have limited utility. The practitioner must know the limits of a given component and how to recognize when those limits are exceeded.

Document Automated Image Processing

Automated image processing that takes place within a camera is typically recorded and preserved in the metadata of the image file. Therefore, there is no need to document this processing in any other manner.

Automated image processing that is performed by an application outside of the camera should be documented. This may be done either through the use of a laboratory SOP and/or as part of the notes on a case-by-case basis as determined by individual agencies. See SWGIT document "*Best Practices for Documenting Image Enhancement*" for more information.

Section 19

Issues Relating to Digital Image Compression and File Formats

Introduction

This document provides a foundation of knowledge of compression algorithms and file formats utilized in digital imaging, including photography and scanning. It does not cover video compression algorithms or file formats. Understanding these processes and their advantages and disadvantages will allow agencies to make informed decisions for the appropriate application of file formats and compression algorithms. For a comprehensive understanding, the reader is encouraged to seek out other sources.

Compression

Compression is the process of reducing the size of a data file utilizing algorithms to rearrange the way data is organized within the file. Compression can be used to facilitate the storage and transfer of large files. The resulting file may retain all of the data or there may be data, including visual information, that is lost. Compression algorithms that retain all of the original data are "lossless," and those in which data is lost are "lossy." By setting the camera or software to the least amount of compression (or the fewest amount of pictures you can store), you will significantly decrease the amount of data lost. The decision to use lossy or lossless compression will be dictated by the intended use of the image.

Lossless Compression

When using lossless compression, no information is lost, but the compressed file uses fewer bits to represent the information. When the file is re-opened, the original data is reconstructed. Generally, lossless compression can achieve compression at a ratio of about 2:1 (thus reducing the file size by half). LZW (Lempel-Ziv-Welch algorithm) is an example of lossless compression.

Lossy Compression

When using lossy compression, information is lost and cannot be retrieved in its original form. Lossy compression can achieve compression ratios of greater than 2:1. JPEG (Joint Photographic Experts Group algorithm) is commonly used to accomplish this.

How it works

Image files can contain redundant or irrelevant data. During compression, this data is reorganized or removed. This makes the file smaller while keeping a pathway so that the data can be reproduced. Depending on the method selected, the user may or may not have control over the result. The average user of commercially available software will have limited control on how of the algorithms are deployed. The following tools are used alone or in concert with one another to achieve the desired compression for a file.

Run-length encoding is a variable length code. It is a lossless method designed to remove redundant data. No information is lost, it is just represented in a more concise way. The coded version depends on how frequently characters are repeated in the original data set. If there is much repetition, you will get a shorter coded file.

Example: 111111112223 → 182331 (2:1 compression)

In this example, a string of 12 values takes the space of only 6. There are eight occurrences of the number "1" represented by the number 18 in the string, three occurrences of the number "2" which is represented by 23 and one occurrence of the number "3" represented by 31.

Lexicographic encoding is also a variable length code. It is a lossless method designed to remove irrelevant data. The most repeated character is given the shortest code value. Code values can be stacked into packages that are more concise. No information is lost.

Example: 201121001

In this example, the number one is given the binary code value "0" because it is the most frequent value. Zero has the second highest occurrence and is given the binary code value "1". Finally, two is given the binary code value "10" because it is the least occurring. The original string contains nine numbers of 8 bits each for 72 bits or 9 bytes (9 x 8 = 72 bits or 9 bytes). In the coded version, no number needs more than two bits. Four two-bit numbers can comprise one eight-bit byte. The compressed version would only require 11 bits or less than two bytes.

Quantization encoding maps multiple values to a single replacement value. It is a lossy method designed to reduce the number of values used.

Example:	Original Value (3bits)	Encoded Value (2 bits)
7		
	}	3
6		
5		
	}	2
4		
3		
	}	1
2		
1		
	}	0
0		

In this simple example, an original value requiring 3 bits of data is transformed through quantization and now only requires 2 bits of data. For the purposes of this example, the original value was limited to 8 numbers. As the range of the original values increases there are more levels of compression available

JPEG Compression

JPEG uses some lossless algorithms, but also uses quantization. The quantization of the file can result in lost data. The amount of quantization is variable. JPEG can reduce file sizes 5:1 with minimal degradation and upwards to 20:1 with significant degradation. Many programs and cameras allow the user to choose the JPEG quality setting. Care should be taken to choose the level that is appropriate for the situation.

The JPEG algorithm begins by splitting the image into three separate channels creating three separate images. Each color channel image is broken into segments that are 8 pixels by 8 pixels in size (8x8 blocks). Each 8x8 block is represented by a mathematical function creating a new 8x8 block. Quantization is applied based on the "quality" level the user selects. The more quantization applied the smaller the file size resulting in greater loss. JPEG can be lossless if the quantization level is set to zero. After quantization, the 8x8 blocks are reassembled and the compressed color channels are combined back into one image.

As Figure 1. Demonstrates, excessive compression can have a dramatic visual effect. The image on the left has been compressed substantially more than the image on the right. Artifacts become more obvious and there is a substantial difference in image quality.

Figure 1. Demonstrates the difference between two image one using minimal compression (right) and one using more compression (left).

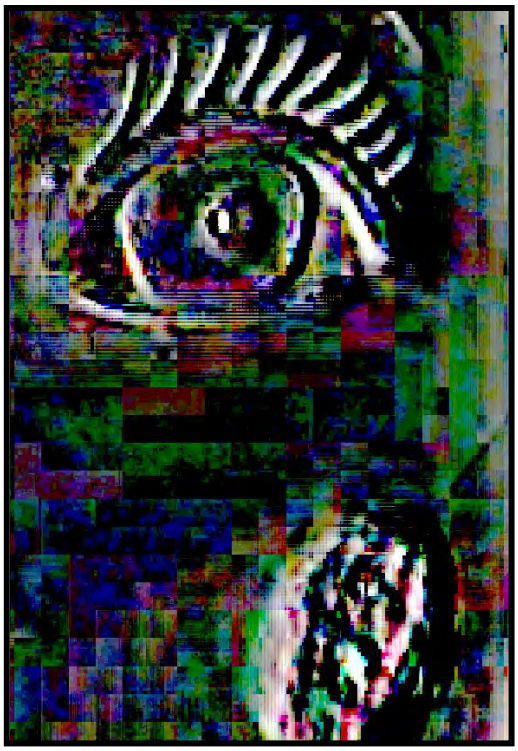
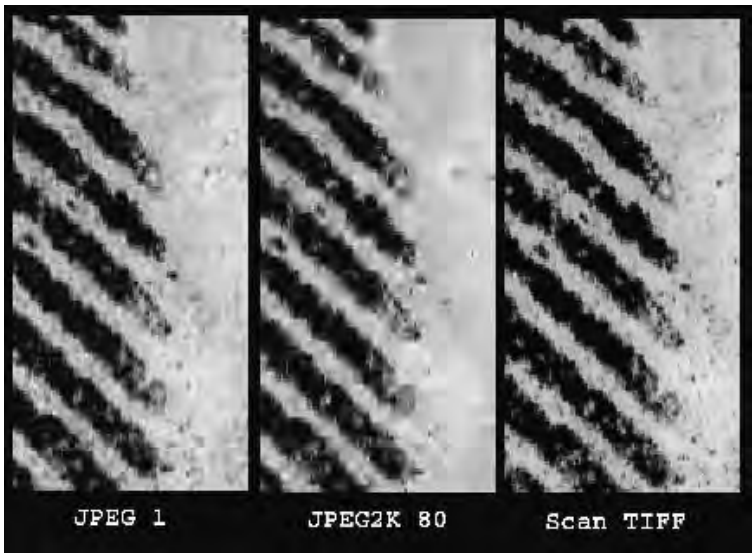


Figure 2. Represents the differences between the two images. White areas represent image data lost, dark areas represent image data preserved and colored areas represent changes in color values.

JPEG2000 is similar to JPEG but uses a different mathematical function. It does not segment the image using 8x8 blocks as JPEG does. It uses downward interpolation to create smaller versions of the image and applies a mathematical function followed by quantization to achieve compression. Compared to standard JPEG, JPEG2000 can achieve a greater compression of image files while maintaining the same image quality. JPEG2000 can reduce file sizes up to 20:1 with minimal degradation. It can compress up to 80:1; however, significant degradation occurs at this level.



In this example, the image on the right represents a portion of a fingerprint scanned using TIFF format and uncompressed. The image on the left is compressed with JPEG at 20:1 and the image in the center is compressed using JPEG2000 at 80:1. Note there is little or no difference in quality between JPEG and JPEG2000 even though there are substantial differences in the amount of compression.

Compression Artifacts

Compression artifacts are features created in the image that are not part of the original scene. Listed below, are some of the more common artifacts found when using excessive amounts of lossy compression.

Blocking - The JPEG algorithm breaks the image up into 8x8 blocks in each of the three-color channels. It processes each block separately, and then puts them all together again. In some cases, the blocks are very visible, and the colors appear altered.

Contouring – Exaggerated differences at edges and banding in a gradient.

Local color distortion – Appears as strange color patches in small locations on the image.

High frequency losses – Edges may appear fuzzy and fine detail patterns may be blurred.

Application of Compression

Compression can be applied at the time of capture or during processing and saving. This compression can be through hardware or software and may not be readily apparent to the user. The use of lossy compression and the degree to which it is applied is dependent on the end use. It may be acceptable to compress a Category I image that is used for documentation purposes. Lossless compression should be used on Category II images that are used for analysis; however, the use of lossy compression on these images does not preclude them from being analyzed if the pertinent features are retained. For more information on Category I and II images see SWGIT document "*Best Practices for Documenting Image Enhancement*".

Other Considerations

When considering compression, agencies have to balance cost, workflow, time, and image quality. Compression can make analysis more difficult even though the image is still usable. See SWGIT document "*Digital Imaging Technology Issues for the Courts*" for more information.

When considering an overall workflow agencies should test the system from beginning to end to make sure it meets their quality needs first. Concessions based on cost and timesavings can be considered afterward. Employees should understand the philosophy behind these decisions. Specific references to archiving can be found in SWGIT Document "*Best Practices for Archiving Digital and Multi-Media Evidence (DME) in the Criminal Justice System*".

Be aware that some images are compressed for transmission or storage. It may be necessary to inquire if a received file was compressed because a higher resolution image may be available. When received images are compressed, care should be taken not to compress them further. If further processing is required, it is preferable to save a copy of the file in an uncompressed format. Processing can continue as needed then save with no compression or a lossless method. **Note:** It is recommended that the submitting agency notify the receiving agency when compression is used.

Saving Compressed Files

When saving a lossy-compressed file, any changes made are permanent. Resaving the image in an uncompressed format does not recover the data lost. Multiple resaves of a compressed file may magnify changes due to compression. Simply opening, viewing, and closing a file without saving does not result in further compression or degradation.

Users should have a good understanding of the camera settings required to accomplish the specific task. The default camera settings may not always be the best. This is also true for image processing software. When multiple users are using the same equipment, the settings are usually based on the last user's settings.

File Formats

A file format is the structure by which data is organized into a file. A file format is the common language that allows data to be shared. File formats often allow the use of compression to reduce the size of the file. The selection of file format is dependent on equipment available, workflow, and end use.

Data in an image file commonly contains a header, data block and footer. The header contains information about the image file including the type of file format, compression algorithm and possibly other metadata. The data block is the image content data. The footer may contain information about where the file ends and possibly other metadata.

Information in the header instructs the computer on how to open the image content information contained in the data block. If the header information is lost, corrupted or inconsistent with the data block the image may not open.

Some operating systems use file extensions as a convenient way for the computer to anticipate what the file format will be. However, it should be noted that file extensions can be changed and may not represent the actual file format. When this occurs, it can create problems using the file.

Common File Formats

Many image file formats exist for different applications and vendors. This is not an all-inclusive list.

JPEG File Interchange Format (JFIF) and Exchangeable Image File (EXIF) are common file formats that store JPEG-compressed information. These file formats often use the file extensions .JPG or .JPEG. This leads to confusion between JPEG, which is a compression algorithm and JFIF/EXIF that are file formats.

The EXIF format is capable of storing a large amount of metadata. Typically, when a camera is set on JPEG, an EXIF file is the result. The advantage to using EXIF is that metadata is stored in the file and can be used to document changes.

.JP2 file format is the file format for the JPG 2000 compression algorithm.

Tagged Image File Format (TIFF) is a flexible format that can be compressed or uncompressed. TIFF images from digital cameras tend to be large because they are limited on amount of compression and has all of the color values for all of the pixels. Although not common, it is possible to add a tag to a TIFF image essentially making it proprietary. The TIFF specification allows the incorporation of diverse compression algorithms, including some that are lossy. While the most common algorithms associated with the TIFF format are lossless one can not assume this with every image.

Photoshop Document (PSD) is a format specific to Adobe software. In addition to the image information, all layer information is retained. It is useful for working within Photoshop but images cannot be used in most other applications. They are not suitable for archiving due their large size and proprietary nature.

RAW file format is not a specific file format but a class of formats. Each camera model essentially has its own version of a RAW file format. The data block of a RAW file contains the unprocessed pixel readings from the sensor chip and camera metadata.

Most RAW files are proprietary and specific to each camera model. Typically, cameras come with viewing software that requires conversion to a standard viewable format. Certain software packages also have utilities or plug-ins to handle these files but they are not necessarily compatible with all cameras.

Long-term storage of RAW files requires special considerations. There are many variables involved and it is dependent on camera model, sensor chip and processing. Each sensor has a specific way it captures data that will not be compatible with any other camera utility. Manufacturers are very hesitant about sharing this information. Provisions have to be made so that software and hardware will be available for opening the files in the future. Utilities provided by camera manufacturers are rarely supported beyond five years and may have compatibility issues with changes in operating system, file extension, etc. Open source RAW formats, such as Adobe Photoshop's Digital Negative (DNG) format, may simplify some of these cross platform concerns by converting a proprietary RAW format to an open source RAW format for archiving purposes.

There are resource considerations when capturing and storing in a RAW format. At some point, the original RAW file must be converted to a viewable format. The resulting image file after the conversion is considered a processed file and both files should be retained. This will have an impact on staff, storage facilities and equipment. It should be noted that once the conversion process has taken place the processed file cannot be converted back to its original RAW format.

Adobe Photoshop's Digital Negative (DNG) format is a royalty free RAW image format designed by Adobe systems. DNG is based on a TIFF format and mandates use of metadata. DNG was a response to demand for unifying camera RAW file formats.

Portable Network Graphics (PNG) format is used for internet applications. It does not support meta data.

Graphics Interchange Format (GIF) was originally developed by CompuServe for internet applications. It is an 8-bit format that has reduced color set, supports animation and LZW compression. It supports a non-rectangular image.

Bitmap (BMP) is a very basic format that allows most applications to open the image and store it using a different format.

Picture File (PICT) was primarily used in a Macintosh environment. It is rarely used today.

Other proprietary formats can exist that are formulated by vendors of turnkey systems. The vendor retains total control of the image using a key and third party software cannot open the file. The images may or may not be stored on site. These systems should be avoided.

Cautions

Knowing the characteristics and limitations of the compression and file format are essential to allow you to respond when an image is challenged.

Compression and changing file formats can strip metadata, and may or may not make the image unrecognizable or unusable.

Imaging management programs may alter metadata from the original file.

Incompatible file formats can create problems with interoperability between systems.

New algorithms are developed constantly that may not be valid. When implementing a new algorithm be sure to validate it.

Section 20

Recommendations and Guidelines for Crime Scene/Critical Incident Videography

OBJECTIVE

The objective of this document is to provide recommendations and guidelines for the use of video camcorders to document crime scenes and critical incidents. Crime scene/critical incident videography should not replace or take precedence over still photography, but can be used as an additional investigative or demonstrative tool.

INTRODUCTION

Crime scene/critical incident videography augments still photography by providing a portrayal of the crime scene that gives the jury a sense of being there. Crime scene/critical incident videography can provide the context of the scene or event and give perspective of the entire relevant area. It can also depict the relationship of items of importance to each other and the physical landmarks within the scene.

Commonly Documented Incidents

- Homicides, suicides, questionable deaths, violent crimes, arson
- Natural disasters: floods, hurricanes, weather related incidents
- Other disasters: terrorism incidents, bombings and explosions, mass transit/plane crashes, hazardous material incidents
- Crowd control incidents
- Evidentiary demonstrations/re-enactments
- Officer involved shootings

Equipment

The following list is recommended equipment for videography. Camcorders with removable media are recommended.

- Video camcorder
- AC adapter
- Fully charged batteries / charger
- Power inverter
- Video light with charger
- Appropriate media for camcorder (new blank tape or forensically wiped or formatted media)

- Sturdy fluid head tripod (with quick release)
- Lens cleaning solution and non-abrasive lint-free cloth
- External microphone (wireless or wired)
- Headphones or earphones
- Audio shorting plug (to disable audio)
- Duct or gaffer's tape
- Identification placards/slates
- Camera bag/hard case
- Rain cover for camera
- Lens cap
- Appropriate video/audio cables
- Neck strap to secure equipment
- Rubber gloves, masks, cloth or rubber booties and other personal protective equipment (PPE)

Maintenance

- Proper care and maintenance of equipment should be based on manufacturer recommendations.

- Continued proper operation of key components should be verified and documented on a regular basis, according to agency policy.

- For retention of equipment see SWGIT document "*Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System*".

Training

Personnel responsible for video documentation should have an understanding of the fundamentals of videography, knowledge of the video recording technology, equipment used, and a basic knowledge of commonly accepted crime scene procedures. The ability of a videographer to properly document a scene should be established and maintained through practical experience and training, both formal and on the job.

The videographer should have a basic working knowledge of his/her respective jurisdictions' legal processes. This knowledge should include familiarity with rules of evidence as they pertain to admissibility and reliability.

General Documentation Procedures

- Prior to arrival at the scene, verify all equipment is available and in proper working order. The date/time generator of the equipment should be verified for accuracy.

- Upon arrival, confer with the lead investigator. The investigator and videographer should walk through the scene without video equipment, noting all evidence or items of importance. The scene should be cleared of all personnel during video recording, when possible.

- The scene should be documented in the exact condition the videographer found it upon his/her arrival.

- Each scene should begin with a placard or slate containing information including date, time, location, videographer and case number. See Appendix A for a sample placard or slate. A brief audio recording of this information is also acceptable.

- In addition to the placard or slate, case notes should include equipment information (e.g. camera make, model and serial number).

- Unless circumstances dictate otherwise, audio should not be recorded during documentation. In instances where audio is required, it should be monitored for proper recording.

- All camera movements including pans, tilts and zooms should be conducted in a slow, smooth, and deliberate manner.

- Recordings may be paused and restarted. If possible, similar landmarks or items should be used as points of reference.

- Documentation of the scene should begin with a slow 360° pan of the exterior and surrounding area from a fixed position to document landmarks, lighting, traffic and other investigative factors.

- Record video throughout the scene showing the location and proximity of important items in relation to one another. Starting with the main point of entry, capture general images, proceeding to medium range images and conclude with close-ups.

- Confirm with the lead investigator that all locations and items of importance have been documented.

- If additional items not previously identified are located, document those items in the same manner.

- Confer with the lead investigator and conduct a brief visual verification of the recording prior to leaving the scene.

- Though the length of the video will be dependent on the complexity of the scene, an effort should be made to be as concise as possible. As an example, a single location with few items of importance should take no longer than twenty minutes.

Media Handling Procedures

These procedures are intended to protect the video from physical damage, accidental erasure, or other alterations.

Tape Based Media:

- Immediately after recording, remove the write protect tab from the tape cassette or slide the tab to the "SAVE" position.
- The tape should be labeled with the following when applicable: agency, videographer, location, date, time and case number.
- Protect the tape from magnetic fields such as those found near police radios, electric motors, solenoids and metal detectors.
- Avoid exposure to direct sunlight, excessive humidity and temperature extremes. Storage and transportation should be in a cool and dry environment.
- Create a copy of the original tape (including metadata such as time/date information) and verify its accuracy. The copy should be used for all subsequent viewing.
    - If the original videotape must be reviewed, it should not be paused.
- All copies and originals should be marked as such and handled in accordance with agency policy.

File Based Media:

- When possible, separate media should be used for each scene. Since the storage media may not be able to be labeled (e.g. internal camcorder hard drive), the placards or slates recorded at the beginning of each scene should be used to assist in the differentiation between scenes.

  Note: It is advisable to perform a forensic wipe of media before each use (including the first use) in order to prevent residual data from previous recordings from being included in unrelated cases.

- Protect the storage media (e.g. removable card, internal camcorder hard drive) from magnetic fields such as those found near police radios, electric motors, solenoids and metal detectors.
- Avoid exposure to direct sunlight, excessive humidity and temperature extremes. Storage and transportation should be in a cool and dry environment.

- After returning from the scene, prior to review, download and verify copies of the original digital files to an appropriate storage device/media. For more information, see SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*".

- A working copy should be produced for review and verified for accuracy. Working copies should be prepared in a commonly accepted file format, labeled appropriately, and should include metadata such as time/date information. These copies may be distributed in accordance with agency policy.

- Once copies of the original digital files are archived and verified, data remaining on the original recording media/device should be forensically wiped or formatted prior to reusing the media/device. For more information, see SWGIT document "*Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System*".

- If at any time a bit stream duplicate of the original recording media/device is produced, a forensic wipe must be performed prior to using the media/device.

Appendix A

Sample Identification Placard/Slate

Video Identification Card

Case Number:	**Date / Time:**
Location:	
Videographer:	**Lead Investigator:**
Comments:	

Section 21

Procedure for Testing Scanner Resolution for Latent Print Imaging

INTRODUCTION

The purpose of this document is to describe a procedure to ensure that a scanner can capture a latent print image at an achievable resolution that enables recording of level 3 detail.

LIMITATIONS

This procedure is designed to test the ability of a scanner in reflected light mode to capture the necessary level of detail when viewed on a monitor. This procedure does not address capture by a scanner in transmitted light mode. This procedure also does not address the output of image data to printed media.

A NOTE ON 1000 ppi STANDARD

The procedure described in this document is in accordance with current SWGFAST guidelines [Standard for Friction Ridge Digital Imaging (Latent/Tenprint)[1]], as well as National Institute of Standards and Technology (NIST) standard (NIST SPECIAL PUBLICATION 500-271, ANSI/NIST-ITL 1-2007[2]), which specify 1000 pixels per inch (ppi) at 1:1 as the minimum scanning resolution for latent print evidence. This standard appears primarily to be historical, though recent studies suggest that it is suitable for capturing level 3 detail[3].

While the 1000 ppi resolution standard permits the capture of level 3 detail in latent prints, it does not mean that any image recorded at a lower resolution would necessarily be of no value for comparison purposes. However, there are some latent print impressions that are so degraded or contain such limited quantity of information that at least 1000 ppi resolution is required to conduct an accurate examination. Some automated fingerprint identification systems require 1000 ppi for submission purposes.

As one commercial testing group notes, the relationship between nominal resolution and achievable resolution (sometimes called "resolving power") can vary greatly by manufacturer:

> …[T]here is … discrepancy between the nominal resolution of a scanner and the actual achievable resolution in the practice. In our film scanner tests we always measure the effective resolution of a scanner, thus the resolution that is achieved in practice… While in

[1] www.swgfast.org/standard_for_friction_ridge_digital_imaging_1.0.pdf Accessed January 12, 2010.
[2] http://fingerprint.nist.gov/standard/ Accessed January 12, 2010.
[3] Jain, A.K., Chen, Y., and Demirkus, M. Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features. IEEE Trans. PAMI 29 (1): 15-27, 2007.

> practice, [some] top-models achieve approximately 97% of their nominal resolution, in case of some film scanners of [other manufactures], the resulting value is of only 50%. Many times, the flat bed scanners with an integrated transparency unit only achieve 10-20% of their nominal resolution in practice. For the user, the effective resolution is the decisive value and not the nominal resolution…

Ref: Patrick Wagner Purchase of a film scanner, tips and purchase criteria http://www.filmscanner.info/en/FilmscannerKauf.html last accessed 11 Jan 2011

There is a dearth of peer reviewed literature comparing nominal and achieved resolution, but the achieved resolution can be approximated. Jain has demonstrated that sampling at a nominal 1000 ppi can provide level three detail. Zhang, et al. have similar results. By application of the Nyquist theorem, a 1000 ppi nominal resolution can theoretically achieve a maximum resolution of 500 line pairs. In practice, as noted elsewhere, Nyquist sampling is inadequate, and three to four samples are required instead of two, resulting in resolution between 250-330 line pairs per inch, or 9.8-13 cycles per mm.

Ref: Jain 2007 already in footnotes.
Ref: Zhang D, Liu F, Shao Q., Lu G, Luo N. Selecting a reference high resolution for fingerprint recognition using minutiae and pores. IEEE Trans Instrument. Meas. 2010 99:1-9

EQUIPMENT/MATERIALS

- Scanner (and associated software and connection to computer and monitor)
- Resolution test target (e.g., T-90-N-CG "Ultra High Resolution Target")
- Loupe or magnifier

To determine that a scanner is capable of capturing an image at a given resolution, it is necessary to use a test target. The test target used in this procedure is the T-90-N-CG "Ultra High Resolution Target", from Applied Image, Inc., Rochester, NY. This target is used as an example, only, and its use here should not be construed as an endorsement. Other test targets are available, such as from the International Standards Organization (ISO), which has a standard target for measuring resolution of scanners "ISO-16067-1 Reflective Scanner Test Chart."

DESCRIPTION OF RESOLUTION TEST TARGETS

Resolution test targets come in a variety of forms and styles. Horizontal and vertical multi-bar test targets are the focus of this procedure. Such multi-bar test targets consist of pairs of dark and light parallel lines ("bars") of equal width ("line pairs" or "cycle") which repeat at a given frequency. The frequency is then defined in terms of cycles per unit distance. On the T-90-N-CG chart, spatial frequencies are reported in cycles per millimeter.

As an example, a set of line pairs in which the width of each individual line is 0.1 millimeter (i.e., dark line width = 0.1 mm and light line width = 0.1 mm) would have a combined line pair width of 0.2 mm, and would be described as having 5 cycles per mm (1/0.2 = 5).

1000 ppi RESOLUTION AS MEASURED IN CYCLES PER MM

Because a nominal resolution of 1000 ppi corresponds to an achievable resolution of approximately 9.8-13 cycles per millimeter. Any test target within this range would be sufficient; the 12.5 cycle per millimeter region of the T-90-N-CG chart is demonstrated.

PROCEDURE

1. Locate the portion of the test chart which depicts 12.5 cycles per millimeter (See Figure 1.)

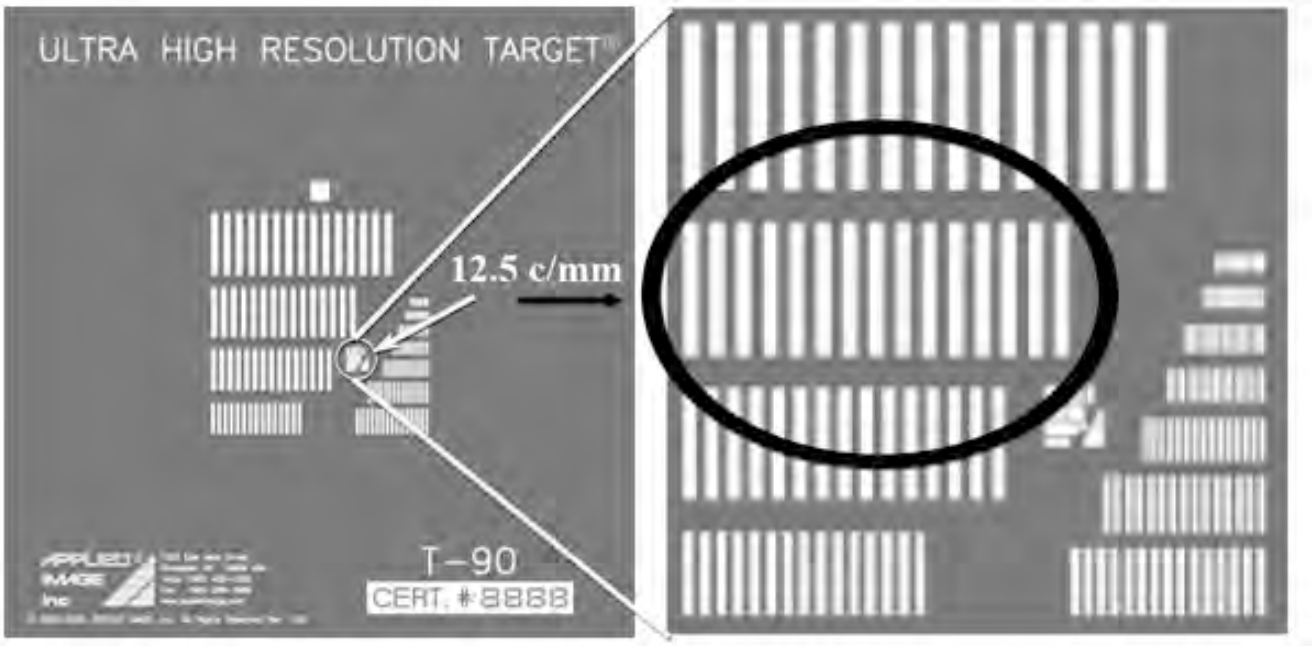


Figure 1.

2. Visually verify (count) the number of dark and light lines and record each (e.g., 15 light and 14 dark – See Figure 2.). It is recommended that a magnifier or loupe be used in the counting process.

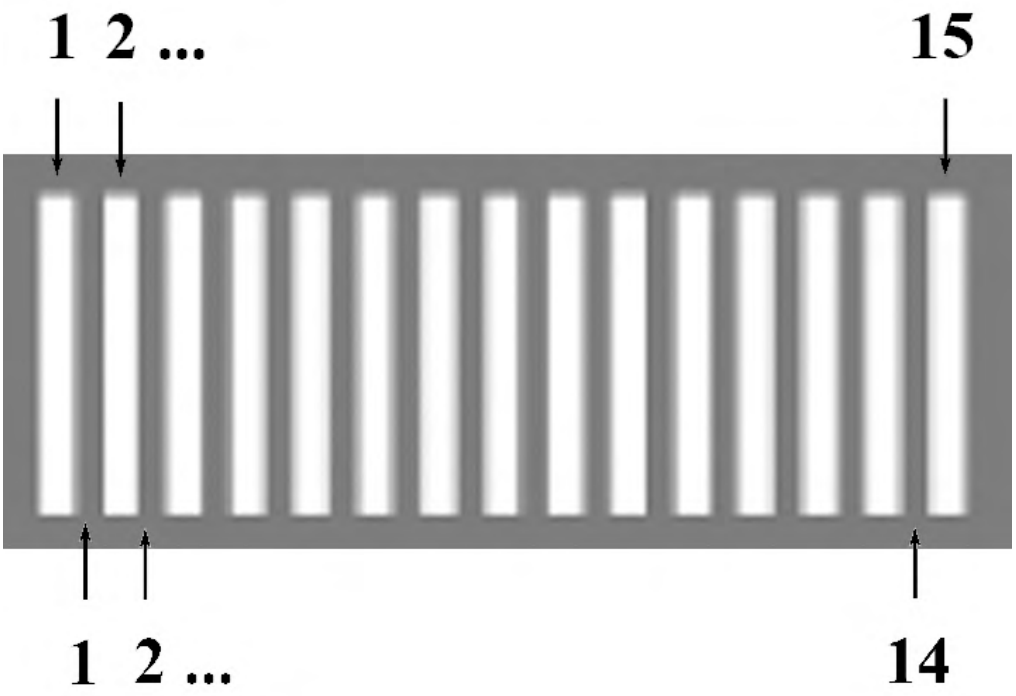


Figure 2.

3. Ensure scanner is on and set operational parameters to those normally used for scanning of latent print evidence, as appropriate.

4. If not already done in Step 3, set scanner to 1000 pixels per inch.

5. Place test chart on scanner platen with top of chart at top of scanning region. This will allow the user to measure the resolution in the horizontal aspect (as depicted in figures above).

6. Activate scanner.

7. Save file using either lossless compression or no compression (such as TIFF or Bitmap).

8. Open file in image processing application.

9. View region which depicts 12.5 cycles per mm.

10. Zoom image so that individual pixels are visible. If the scanner has accurately captured 12.5 cycles per mm, then it should be possible to distinguish the dark and light line pairs in this region. It should not be necessary to use image post processing to improve the visibility of the line pairs.

11. To confirm accurate capture, it is necessary to verify that the correct number of dark and light line pairs per mm have been recorded by counting them and checking this number against the number recorded in step 2 (e.g., 15 light and 14 dark).

12. If the number counted in step 11 matches the number counted in Step 2, then you have verified that your scanner can sample at 12.5 cycles per millimeter in the horizontal direction and exceed the 1000 ppi standard. If not, then your scanner does not meet the 1000 ppi standard and the scanner should be set to a higher nominal resolution and retested. Note that some scanners exhibit higher achievable resolution in the center of the scan area. Thus, it may be appropriate to retest at different locations on the scanner.

13. Rotate the chart 90° either to the right or left and repeat steps 6 through 12 to measure vertical resolution.

It is recommended that this process be documented in accordance with agency policy.

It is further recommended that this procedure be repeated on a regular basis (e.g., annually) in accordance with agency quality assurance and quality control practices. Likewise, if the scanner requires repairs, then this procedure should be performed prior to use in case work.

Section 22

Procedure for Testing Digital Camera System Resolution for Latent Print Photography

INTRODUCTION

The purpose of this document is to describe a procedure to ensure that a digital camera system can capture a latent print image at an achievable resolution that enables recording of level 3 detail.

LIMITATIONS

This procedure is designed to test the ability of a digital camera system to capture the necessary level of detail when viewed on a monitor. This procedure does not address the use of film cameras or output of image data to printed media.

A NOTE ON 1000 ppi STANDARD

Historically, latent prints were photographed so that an image on film, when developed, would be at the exact same dimensions as the latent print itself ("1x" or "1:1"). This would allow for rapid contact printing for comparison against record prints. Digital imaging workflow is not based on the physical size of the capture device (as was the case with film cameras), rather, it is based on the resolution required to capture the necessary detail in the digital image file.

The procedure described in this document is in accordance with current SWGFAST guidelines [Standard for Friction Ridge Digital Imaging (Latent/Tenprint)[1]], as well as National Institute of Standards and Technology (NIST) standard (NIST SPECIAL PUBLICATION 500-271, ANSI/NIST-ITL 1-2007[2]), which specify 1000 pixels per inch (ppi) at 1:1 as the minimum nominal scanning resolution for latent print evidence. This standard appears primarily to be historical and directed towards scanners, rather than cameras, though recent studies suggest that it is suitable for capturing level 3 detail[3].

While the 1000 ppi resolution standard permits the capture of level three detail in latent prints, it does not mean that any image recorded at a lower resolution would necessarily be of no value for comparison purposes. However, there are some latent print impressions that are so degraded or contain such limited quantity of information that at least 1000 ppi resolution is required to conduct an accurate examination. Some automated fingerprint identification systems require 1000 ppi for submission purposes.

[1] www.swgfast.org/standard_for_friction_ridge_digital_imaging_1.0.pdf Accessed January 12, 2010.
[2] http://fingerprint.nist.gov/standard/ Accessed January 12, 2010.
[3] Jain, A.K., Chen, Y., and Demirkus, M. Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features. IEEE Trans. PAMI 29 (1): 15-27, 2007.

As one commercial testing group notes, the relationship between nominal resolution and achievable resolution (sometimes called "resolving power") can vary greatly by manufacturer:

> …[T]here is … discrepancy between the nominal resolution of a scanner and the actual achievable resolution in the practice. In our film scanner tests we always measure the effective resolution of a scanner, thus the resolution that is achieved in practice… While in practice, [some] top-models achieve approximately 97% of their nominal resolution, in case of some film scanners of [other manufacturers], the resulting value is of only 50%. Many times, the flat bed scanners with an integrated transparency unit only achieve 10-20% of their nominal resolution in practice. For the user, the effective resolution is the decisive value and not the nominal resolution…

Ref: Patrick Wagner Purchase of a film scanner, tips and purchase criteria http://www.filmscanner.info/en/FilmscannerKauf.html last accessed 11 Jan 2011.

As with scanners, camera systems also rarely achieve nominal resolution in practice. One recent study showed that high-resolution black-and-white TMAX film with a nominal resolution of 34.56 megapixels using a stabilized professional camera under studio conditions was able to achieve a pixel-equivalent resolution of 13.75 megapixels.

Ref: Herbert Blitzer, Karen Stein-Fergusen, Jeffrey Huang. Understanding Forensic Digital Imaging. Academic Press. 2008 Chapter 17, p 320.

There is a dearth of peer reviewed literature comparing nominal and achieved resolution, but the achieved resolution can be approximated. Jain has demonstrated that sampling at a nominal 1000 ppi can provide level three detail. Zhang, et al. have similar results. By application of the Nyquist theorem, a 1000 ppi nominal resolution can theoretically achieve a maximum resolution of 500 line pairs. In practice, as noted elsewhere, Nyquist sampling is inadequate, and three to four samples are required instead of two, resulting in resolution between 250-330 line pairs per inch, or 9.8-13 cycles per mm.

Ref: Jain 2007 already in footnotes.
Ref: Zhang D, Liu F, Shao Q., Lu G, Luo N. Selecting a reference high resolution for fingerprint recognition using minutiae and pores. IEEE Trans Intrument. Meas. 2010 99:1-9

Equipment/Materials

- Camera system (including tripod, lens, copy lighting, filters)
- Computer hardware to include monitor and image processing software
- Scale
- Resolution test target (e.g., T-90-N-CG "Ultra High Resolution Target")
- Loupe or magnifier

To determine if a camera system is capable of capturing an image at a given resolution, it is necessary to use a test target. The test target used in this procedure is the T-90-N-CG "Ultra High Resolution Target", from Applied Image, Inc., Rochester, NY. This target is used as an example only, and its use here should not be construed as an endorsement. Other test targets are available, such as from the International Standards Organization (ISO), which has a standard target for measuring resolution of scanners "ISO-16067-1 Reflective Scanner Test Chart." ISO also has a test chart for digital and electronic imaging devices (ISO 12233 Test Chart), but this chart does not include explicitly defined regions at the resolution of interest for this procedure. Therefore, its use in this procedure would be problematic.

DESCRIPTION OF RESOLUTION TEST TARGETS

Resolution test targets come in a variety of forms and styles. Horizontal and vertical multi-bar test targets are the focus of this procedure. Such multi-bar test targets consist of pairs of dark and light parallel lines ("bars") of equal width ("line pairs" or "cycle") which repeat at a given frequency. The frequency is then defined in terms of cycles per unit distance. On the T-90-N-CG chart, spatial frequencies are reported in cycles per millimeter.

As an example, a set of line pairs in which the width of each individual line is 0.1 millimeter (i.e., dark line width = 0.1 mm and light line width = 0.1 mm) would have a combined line pair width of 0.2 mm, and would be described as having 5 cycles per mm (1/0.2 = 5).

1000 ppi RESOLUTION AS MEASURED IN CYCLES PER MM

Because a nominal resolution of 1000 ppi corresponds to an achievable resolution of approximately 9.8-13 cycles per millimeter. Any test target within this range would be sufficient; the 12.5 cycle per millimeter region of the T-90-N-CG chart is demonstrated.

PROCEDURE

This procedure should be repeated for every lens, filter, configuration (aperture, ISO, etc.) and close-up accessory combination used regularly in the capture of latent print images.

Prior to testing for resolution, it is necessary to determine the camera system's field of view to record at the equivalent of 1000 pixels per inch or more at the target (Part 1). This establishes a starting point for defining the field of view which may be modified based on the results of Part 2.

Part 1: Field of view determination to achieve a minimum of 1000 ppi

The pixel dimensions on the sensor define the area of maximum coverage for 1000 ppi. The reader should refer to the specifications for the camera being tested to determine what values are appropriate.

1. Determine the number of effective pixels for the camera. See the manufacturer's specification sheet for this value. For this procedure, a 12-megapixel camera with 4288 x 2848 effective pixels is used as an example.

2. Divide the pixel resolution by 1000. In this example, 4288 x 2848 pixels divided by 1000 pixels per inch results in 4.288 x 2.848 inches (4-1/4 x 2-13/16 inches). This represents the area of coverage in which the camera should be capable of capturing at 1000 ppi.

3. Make a template (or frame) to the exact dimension of this area of coverage (4-1/4 x 2-13/16 inches).

4. Place template on a flat surface.

5. Insert a flat scale inside the area bounded by the template.

6. Mount camera on tripod or copy stand above the flat surface on which the template rests. Ensure the camera focal plane is parallel with flat surface.

7. If using a fixed focal length lens, proceed to step 8. If using a zoom lens, proceed to step 9.

8. While looking through the viewfinder, adjust the height of the camera to fill the frame with the template, while keeping the image in sharp focus with the camera set to manual focus and manual exposure. If focus cannot be accomplished for this lens, then the 1000 ppi standard cannot be met and the test should be terminated for that lens. Otherwise, go to step 10.

9. When using a zoom lens, repeat step 8 for each of the zoom settings that will be used for photographing latent prints. This will result in different camera heights for different zoom settings. If focus cannot be accomplished for some zoom settings, then the 1000 ppi standard cannot be met for those settings. If focus cannot be accomplished for this lens at all, then the 1000 ppi standard cannot be met and the test should be terminated. Otherwise, go to step 10.

10. Record the height determined in step 8 or 9. This height is the maximum camera-to-subject distance to provide 1000 ppi resolution.

11. The camera setup is ready to replace the template with the resolution test target and proceed to Part 2.

Part 2: Camera setup for latent print photography

1. Locate the portion of the test chart which depicts 12.5 cycles per millimeter (See Figure 1.)

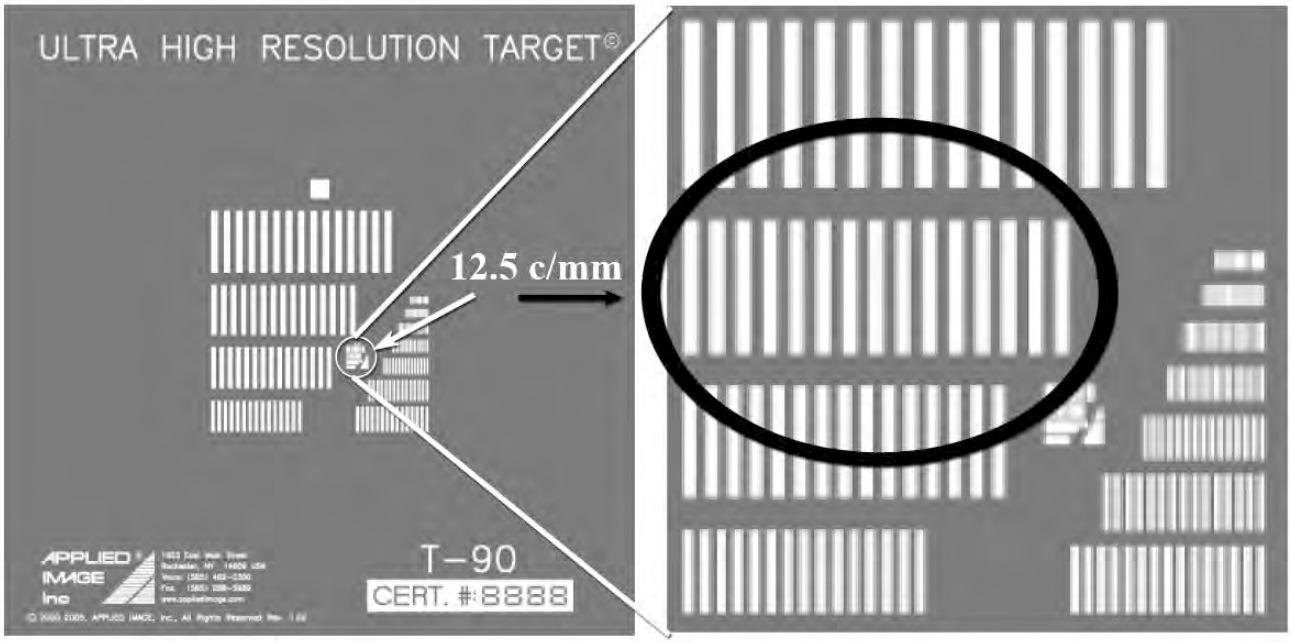


Figure 1.

2. Visually verify (count) the number of dark and light lines and record each (e.g., 15 light and 14 dark – See Figure 2.). It is recommended that a magnifier or loupe be used in the counting process.

Figure 2.

3. Place test chart on flat surface below camera so the test bars are in a vertical orientation (see Figure 2 above). The camera back must be parallel to this surface.

4. Set the camera using manual focus and manual exposure controls.

5. Select camera settings to capture image file using normal file format used for latent print image capture. NOTE: SWGIT recommends the use of lossless file formats such as RAW or TIFF when capturing latent print images. The use of file formats that utilize lossy compression can introduce artifacts which may invalidate the test results.

6. Capture an image file with the camera.

7. Open file in image processing application.

8. View region which depicts 12.5 cycles per mm using the workstation monitor.

9. Zoom image so that individual pixels are visible. If the camera has accurately captured 12.5 cycles per mm, then it should be possible to distinguish the dark and light line pairs in this region. It should not be necessary to use image post processing to improve the visibility of the line pairs.

10. To verify accurate capture, it is necessary to verify that the correct number of dark and light line pairs per mm have been recorded by counting them and checking this number against the number recorded in step 2 (i.e., 15 light and 14 dark).

11. If the number counted in step 10 matches the number counted in step 2, then you have verified that this camera system configuration can sample at 12.5 cycles per millimeter in the horizontal direction and meets or exceeds the 1000 ppi standard. If not, then this camera system configuration does not meet the 1000 ppi standard. Resolution may be increased by decreasing the field of view (zoom in or get closer); some cameras may allow other types of resolution adjustments.

12. Rotate the chart 90° either to the right or left and repeat steps 3 through 11 to measure vertical resolution. In some cases, the resolving power of the camera may be lower in the horizontal or vertical direction. Therefore, the shorter of the two distances determined should be recorded and used.

13. If resolution was modified by changing the field of view, the final distance from the target should be recorded for future use. This can be implemented in several ways, such as but not limited to, a string of the known length used to measure the maximum camera to subject distance or a template to determine the maximum field of view.

It is recommended that this process be documented in accordance with agency policy.

It is further recommended that this procedure be repeated on a regular basis (e.g., annually) in accordance with agency quality assurance and quality control practices. Likewise, if the camera requires repairs, then this procedure should be performed prior to use in case work.

Section 23

Best Practices for the Analysis of Digital Video Recorders

The objective of this document is to provide guidance regarding appropriate practices in the retrieval of video/audio evidence and any associated metadata (referred to in this document as data) from Digital Closed Circuit Television (DCCTV) systems that record to a Digital Video Recorder (DVR). This document specifically addresses DVRs that have been powered down or removed from the scene.

It is strongly recommended to retrieve data at the scene while the DVR is still powered on and operational. For the best practices regarding on-site retrieval methods, see Technical Support Working Group (TSWG) "*Best Practices for the Retrieval of Digital Closed Circuit Television Systems*" [1] and Home Office Scientific Development Branch (now referred to as the Home Office Centre for Applied Science and Technology (CAST)) "*Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0*" [2].

If determined that data retrieval at the scene is not feasible, practical, or appropriate, the procedures outlined in this document should be followed to maximize the likelihood that the data is preserved and accessible for playback.

DVR analysis may not follow the methodologies from the computer forensics discipline. The key differences between DCCTV retrieval and a computer forensic examination are that the recording device's operational settings may have to be reconfigured to retrieve the video data, the entire system contents may not require a forensic examination, and typically the owner of the DVR is not the subject of the investigation.

This document does not address the examination of hard disk drives (HDDs) submitted without the DVR. In instances where HDDs are submitted without the DVR, every reasonable attempt should be made to obtain the DVR that recorded the data to the HDD. In addition, recovery of data via reverse engineering techniques is not addressed.

This document refers to the internal storage of the DVR as HDD(s), but DVRs may have alternative storage media (e.g. flash media). Some adjustments to the DVR analysis workflow may be required on a case by case basis.

This document is not intended to address Forensic Video Analysis techniques that may be performed after the retrieval of data. For guidance on Forensic Video Analysis, see SWGIT document "*Best Practices for Forensic Video Analysis*". For guidance on Forensic Audio see SWGDE document "*Best Practices for Forensic Audio*".

[1] http://www.tswg.gov/subgroups/isf/electronic-evidence/DCCTV_Web_doc.pdf
[2] http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08_Retrieval_of_Video_Ev12835.pdf?view=Binary

BEST PRACTICES

The following are guidelines that describe the SWGIT recommended best practices for DVR analysis.

Evidence Management

Agencies should have documented procedures for the handling, transportation, and storage of evidence. Agencies should have chain of custody procedures in place and should follow these procedures.

At all times precautions should be taken to ensure evidence is protected from external factors that may cause damage to the DVR, media or to the data contained on the media (e.g. magnetic fields, static electrical charges, and electrical hazards).

Quality Control and Quality Assurance

Quality control and quality assurance policies and procedures should be implemented and documented. Technical and administrative peer reviews are integral components of quality control.

Safety

Carry out a risk assessment in order to identify any potential hazards that may arise due to the condition of the DVR, taking account of the following:

Electrical shocks can occur if the device is opened or dismantled.

Electronic devices inappropriately connected may short circuit causing malfunction, loss of data and failure.

Foreign substances may be present on the evidence, it is recommended that protective gloves and eye gear be worn since these substances may carry blood-borne pathogens.

Security

There should be procedures in place to maintain the security of the working data, all notes, and other such analysis related materials to provide the level of security and privacy needed by the organization. For example, archived case related materials should be stored in a manner that limits access. The degree of access will be agency specific.

Infrastructure

Agencies should have sufficient space, equipment and facilities to adequately support the required quality and volume of work.

Work Management

DVR analysis is a labor-intensive process. An upper limit on caseload should be established for every category of tasks.

Documentation

Agencies should establish standards for information included in, and the format for, reporting results.

Training, Competency, and Proficiency

Analysts and/or examiners are encouraged to review SWGIT "*Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System*", "*SWGIT/SWGDE Guidelines and Recommendations for Training in Digital and Multimedia Evidence*", "*SWGIT/SWGDE Proficiency Test Program Guidelines*", Technical Support Working Group (TSWG) "*Best Practices for the Retrieval of Digital Closed Circuit Television Systems*" [3] and Home Office Scientific Development Branch (now referred to as the Home Office Centre for Applied Science and Technology (CAST)) "*Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0*" [4].

Analysts should have certification in their knowledge domain and associated forensic discipline, when such certification is appropriate and available. Note, however, that the existence of an external professional certification program does not imply that it is necessary, sufficient, or appropriate.

Analysts should demonstrate competency in their discipline prior to being assigned unsupervised case work responsibilities. Analysts should remain proficient through continuing education, training, and peer review of examinations. Agencies should document competency, proficiency and continuing education for each analyst.

The analyst should demonstrate:

- an understanding of the scope of work and how it will be applied in the forensic environment;
- subject matter knowledge and competence;
- working knowledge of DVR recording technology, retrieval methods and evaluation techniques;
- working knowledge of applications and tools utilized in the specific agency;
- working knowledge of SWGIT guidelines for capturing, storing, and processing image/video and audio, including issues relating to topics such as data integrity and compression artifacts;
- understanding of relevant legal precedents;
- knowledge of appropriate case work documentation.

Standard Operation Procedures (SOPs)

There should be Standard Operating Procedures (SOPs) in place for the analysis being performed. These SOPs should be agency specific, reflect the workflow and be general enough to permit flexibility for the required tasks.

[3] *Ibid.*
[4] *Ibid.*

Evidence Marking
Evidence needs to be marked per agency policy. Markings could include labelling with initials, ID number, case number or any other identifying information.

Any identifying information (such as serial numbers) should be documented.
Inappropriate marking or labelling methods may affect playback and could potentially damage the evidence.

Avoid use of markers that contain solvents.

Avoid use of adhesive labels other than on outside solid surfaces.

Chain of Custody
Throughout the entire DVR analysis process, chain of custody must be maintained per agency policy.

Submission Review
A submission form should be completed for every case the examiner receives, regardless of what type of examination or service the requestor is seeking. ***See Appendix A for an example***.

Ensure examiner safety is maintained by determining and documenting whether biohazards such as blood or body fluids are present or other special handling is required.

Determine if other examinations (such as latent print or trace evidence) are required and identify appropriate measures to ensure evidence integrity.

DVR ANALYSIS WORKFLOW

Note: The following workflow should only be performed by trained individuals who are competent and proficient in its proper use and application.

1. Document the physical condition of the evidence (which may include photographs). Physical inspection may include the following:
    - Physical damage
    - Contaminants (e.g. direct, grease)
    - DVR characteristics (e.g. make, model, number of cameras, serial number)
    - DVR output options (e.g. optical drive, USB, network)
    - Existing labels or identifiers
    - When possible, determine if removable media is present in the DVR (e.g. flash media or CD/DVD in the drive).

    Note: If optical media is located, it is appropriate to remove the media, perform a physical inspection and label appropriately. If flash media is located, do not remove the media until research is conducted to determine its contents (e.g. video data, system data).

2. Verify all necessary components, documentation and software are enclosed with the evidence. Examples of these include peripherals, keys, user manuals, passwords, etc.

Multiple levels of access and required passwords may exist, and not all may allow access to export the proprietary data.

Any deficiency should be documented and resolved, if possible, before beginning any forensic analysis (e.g. obtaining required peripheral device or replacement of a damaged power supply). If necessary, contact the submitter and/or other sources to obtain the needed item or information.

3. Prior to continuing analysis, read the user manual and literature. Refer to any additional resources as appropriate. Pay particular attention to potential issues addressed in the manual that may provide additional guidance regarding the course of analysis (e.g. the removal of the HDD may cause the data not to play back in the DVR or a specific brand of HDDs may be required by the DVR).
4. Photograph the DVR and media (such as internal HDDs) in order to document location, connections and physical condition.
5. Mark internal cables and HDDs for identification and proper placement/orientation.
6. Remove the HDD(s) from the DVR using appropriate tools including anti-static protection, as needed.
7. For each HDD, document the make, model, interface, capacity, serial number and jumper settings.
8. Conduct physical inspection of the HDD(s) and label as appropriate.
9. Produce a forensic clone of the HDD(s).
    - It is strongly recommended that forensic clones are produced as opposed to forensic image files.
    - The same make, model and size HDD(s) should be used for the forensic clone(s) when possible.
10. Retain the original HDD(s) as evidence and continue analysis using the forensic clone(s).
11. Properly label the forensic clone(s).
12. Confirm the jumper settings, if present, of the forensic clone(s) are in the same configuration as the original HDD(s).
13. Install the forensic clone(s) in the DVR.
14. Confirm the DVR and external power supply voltage settings are correct.
15. Boot the DVR. Confirm the forensic clone(s) are recognized by the DVR and the data is playable.

    Note: The boot process and/or the HDD menu of the DVR may indicate whether the forensic clone(s) are recognized.

    - If the DVR does not power on or boot successfully, check the following:
        - External power to the DVR is connected properly and the DVR and the forensic clone(s) are receiving power.

- All power switches have been turned on. Some DVRs have multiple power switches.
- Consider using an alternative available power connection, from the motherboard or external source, to the forensic clone; it may have different power requirements than the original.
- Internal cables are secure, operating properly and connected in the correct order (e.g., IDE master/slave configuration). This is predominantly an issue with PC based DVRs which store system files on internal HDD(s).
- DVRs can contain CMOS batteries that if depleted may prevent booting (this can also cause all settings to be lost). Check and replace, if necessary, keeping in mind that important settings can be permanently lost.

- If the DVR boots successfully, but the forensic clone(s) are not recognized, check the following:
  - Make, model and size of the forensic clone(s) are the same as the original HDD(s).
  - Forensic clone(s) are properly installed and connected to the DVR.
  - Cables are secure, operating properly and connected in the correct order (e.g., IDE master/slave configuration).
  - Jumpers are in the correct position, which may differ between the forensic clone(s) and the original HDDs due to brand variances, and may need to be changed to "master" if hard disk write blockers are being used in the chain.
  - Consider using an alternative available power connection, from the motherboard or external source, to the forensic clone; it may have different power requirements than the original.
  - Forensic clone(s) are receiving power and operating properly (e.g. spinning).
- If the forensic clone(s) are recognized by the DVR, but the data is not playable, check the issues addressed above. In addition, the following steps should be considered:
  - Check the DVR for an indication of the amount of recorded footage and/or available storage for recording.
  - Use a hexadecimal editor (e.g. WinHex) to confirm the HDD is not blank.
  - Determine the last time the recorded video was viewed, how the DVR was collected, and whether the DVR has been accessed since collection.
  - Review system documentation and/or contact the manufacturer for guidance.

Note: These issues may reflect the index of the DVR (which associates metadata with recorded footage) has been changed, corrupted, or deleted. The manufacturer may be able to assist with technical knowledge of processes to enable playback. If the index has been deleted, search functions are unlikely to work. Try pressing the play button to attempt to access recent recordings and then rewind to see if video of interest is present.

- If successful results are still not obtained, the DVR may be faulty. Non-evidentiary media (e.g. HDD) should be used to produce test recordings and to verify test recordings play back as expected. If, after testing, the DVR has been determined to be faulty, contact the manufacturer to determine the appropriate course of action. Solutions may include replacement of parts according to manufacturer specifications, or replacement of the DVR with a properly functioning unit.
- If the DVR has been determined, through testing, to be operating properly, the following procedures may be required to retrieve the data. Prior to performing these procedures, the investigator should be informed of the technical challenges and advised of the risks in proceeding.
    - Use of write protection hardware in conjunction with the DVR and original HDD(s) for analysis.
    - Use of the original HDD(s) and DVR without write protection for analysis. Prior to using the original, ensure your forensic clone has not been altered by validating the hash value. If necessary, produce a new forensic clone.

Note: If followed, the DVR analysis workflow described within this document produces successful results in a vast majority of cases. If this process is not successful, consider consulting an individual trained in the interpretation and extraction of data.

16. Conduct an examination of the DVR (logged in as administrator or technical equivalent) in its powered on state.

    Note: Changing the original settings may be necessary to conduct this examination. If settings are changed, document the original configuration and what changes were made.

    Determine the following:

    - System date and time as reported by the DVR and current date and time to establish an approximate offset.

    Note: It is recommended that any previous time and date checks that may have been carried out on the DVR prior to submittal be documented to check for potential anomalies. For example, the clocks on some DVRs do not increment when in a powered off state, or the clock may have reset to a default time after being powered down during seizure.

    - System manufacturer, firmware version, proprietary software name and version.

- Additional user names and passwords.

- Number of cameras capable of being recorded, how many were connected and how many were recording during period of interest.

- Current settings of the DVR to include: motion recording, event recording, frame rate, frame size, compression setting.

- Native and open file format .

17. Conduct an assessment of the DVR to determine the following information:
    - The data for the pertinent date and time was recorded and is present on the DVR.
        - If the data does not appear to be present, verify through all search options listed in the manual that data cannot be located by another search mechanism.
    - Earliest recorded date and time located as well as last date and time recorded.
    - Non-contiguous timeframes (such as missing days) should be identified and documented when appropriate.
    - Pertinent segment(s) of interest and the amount of data to be recovered from the DVR.
    - DVR data recovery options and which one may provide the native file format or otherwise best evidence.

18. By referencing the information gathered during the physical inspection, research and system examination, a protocol should be formulated for the best retrieval method for the recorded data. The specific steps and the order in which they are performed may vary. The procedure may include the following:
    - Internal archival device (e.g. CD/DVD writer, flash media drive).
    - Data transmission connection (e.g. USB, Firewire).
    - Network connection (e.g. Ethernet).
    - Video signal connection (e.g. S-Video, composite).

19. If data collection is determined to be the best method of retrieval, and the amount of data to be collected has been determined, conduct a test download to calculate the amount of media and physical time necessary for the retrieval.

20. Download the native or proprietary data to non-rewritable media. It is recommended to also retrieve an open file format.

21. If the data is downloaded to rewritable media, transfer the data to a non-rewritable media or secure electronic storage as soon as practical.

- Downloaded data not stored on non-rewritable media requires equivalent levels of protection, such as access control and tamper-proof logs.

22. Large amounts of data may be retrieved and placed on one or more hard drives. If the data is not otherwise stored as prescribed above, these hard drives then become evidence.

23. Calculate, verify and document hash values, when applicable.

24. Make sure all required proprietary software and/or codecs are included.
    Verify the native and/or open file format data is accessible on a separate computer.

25. It is recommended to also collect a digital or analog magnetic recording of the data (e.g. Mini-DV)

26. Document data retrieved from the DVR:
    - Date and time ranges for each camera
    - File format(s)
    - Magnetic recording(s)

27. If settings on the DVR were changed during examination, return them to the previous settings, if applicable.

28. If applicable, provide a copy of the proprietary software with playback instructions.

29. Confirm that the DVR operates as expected prior to return.

30. When the system is sent back to the submitter, return the DVR with the forensic clone(s) installed and the original HDDs packaged separately. This is the preferred method, but agency policy regarding the return of evidence should be taken into consideration.

TECHNICAL CONSIDERATIONS

The procedures described within this document are recommended best practices. However, due to the proprietary and often limited functionality of some DVRs, technical consideration should be taken to prevent mechanisms which may result in lost or inaccessible data. These considerations include the following:

- Improper removal of the DVR from the scene or hard drives from the DVR may result in loss of data and/or difficulty in playback of the data
- Disconnecting the HDD from the main board of the DVR may cause the HDD to be permanently disassociated from this device, rendering the data inaccessible by that device.
- Clone copy HDDs may be unrecognizable by the DVR.
- Connecting a HDD write blocker in line with the HDD may result in the HDD being unrecognizable by the DVR.
- Some DVRs are equipped with timed expiry which can result in the data becoming inaccessible by the device.

- Some DVRs go into auto-record mode when switched on, even if no video source is connected. For non PC-based DVRs, consider booting without the HDDs connected, allowing password to be determined without risk of data being overwritten. Once the password has been established it should be possible to disable the recording if auto record mode is engaged. This may involve turning off all or a combination of the following settings: manual, circular, scheduled, event and motion recording. Any changes made to settings should be noted.

Appendix A – Sample Video Submission Form

SUBMISSION OF VIDEO EVIDENCE

Date		Agency Case #		
Submitter Name & Title				
Agency				
Offense		Phone #	Cell #	
Offense Date		Email		
VICTIM (or SUBJECT)		**RACE**	**SEX**	**DOB**
1				
2				
SUSPECT		**RACE**	**SEX**	**DOB**
1				
2				

Brief Details of Case (Attach Report if Necessary)

_____
_____
_____
_____

Examinations Requested

_____
_____
_____
_____

Item(s) Submitted (including seals & packaging)

_____
_____
_____
_____

CCTV System Information

Digital Video Recorder Make, Model, Serial Number _____

Computer Based Stand Alone Networked (Circle One)

Playback software name and version_____

Software provided with evidence YES or NO (Circle One)

System and/or Software Password _____

Included Peripherals/Manuals _____

Retention Time (if known)

_____

System Settings:

Image Quality (i.e. high, medium, low) _____

Frames per second (fps)/pictures per second(pps) _____

Image/Frame recorded size (e.g. 320 x 240) _____

Can it be determined if any cameras are alarm or motion triggered? _____

Number of hard drives, storage capacity of each _____

System firmware version _____

Other available system settings (e.g. event log)_____

Hybrid or Other Equipment Make, Model, Serial Number_____

VHS SVHS Other _____ (Circle One)

What record mode was the system? (Circle One) 2 hour, 6 hour, 12 hour, 24 hour, 48 hour,72 hour, Other _____ Unknown

Multiplexer YES or NO Make and Model _____

Basic Information

Does the recorded date/time accurately represent the time of day? (circle) YES or NO

Date/Time displayed _____

Actual date/time _____

# of Camera/s _____ Active # of cameras _____

Camera make and model _____

Are any cameras infrared-sensitive and if so identify _____

Is audio being recorded? _____# of microphone/s _____

Is a copy of the most current maintenance/service log attached? (circle) YES or NO

Other Information: _____
_____

Scene Contact Information

Scene Address _____

Hours of operation_____

Scene point of contact _____Telephone: _____

CCTV system point of contact _____ Telephone: _____

Location of Equipment at Scene _____

Please provide a sketch of the scene indicating camera/microphone position and placement.

Submitted By _____ **Print Name**_____
Signature

Recommended Guidelines for Developing Standard Operating Procedures

Introduction:
Standard Operating Procedures (SOPs) are agency unique documents describing the methods and procedures to be followed in performing routine operations. SOPs are essential to improve the quality and to implement uniform processes for conducting digital & multimedia evidence forensic tasks in a precise, accurate manner. SOPs should be task-based and written for each procedure conducted. They should be reviewed at least annually. The previously approved versions of an SOP should be retained for reference.

Scope:
SOPs should conform to agency-specific policies. Such policies may address document format, workflow, approval process, and tasks performed. SOPs may be stored separately, in one large collected manual, or organized by functional unit. For instance, a single manual may be more convenient, but having separate SOP documents may be more amenable to the discovery process. SOPs should contain all information necessary to perform the task being described. Individual agency needs and/or processes will dictate what information is necessary.

General Guidelines:
SOPs may include but are not limited to:

- The name of the SOP, effective date and/or other version control.
- The purpose and scope of the SOP.
- Definitions and abbreviations that are not commonly used or have a special connotation in the SOP. The source of these definitions should be cited.
- A list of equipment, materials and standards/controls.

    - **Note:** Since equipment and material lists are frequently updated, it may be beneficial to create a separate listing of this equipment. This will allow for a document that can be updated independent of the SOP.

    - Equipment calibration and similar preparatory steps, if applicable.
    - Any known limitations of the equipment, software or procedure.
    - A list of steps used in performing the task, including appropriate parameters or options to be used.
    - Appropriate references. This may include equipment manuals, other published procedures, journal references, etc.
    - Any additional information/materials the examiner needs to be aware of that are not already included in the sections above, such as safety issues or

operational precautions.
- Authorization and approval information.

Sample SOPs are provided for your reference. These are examples only and are not meant to be boilerplate.

Section 24

Best Practices for the Retrieval of Digital Video

Purpose

The purpose of this document is to provide the best methods for the retrieval of video/audio data evidence and any associated metadata (referred to in this document as data) from Digital Closed Circuit Television (DCCTV) recording systems.

These best practices, guidelines and recommendations are intended to provide responding law enforcement personnel guidance in securing and collecting data from DCCTV systems. This will ensure that best methods are utilized to retrieve the recorded data and maintain its integrity.

The retrieved data should be retained as the master evidence. Whenever possible, the native/proprietary recorded data from the DCCTV recording system should be retrieved to maintain the integrity and image quality of the evidence.

These guidelines are meant to inform agencies of the best practices for DCCTV retrieval and to aid in the development of Standard Operating Procedures (SOPs). These practices should be used in conjunction with current agency policies.

Scope

This document is intended to provide procedures for the collection of data that ensure playback while maintaining best evidence. DCCTV retrieval is the collection of relevant data from a digital video recording system. This may not follow the methodology of computer forensics. The key differences between DCCTV retrieval and a computer forensic investigation are that, with DCCTV retrievals the recording device's operational settings may have to be reconfigured to retrieve the data, and the entire system's contents may not require a forensic examination. This document is not intended to address forensic video or audio analysis techniques performed after the retrieval of data. See SWGIT document "*Best Practices for Forensic Video Analysis* "and SWGDE document "*Best Practices for Forensic Audio*" for more information.

Recognizing DCCTV Evidence and its Nature

Due to its value in the evidentiary process, as well as its potential value for intelligence and security matters, it is imperative that Law Enforcement recognize, protect and properly collect data from DCCTV systems.

- DCCTV information may exist at a scene or at adjacent locations
- Look up, look down, and look around
- DCCTV may be recorded or stored at a remote off-site location

Types of Digital Video Recording Systems (DVRs)

DCCTV systems primarily found in residential, commercial or governmental institutions include two major types:

- Stand-Alone Embedded Digital Video Recorder
- Personal Computer

Stand-Alone Embedded Digital Video Recorder – menu-driven device containing a recording system that typically uses a non-traditional operating system.

PC-Based Digital Video Recorder – may appear to be a standard computer or may be a proprietary turnkey system with video recording capability.

Both systems may have the following:

- Built-in multiplexer
- Transactional data
- Audio recording capabilities
- Other peripheral devices as part of the system
- Network capabilities
- Camera control capabilities
- PC-based systems may also contain business and/or personal data

DVR Recordings

All DVRs utilize compression when recording data to reduce the amount of storage and transmission requirements. Most digital video recording systems utilize a proprietary native file format to record data. This usually requires proprietary playback software or a special codec from the manufacturer to play back the files and any metadata (e.g., time, date, camera number).

In addition to the retrieval of the native/proprietary video files, many systems allow the data to be downloaded/exported in an "open file format" that will be viewable in a non-proprietary software (e.g., AVI in Windows Media Player or MOV in QuickTime). It should be taken into consideration that these methods often further compress the video data.

Whenever possible, the native/proprietary recorded video file(s) from the DCCTV recording system should be retrieved to maintain the integrity and image quality of the evidence. In addition, consideration should be given to retrieving a non-proprietary video file to facilitate quick viewing.

Steps To Take Upon Scene Arrival

- Notes should be kept detailing the methods used and steps taken.

- Determine if a manual is available to assist with system information (e.g., passwords, output options).

- Establish that relevant video has been recorded by reviewing the recording. Preferably, a person with knowledge of the recording device should operate it during playback, if it is appropriate for them to do so.

- Determine the earliest recorded date. This will determine approximately how much time you have to retrieve the data before the system overwrites it.

    - For example, if the earliest recorded date is seven days prior to the incident date, you may have no more than seven days before the relevant data is written over.

- Determine if retrieval can be performed by the venue owner/security system's operator. If yes, will it be in line with best practices?

- Determine if the DCCTV installer company or a trained operator is available to assist in the retrieval.

- Compare the time displayed by the DCCTV system with the current time. Document the difference, if any. It is suggested that a reference clock be used, such as the Navy Observatory Master Clock at (202) 762-1401 and (202) 762-1069, or NIST Telephone Time of Day Service at (303) 499-7111. These services will provide Universal Time and/or Eastern Time.

- Acquire and document the following information:

    - Digital video recorder make, model and serial number

    - Whether system is PC-based or Stand-Alone Embedded

    - Number of recording units installed

    - Whether system is networked

    - System time and date displayed

    - Actual current date and time (from reference clock)

    - Recording capacity of the system and when it will overwrite

    - Number of camera(s) and the active camera numbers

    - Camera(s) make and model

    - Are any cameras infrared-sensitive and, if so, identify.

    - Is audio being recorded? If so, how many channels and are they all downloadable/exportable?

- Multiplexer make and model, if applicable
- Device and/or operating system password
- System settings
    - Image quality (e.g., high, medium, low)
    - Frames/pictures per second
    - Recorded image/frame size (e.g., 320 x 240)
    - Can it be determined if any cameras are alarm or motion triggered?
    - Number of hard drives; storage capacity of each
    - System firmware version
    - Other available system settings (e.g., event log, passwords)
- Playback software password
- Playback software name and version
- Is a copy of the most current maintenance/service log available or obtainable?
- Other information of importance
- Scene contact information
    - Scene address
    - Hours of operation
    - Scene point of contact (with access to DVR) and telephone number
    - DCCTV system installer point of contact and telephone number

- Photograph system (front and back).
- Sketch DCCTV camera placement and position (See Appendix A).
- Remove network cable, if necessary.
- Determine how much data needs to be retrieved.
- Determine best method for retrieval.

Assessing the Recording System for Output

A determination should be made as to how much and what type of data needs to be retrieved from the DCCTV recording device. An evaluation of the output options of the system should help determine the best and most practical method. When making this assessment, collection of the native/proprietary video file(s) should remain the highest priority to ensure image quality. Other factors to consider include: the amount of media required, law enforcement hours that will be incurred, and the data transfer time.

Examples:

If the incident is a 10-minute robbery, the system has a CD writer and the proprietary file(s) fit on a CD, then collection on CD would be the best method.

If the request is for 24 hours of video and the system has an external USB port, connecting an external USB hard drive may be the best option. This assumes that the system allows for recovery of large amounts of data at one time.

If the request is for 30 days of video, the best, or only, option may be producing a forensic clone of the hard drive(s) and/or removing the recording unit from the scene. See SWGIT document "*Best Practices for the Analysis of Digital Video Recorders*".

DVR Recording System Outputs (systems may include more than one)

This list is not exhaustive and other methods may exist based on the recording system.

- Optical Disc (e.g. CD-R/DVD-R, CD-RW/DVD-RW, Blu-ray)
- Flash media (e.g. Compact flash (CF), Secure Digital (SD))
- USB (1.0, 2.0 and 3.0)
- IEEE 1394 Firewire/iLink
- eSATA
- Network port
- Analog video (RCA, S-Video, Composite)
- VGA/DVI/HDMI output
- SCSI port (50 pin and 60 pin)
- Removable hard drive
- Magnetic digital data storage tape (DAT, DLT, DDS, AIT)
- DV cassette drive (e.g. Sony HSR-1P)
- Iomega Jaz
- Iomega Zip
- Magneto Optical

Important:

- Administrative and/or engineer login access to the DVR usually allows more options for retrieval, including native/proprietary files.

- Time/date stamp with file. You may have to take the downloaded/exported file without the time/date data to ensure the highest quality footage, and take a second retrieval of the footage which includes the time/date data utilizing the output option that may be of lesser quality to ensure you have the information.

- On systems where the time/date stamp can be moved, ensure that this overlay does not obscure critical events.

- The amount of time and storage needed to retrieve the video data may dictate the best method for retrieval.

- Performing a test retrieval will assist in estimating the time and storage requirements for the chosen output option.

- Once the appropriate output option is chosen and the video data retrieved, a master should be retained. Depending upon the data retrieval method chosen, additional steps may be needed to create the master.

The following are all possible output options in their respective order of suggestion

The intent of "respective order" is to consider the list from beginning to end as being organized from most advisable to least advisable – from a technical and quality of service standpoint.

CD/DVD Writer

Many DCCTV systems have a built-in or external CD/DVD writer to retrieve the recorded video. In some instances, an external CD/DVD writer can also be connected through a USB/Firewire/SCSI port (see USB/Firewire/SCSI Devices).

- Generally, the DCCTV system software will have an archive, backup, copy, or export function in which you can retrieve the data directly to the CD/DVD writer.

- Generally, the system software will allow you to copy the proprietary viewer to the disc while burning, however, you may have to manually select this option.

- Write-once CD-Rs, DVD-Rs, or DVD+Rs should be used.

- Some drives may only write to a specific brand(s) of media. If difficulties are encountered when writing data, try another brand of media.

  Some DCCTV systems may only take a CD-RW/DVD-RW disc. If the data is downloaded to rewritable media, transfer the data to non-rewritable media or secure electronic storage as soon as possible. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*".

- The system may require you to format the CD/DVD, either in the DVR itself or in another computer.

- The system may require you to finalize the CD/DVD in the original recording device before the disc can be read in other devices.

- After retrieval, verify that the downloaded/exported file(s) play back correctly on another system, and that the proper dates and times were retrieved.

- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.

- The resulting produced WORM media or file(s) on the secure electronic storage is the master evidence. If more than one disc is created, each should be identified for proper order of playback.

Flash Media

Some DCCTV systems have a flash card option, which is usually intended for short video sequences and should be used as a temporary storage medium only. Even though many cards now have the ability to hold gigabytes of information, the majority of these drives are not intended for permanent storage and are not as readily available as CD/DVD writers. If data is recovered via these drives, all data should be transferred from the flash media to a more permanent media to create the master evidence at the earliest possible time. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*". The drive should then be wiped before reusing.

Some systems require appropriately sized and formatted flash media (see the system manual for more information).

Some systems that employ flash media drives export files in real time (e.g., a 10-minute file will take 10 minutes to download/export). This may not be the most appropriate option for the retrieval of a large amount of data.

Mass Storage Devices

USB/Firewire/SCSI/eSATA ports can be used to connect external CD/DVD writers, drives, and legacy devices. It should first be established that the port is a working port. Some devices may require activation by installing the necessary drivers on the recording system. It is recommended that the manufacturer be contacted before attempting to install any drivers.

- External USB CD/DVD writers may be used for retrieving smaller amounts of data if no other option exists. External hard drives are a good resource when large amounts of data need to be collected.

- On some PC based systems that utilize a "standard" Windows operating system, it may be possible to copy the native/proprietary file(s) using Windows Explorer. **NOTE:** This does not work on all systems as the file(s) retrieved in this manner may require the use of the hardware/software during the retrieval process for playback later. It is strongly recommended to know the system before utilizing this method or to consult the manufacturer to ensure the file(s) copied will be capable of playback.

- Some DVR systems have a limitation on the amount of data that can be retrieved (downloaded/exported) at a time, typically 1 GB, sometimes 2GB. This limit may not

be specified in the system manual or known to the manufacturer. It is best to keep your file(s) under 1 GB, unless you know for sure it is capable of more.

- Generally, the DCCTV system software will have an archive, backup, copy, or export function in which you can retrieve the data directly to the device attached. You may have to choose the device or navigate to it.

- Generally, the system software will allow you to copy the proprietary viewer to the device, however, you may have to manually select this option.

- After retrieval, verify that the downloaded/exported file(s) play back correctly on another system, and that the proper dates and times were retrieved.

- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.

- External hard drives are usually considered a temporary storage medium. Therefore, at the earliest possible time, all data should be transferred from the drive to a more permanent media to create the master evidence. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*". The drive should then be wiped before reusing. If the file(s) retrieved are too large, the external drive may be retained as the master evidence.

Network Connection

Many DCCTV recording systems have network ports. Furthermore, many DCCTV systems have their own proprietary network viewer software which allows for multi-computer connectivity and recovery of the native/proprietary recorded file(s).

If you do not have any experience with computers or networking, it is highly recommended that you obtain assistance prior to retrieving data using this method.

By utilizing an ethernet crossover cable, computer, and network viewer, a connection to the DVR can be established and the native/proprietary file(s) downloaded/exported. The remote or network viewer software is installed on a separate computer/laptop, the IP address of the DVR is usually configured in the remote viewer software, and a connection is established.

Verify that the network viewer recovers the native/proprietary recorded video file.
Example: Some remote viewers only allow for the collection of still images and not the entire native/proprietary recorded video file.

- Ensure you have administrator rights on the computer/laptop to which you are downloading/exporting the file(s). Disable any firewalls.

- Screen savers should be disabled as they can interfere and/or disrupt the download/export process (See Appendix B).

- **Warning:** Power scheme settings for the computer to which you are downloading/exporting the file(s) should be set to 'always on' with hibernation disabled (See Appendix C-01 and C-02).

- The IP address may be required from the DVR. This usually requires accessing the menu functions of the DVR. Care should be taken not to change other settings on the DVR when doing this.

- Some proprietary remote/network viewers are installed on the DVR system for easy access. Otherwise, searching the vendor's website or contacting the vendor directly may be necessary.

- On some systems, setting up a standard Windows network connection between the computer/laptop and the DVR may be necessary (e.g., computer/laptop 192.168.10.1, and the DVR 192.168.10.2). **NOTE**: It is best practice to try and retain the existing IP settings on the DVR and change those on the computer/laptop to match.

- If a network viewer for the system does not exist, a connection may be possible utilizing Windows Explorer, a web browser, and typing in an appropriate IP address.

- If you have to change the IP address on the DVR, make note of the original IP address so you can change it back when you are finished. Changing the IP address may also require rebooting the system

- Some DVR systems have a limitation on the amount of data that can be retrieved (downloaded/exported) at a time, typically 1 GB, sometimes 2GB. This limit may not be specified in the system manual or known to the manufacturer. It is best to keep your files under 1 GB, unless you know for sure it is capable of more.

- Some networkable systems may only allow for the video to be "streamed" out and may not provide native/proprietary data transfer. Metadata can be lost through "streaming." Unless this is the only option, it is preferable to output to digital magnetic tape.

- Ensure network speed is sufficient to ensure that no possible data is lost and to prevent crashes/timeouts during downloading/exporting.

- You may have to disable any firewall, ensure you have administrator rights on the DVR. After completing data retrieval, confirm you have re-enabled the firewall and various settings.

- After retrieval, verify that the downloaded/exported file(s) play back correctly on another system, and that the proper dates and times were retrieved.

- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.

- Ensure you have also retrieved the proprietary playback software.

- Return all changed system settings to their prior state after data has been retrieved.

- The computer/laptop or external hard drive(s) that you connected to the computer/laptop to retrieve the video file(s) usually are considered a temporary storage medium. Therefore, at the earliest possible time, all data should be transferred from the laptop or external drive to a more permanent media to create the master evidence. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*". If an external hard drive was used, then it should be wiped before reusing. If the file(s) retrieved are too large, the external drive may be retained as the master evidence.

Replacing Hard Drives

In some situations, the quickest solution may appear to be to remove the hard drive(s) from the system and replace them. This option should be considered carefully as there are many factors that come into play. Simply removing a hard drive(s) does not ensure the video contained on that hard drive(s) will playback. Some DVR systems require the actual DVR hardware to playback the video on the drive.

If you have limited computer hardware experience, consider calling someone for assistance. Care should be taken to follow appropriate health and safety procedures, particularly with regard to potential exposure to electricity.

- The system should be properly shut down prior to removing any hard drive, even if the drive appears to be "hot swappable."

- Ensure that all of the system's hard disc drives are retrieved. The system may have a removable drive in a caddy, but also additional internal drive(s).

- Document the master/slave drive configuration of all retrieved drive(s).

- The DVR may require a specific brand, model and size of hard drive to operate correctly. Consult the manufacturer, manufacturer's web site, or system manual for more information.

- The new drive(s) may need to be formatted by the DVR before it will recognize and record to it.

- Once the new drives are installed, restart the system and confirm that recording and playback are operational, as the system may require that vendor specific software/operating system be installed. Failure to install such software can render a system either partially or completely inoperable.

- If you remove the existing drive(s), be aware that you have removed the archive data stored on the CCTV system.

- The removed hard drive(s) is the master evidence. If more than one hard drive is removed, each should be properly identified.

Drive Duplication

In some situations, drive duplication may be necessary. This option should be considered carefully as there are many factors that come into play. Drive duplication does not ensure playback. Some DVR systems require the original hard drive(s) for playback.

It is recommended that a forensic clone of the original hard drive(s) be produced, not an image set.

- The system should be properly shut down prior to removing any hard drive, even if the drive appears to be "hot swappable."

- Some systems require the original hard drive(s) for proper operation. Therefore, if the drive(s) is duplicated, place the duplicated drive back in the system, make sure the system is operational, and retrieve the original drive(s) from the scene. If the system is not operational, the recording device may have to be retrieved, along with the original hard drive(s).

- Ensure you duplicate all the drives in the system as the DVR may have internal drives.

- Document the master/slave drive configuration of all duplicated drives.

- External playback software may exist to access the data on the duplicate hard drive.

- Upon initial inspection, a hard drive duplicated from a system may not appear to contain data when viewed using a standard PC. Many systems utilize proprietary formats that prevent data from being recognized. If you don't see files upon inspection of a forensic clone, the drive may still contain useful data.

- The forensic clone(s) and/or original drive(s) should be inspected using a write blocker and a separate computer/laptop.

- The forensic clone(s) and/or original drive(s) retrieved from the scene are considered the evidentiary master from which working copies may be produced.

Legacy Output

The following output methods usually enable retrieval of the native/proprietary video data and can be located inside the digital recording unit or as an attached external device. In some circumstances, this may be the only method available on the DVR system for retrieval of the video data. Retrieval and playback may require additional steps. These can typically be connected through the SCSI port. Do not discount this as a retrieval method if you do not have these devices.

- DDS TAPE (Digital Data Storage)
- Iomega Jaz
- Iomega Zip
- Floppy
- Magneto Optical

The above media should be considered a temporary medium. At the earliest possible time, all data should be transferred to a more permanent media to create the master evidence. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*".

Removal of DVR Unit

In circumstances where the above listed options have been rejected as either impractical or impossible, then the decision may be made to remove the recording unit itself.

This assumes that it is physically possible to do so, and that the removal is justified. For example, where the volume of data required is very large, it may be time efficient to temporarily remove the recorder and perform the retrieval in the lab, rather than on site. Alternatively, there may be no method for extracting the video data (e.g., CD writer or USB ports) and it may be necessary to remove the recorder and retain the unit as the evidentiary master.

- The recording device should be stopped and the system properly shut down prior to removal.

- Ensure all relevant components of the system are collected (e.g., power supply, remote control, dongle, manual, cables, hard drive keys).

- Ensure all cables are uniquely identified (e.g., camera inputs) to facilitate reinstallation of the system.

- If no other method exists for extracting the data from the DVR recording device retrieved from the scene, the DVR is considered the evidentiary master.

Non Native/Proprietary Data Retrieval

Although they record digitally, some DCCTV systems only have an analog output. For these systems, consideration should be given to collection of the DVR system as the master evidence. If this is not practical, then the following should be considered:

S-Video/Composite Output

- Video can only be retrieved in "real time" and the process should be repeated for each required camera view.

- When a system has both an s-video and composite output, it is recommended that the s-video be used.

- It is recommended that a digital video tape recorder (VTR) be utilized. Some examples of digital VTRs are Digital Betacam, DVC Pro, DVCam, Mini DV, and Digital 8.

- The video recording should be collected to digital magnetic tape.

- Ensure the "time/date stamp" is displayed on output; this may require checking several signals (e.g., composite and s-video).

- It is recommended that the DVR output be directly connected to the VTR and a separate output from the VTR be made to a monitor to ensure that the signal is being received and recorded.

- Prior to recording the video data, check and adjust playback speed on the DVR to "real time"or 1x.

- The collection of video data to VHS tape or Video DVD should be considered a last resort and conducted if it is the only possible option.

- Taking the analog output from a DVR may produce a different frame size from the original native/proprietary frame size.

- The produced magnetic tape is considered the evidentiary master.

NOTE: Video capture cards can be utilized for digitizing a video signal from the DVR to a computer. Most capture cards can take an s-video and composite input, while higher quality cards can input a component, SDI, and HD video signal. It is recommended that the highest quality signal be utilized. Care should be taken to ensure that the recorded frame size is maintained when utilizing this method. The digitized data should be captured as uncompressed (1:1) and retained as the master evidence.

VGA/DVI/HDMI Output

Some DCCTV systems have a VGA, DVI (DVI-A/DVI-I) or HDMI output that allows the video data to be displayed on a computer monitor. Devices are available that allow the DVI (DVI-D) and HDMI signals to be directly captured at their native resolution, while maintaining the signal's progressive scan format. Alternatively, a scan converter can convert a VGA or DVI signal to a standard video signal, usually analog, which can be recorded to video format and retained as the evidentiary master.

Either method should be considered a last resort as the final product may not include all metadata and image quality may be compromised. The latter is especially of concern with scan conversion as it can reduce image quality below that of an s-video/composite output.

Whenever possible, the footage should be captured at its native resolution (without scaling).

Important Information

- Do not change the time and date on the DVR system.

- It is not recommended that any additional software be installed on the DVR system (e.g., CD writing software, if it is not present). If it is absolutely necessary to install additional software, it is highly recommended that the manufacturer be contacted prior to installation.

- A DVR typically records data linearly. When the storage device is full, new data overwrites the oldest recorded data in a manner that is not recoverable. When data is deleted by other means (e.g. formatting the storage device), the space occupied by that data is marked as free for recording. Deleted data in this space may be recoverable for a limited amount of time before being overwritten. DVR file systems are typically non standard. Recovery of these file systems and the proprietary data is a difficult and time consuming process and may not be successful. Before seizing the DVR, check to see if the venue retains back up files and consult an individual trained in the interpretation and extraction of video data.

If it is determined that the video data of interest has been overwritten, check to see if the venue retains back up files.

- Administrative/Engineer access to the DVR usually allows more options for retrieval, including native/proprietary files.

- Time/date stamp with file. You may have to take the downloaded/exported file without the time/date data to ensure the highest quality footage, and take a second retrieval of the footage which includes the time/date data utilizing the output option that may be of lesser quality to ensure you have the information.

- On systems where the time/date stamp can be moved, ensure that this overlay does not obscure critical events.

- A review of the live monitor may appear to be of better quality than the actual recorded video.

- Whenever possible, the system should remain recording during the retrieval of the data.

- Many digital video recording systems allow you to auto-copy the proprietary playback viewer while retrieving the video data. This should always be done where offered. If the system does not allow this, steps should be taken to retrieve the correct version, with full functionality, required for playback/viewing.

- The native/proprietary video data should be retrieved. If time permits, and if the system exports a file that is in a non proprietary format (e.g., AVI) for quick viewing, consider collecting that as well as the native/proprietary.

- If the DVR has multi-camera capabilities, all the video data for the required area of interest should be taken as it was recorded. These cameras should be recorded in isolation, showing one camera full screen and not multi-cameras on a single screen (e.g., not 4, 8, and 16 on a single screen).

- Ensure that the frame rate upon retrieval is as near to recorded frame rate as possible.

- Ensure that the aspect ratio of the video data upon retrieval is as near to the recorded aspect ratio as possible.

- Working copies may be produced from the master evidence.

Evidence Handling Procedures

- To provide an audit trail, contemporaneous notes should be recorded detailing the course of actions taken.

- Initiate a chain of custody for the retrieved evidence, per agency policies.

- If transport of evidence is required, ensure the evidence is packaged and sealed appropriately based on the media (e.g., jewel cases for compact discs, anti-static bags and individual foam insert boxes for hard drives).

- Keep evidence away from magnets, excessive temperatures, and otherwise hostile environments.

Prior to Leaving Scene, Ensure That

- You have completed all the necessary documentation.

- You have collected all required video data.

- The retrieved video data plays back correctly, preferably on another system, and that the proper dates and times were retrieved.

- The proprietary playback software, network viewer, backup player, and/or archive software have been retrieved.

- The recording system has been returned to its original state (e.g., any changes to the system settings have been reset).

- The recording system has been verified as operational, preferably in the presence of venue personnel.

- If removing the recording system, ensure that all necessary peripherals have been retrieved.

- If you have retrieved the recording system, have legal implications been considered?

- Obtain contact information of venue owner, system installer and/or system manufacturer for future questions/reference.

Legal Issues

- Some DCCTV systems are used as both a DCCTV recording system as well as a business computer. This should be considered when it is necessary to remove the digital video recording system from the scene.

- Consideration should be given as to whether owner consent is necessary and applicable for removing the recording system.

- Ensure the scope of the search warrant encompasses the video data and necessary system components.

- Is it necessary or feasible to provide the business with a replacement recording device if their system has been removed?

- If you need to retrieve or replace the recording device's hard drive(s), will you be voiding an existing warranty on the system? If yes, have you received the proper level of authorization?

- If the DCCTV system is an instrumentality or fruit of the offense, seize it.

Recommended Equipment Needed

To enable retrieval from a variety of systems that will be encountered, a range of equipment is recommended. The following is a suggested list of equipment that should permit video data retrieval from the most commonly encountered systems:

- Laptop with:
  - CD/DVD writable drives
  - USB ports
  - Network port
  - Firewire ports
  - eSATA ports
  - Wireless access
  - Capability for installing proprietary viewers - ensure you are Administrator on this computer and there are no restrictions that would impede the download (e.g., firewalls, agency software)

- Flash media reader (multi-format)

- USB floppy drive

- Four port network switch/hub

- External CD/DVD writeable drive -- USB/SCSI/Firewire

- USB and Firewire storage devices in multiple sizes

- IDE, SCSI and SATA hard drives in multiple sizes (80, 160, 300 GB for backwards compatibility)

- Cables to include:

    - Network cables (crossover cable and straight patch cable)
    - Composite and s-video cables, as well as RCA to BNC adapters
    - Audio cables (RCA, stereo, and mono mini)
    - USB cables
    - Firewire cables (iLink, 400, 800)
    - VGA/DVI cables
    - Power cables
    - Extension cords

- Write blockers (IDE, Firewire)

- Blank Media (CD-R,DVD-R,DVD+R, DVD-Ram,CD-RW, DVD-RW, DVD+RW, Blu-ray)

- Blank flash media in varying sizes

- Video monitor (NTSC/PAL)

- Computer monitor

- Still camera with media

- Toolkit containing :

    - Flashlight
    - Anti-static strap
    - Mirror
    - Assorted screwdrivers
    - Pens
    - Permanent marker (appropriate for marking media)

- Digital Video Tape Recorder

- Analog Video Tape Recorder

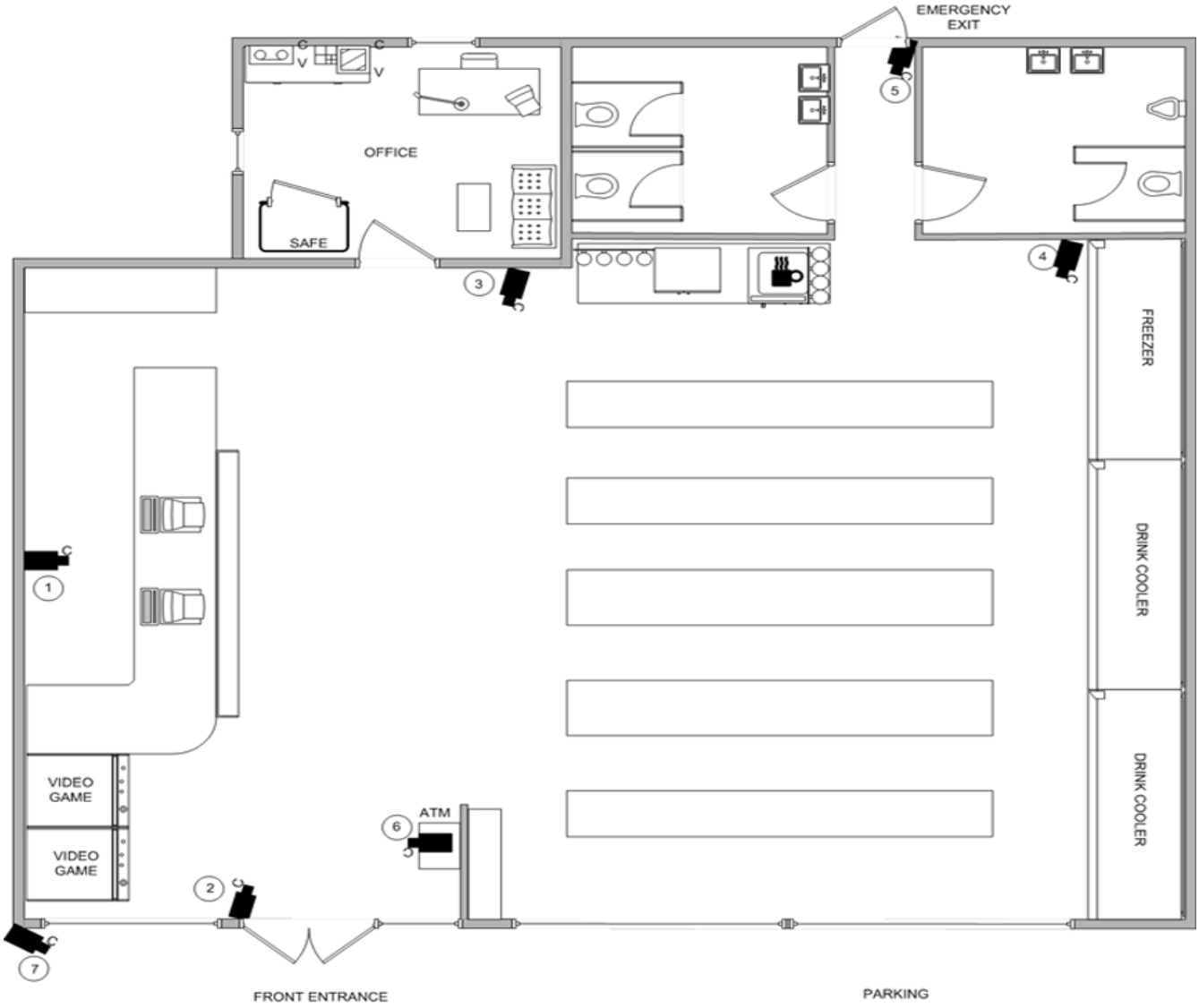
- Magnetic tapes (analog/digital)

- Appropriate forms (chain of custody, notes, consent)

- Appropriate evidence packaging (anti-static bags, jewel cases)

APPENDIX A

EXAMPLE OF SITE PLAN FOR
CONVENIENCE STORE

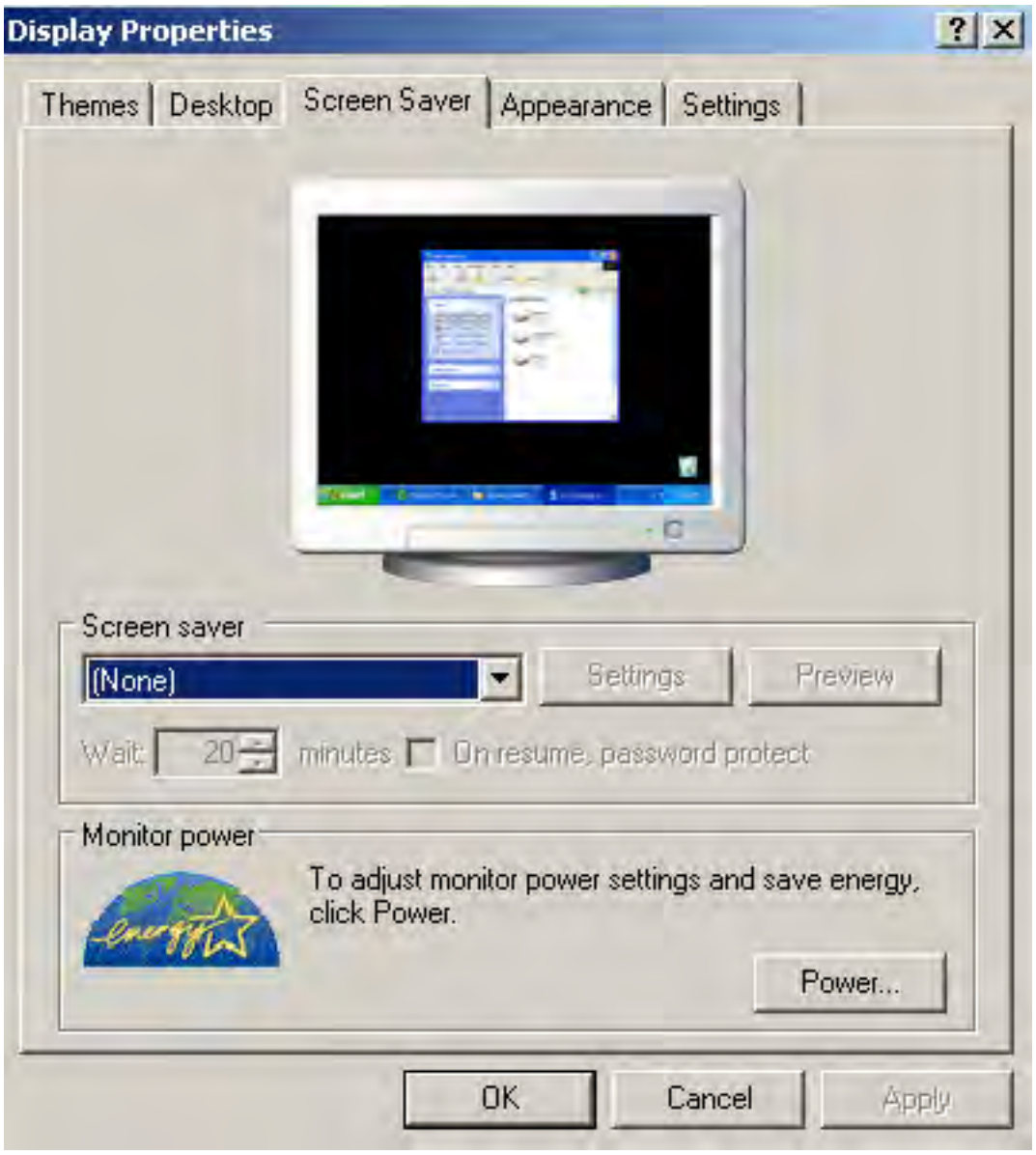


Camera 1: Clerk and check-out area, facing east
Camera 2: Front door entrance, facing north
Camera 3: Outside of office, facing south
Camera 4: Freezer area, facing south
Camera 5: Emergency exit, facing south
Camera 6: Automated teller machine, facing west
Camera 7: Parking lot, facing south-east

Taken from the Scientific Working Group on Imaging Technology (SWGIT) document, Section 4 "*Recommendations and Guidelines for Using Closed-Circuit Television Security Systems in Commercial Institutions*"

APPENDIX B

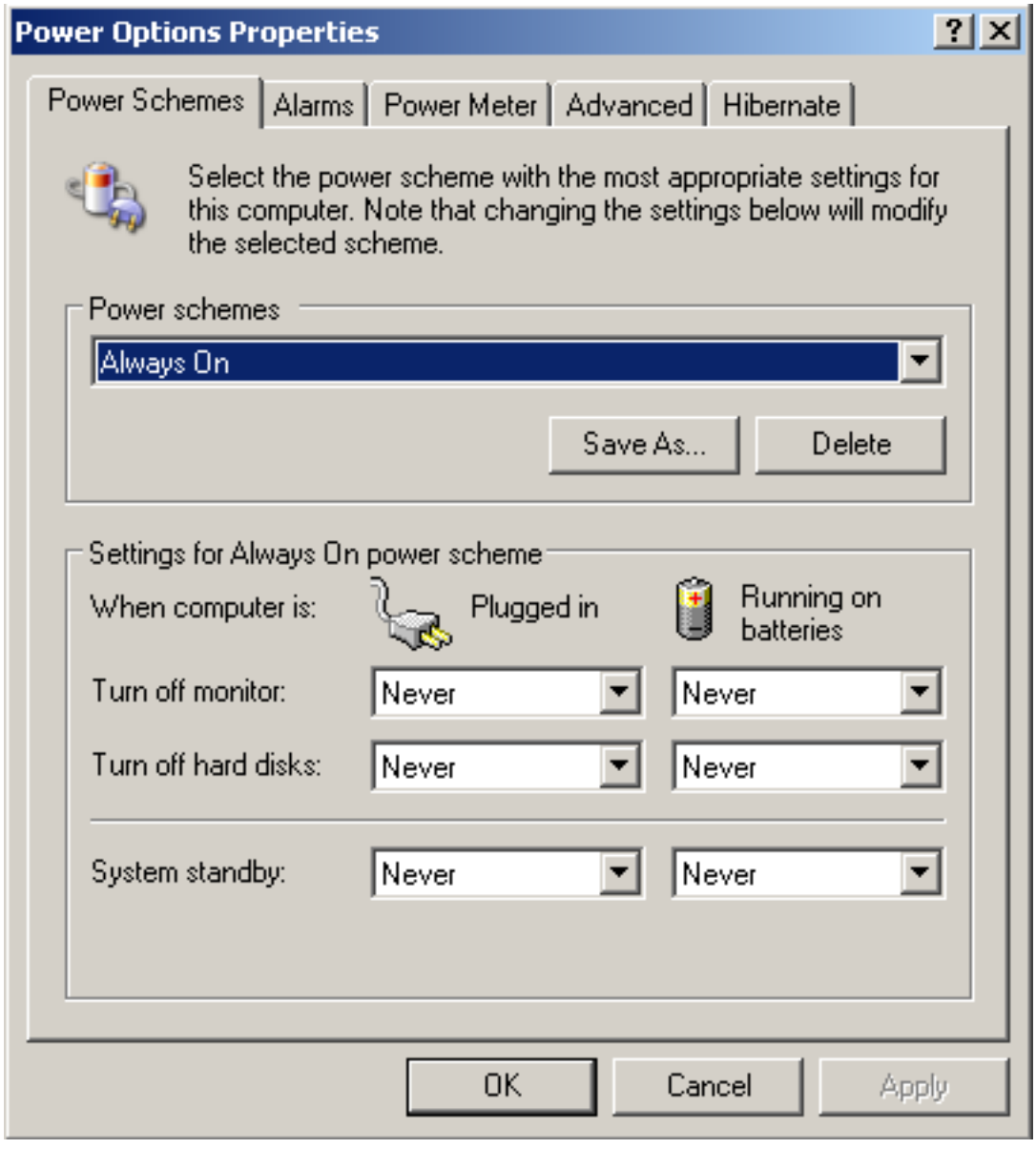
To access these options, refer to the system manual.



APPENDIX C-01

To access these options, refer to the system manual.

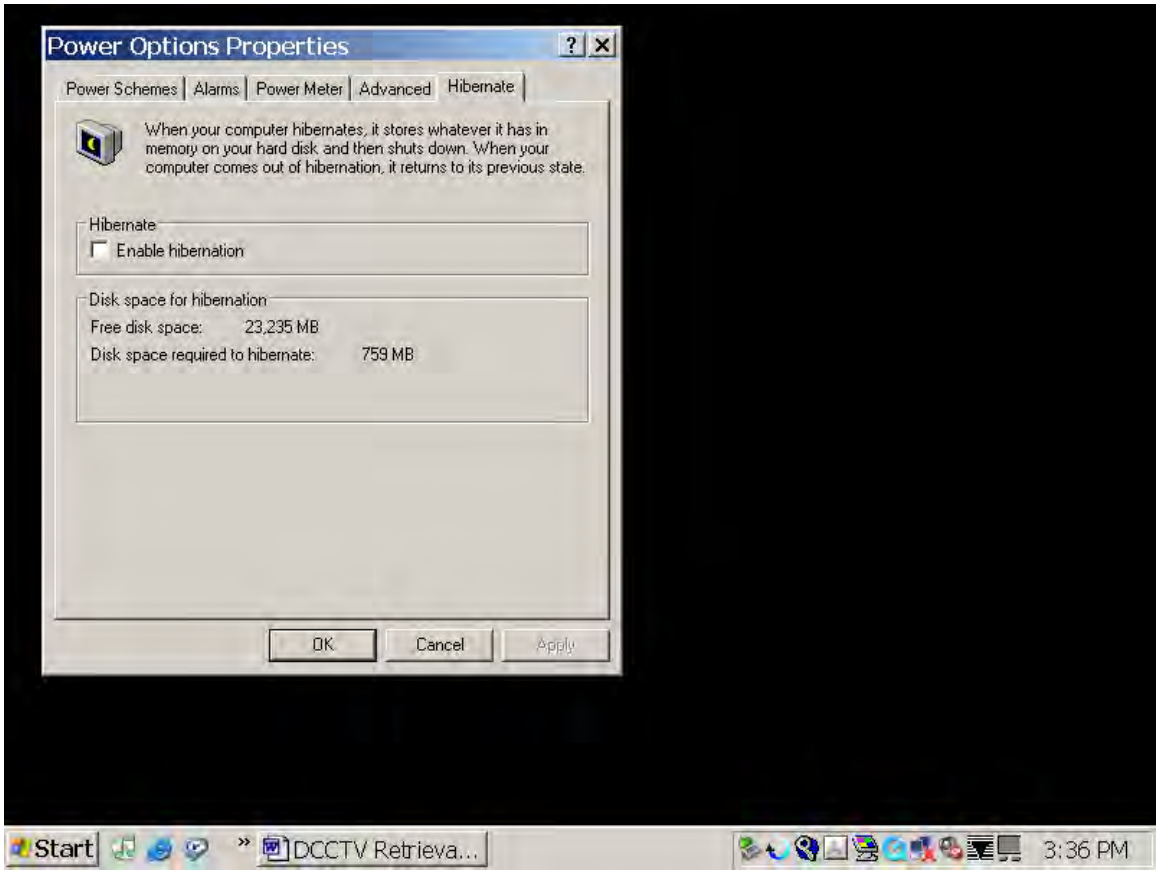
The following settings should be set as shown below.



APPENDIX C-02

To access these options, refer to the system manual.

Enable Hibernation should **NOT** be checked



Scientific Working Group on Digital Evidence

SWGDE Digital & Multimedia Evidence Glossary

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Preface

SWGDE provides this Glossary of Terms with general, as well as discipline specific, definitions as they apply across the spectrum of image analysis, computer forensics, video analysis, and forensic audio. Sources are notated within brackets at the end of the definition when that definition came from outside of SWGDE. The following abbreviations will be used throughout this glossary and appear before the definition as applicable:
(i) – Image Analysis
(c) – Computer Forensics
(v) – Video Analysis
(a) – Forensic Audio

Achievable Resolution
(i,v) Is a direct measurement of the ability of an imaging system to record detail, typically measured by its ability to maintain separation between close subject elements such as fine lines which are usually stated as 'line pairs or cycles per millimeter'. It is often determined by imaging a resolution test chart. With some imaging systems there may be a slight difference in the horizontal and vertical resolution. If so, the lower of the two values is considered the achievable resolution of the imaging system.

Acquisition
(c) See "Image".

Administrative Review
A procedure used to check casework for consistency with agency/laboratory policy and for editorial practice.

Algorithm
A step-by-step procedure for solving a problem or accomplishing some end. [*Webster's Dictionary*]

Analytical Photogrammetry
A method of photogrammetry in which solutions are obtained by mathematical methods.

Archive Copy
A copy of data placed on media suitable for long-term storage, from which subsequent working copies can be produced.

Archive Image
(i,v) Any image placed on media that is suitable for long-term storage.
(c) A bit stream duplicate of the original data placed on media that is suitable for long-term storage.

Archiving
The process of storing data in a manner suitable for long term availability and retrieval.

Artifact
(a,i,v) A visual/aural aberration in an image, video, or audio recording resulting from a technical or operational limitation. Examples include speckles in a scanned picture or "blocking" in images compressed using the JPEG standard.
(c) Information or data created as a result of the use of an electronic device that shows past activity.

Aspect Ratio
(i,v) The width to height ratio of an image.

Audio Enhancement
Processing of recordings for the purpose of increased intelligibility, attenuation of noise, improvement of understanding the recorded material and/or improvement of quality or ease of hearing.

Authentication
The process of substantiating that the data is an accurate representation of what it purports to be.

Capture
The process of recording data, such as an image, video sequence, or audio stream.

Capture card/frame grabber
A piece of computer hardware that accepts an analog or digital signal and outputs the signal as digital data.

Capture Device
A device used in the recording of data.

Carve
(c) The extraction of a portion of data for the purpose of analysis.

CD/DVD (compact disc/digital versatile disc)
Optical disc formats designed to function as digital storage media.

Cellular Network Isolation Card (CNIC)
Identity module card that isolates a device from cellular connectivity. CNIC's do not contain a "cipher key" thus preventing access with a cellular network.

Chain of Custody
The chronological documentation of the movement, location and possession of evidence.

Clarification
(i,v) See "Image Enhancement".

Clean Room/Chamber
To the extent possible, a limited particulate environment (e.g. requirements would follow ISO 5 or Class 100 standard for air quality).

Codec (compressor/decompressor)
(i,v) A device or program capable of encoding and decoding digital data. Codecs encode a stream or signal for transmission, storage or encryption and decode it for viewing. Codecs are necessary for playback of encoded data. Generally, codecs from DCCTV systems are proprietary.

Cognitive Image Analysis
(i,v) The process used to extract visual information from an image.

Colorimetry
The quantification of the color of an object.

Color Range
The range of colors that can be detected by a sensor.

Competency Test
The evaluation of a person's knowledge and ability prior to performing independent work in forensic casework. [*ASCLD*]

Composite Video Signal
(i,v) An analog signal which contains chroma, video, blanking and sync information and has been combined using one of the coding standards NTSC, PAL, SECAM, etc.

Compression
The process of reducing the size of a data file. (See also, "Lossy Compression" and "Lossless Compression".)

Compression ratio
The size of a data file before compression divided by the file size after compression.

Computer Forensics
A sub-discipline of Digital & Multimedia Evidence, which involves the scientific examination, analysis, and/or evaluation of digital evidence in legal matters.

Copy
An accurate reproduction of information.

Data
Information in analog or digital form that can be transmitted or processed.

Data Analysis
The assessment of the information contained within the media.

Data Extraction
A process that identifies and recovers information that may not be immediately apparent.

Data Smear
(c) The modification of data by a running system during the data acquisition process.

Deblurring
(i,v) A type of image restoration used to reverse image degradation, such as motion blur or out-of-focus blur. It is accomplished by applying algorithms based on knowledge or an estimate of the cause of the original degradation.

Deinterlacing
(v) Separating an interlaced frame into two discrete fields.

Demonstrative Comparison
(v) A method of presenting the similarities and/or differences among images and/or objects without rendering an opinion regarding identification or exclusion.

Digital CCTV Retrieval
(v) The process of retrieving video/images from digital CCTV systems.

Digital Evidence
Information of probative value that is stored or transmitted in binary form.

Digital Image
(i) An image that is represented by discrete numerical values organized in a two-dimensional array. [Taken from the "*Encyclopedia of Photography*" 3rd Edition] When viewed on a monitor or paper, it appears like a photograph.
(c) See "Image".

Directory Listing
(c) A list of files contained within an object. It may also contain other information such as the size and dates of the files.

Downloading/Exporting
(i,v) The process of retrieving audio, video, and still images and transactional data from a DVR system. Can be in either the native/proprietary format or an open format.

Duplicate
An accurate and complete reproduction of all data objects independent of the physical media.

Dynamic Range
(i) The difference between the brightest highlight and darkest value that a sensor (e.g. film or CCD) can detect and record in a single image.
(a,v) The ratio of the strongest (undistorted) signal to that of the weakest (discernible) signal in a unit or system as expressed in decibels (dB). A way of stating the maximum signal to noise ratio.

DVR (Digital Video Recorder)
(i,v) A stand-alone embedded system or a computer based system used to record video and/or audio data.

Enhancement
(i,v) See "Image Enhancement".
(a) See "Audio Enhancement".

Erased File Recovery
(c) The process for recovering deleted files.

Extraction
(c) A method of exporting data from a source (e.g. copying data from EnCase preview, dumping data from a cell phone). See "Data Extraction".
(i,v) See "Downloading/Exporting".

Field
(v) An element of a video signal containing alternate horizontal lines. For interlaced video, the scanning pattern is divided into two sets of spaced lines (odd and even) that are displayed sequentially. Each set of lines is called a field, and the interlaced set of the two sets of lines is a frame.

File Format
The structure by which data is organized in a file.

File Slack
(c) The data between the logical end of a file and the end of the last storage unit for that file. ***Ex:*** For the FAT file system, the data between the logical end of the file and the end of the cluster.

Fixed Focal Length Lens (Prime Lens)
(i,v) A lens with a focal length that is not adjustable.

Focal Length
(i,v) Distance from the optical center of a lens to its point of focus at the sensor/image plane when focused at infinity. Smaller focal length values provide a wider field of view; larger focal length values provide a narrower field of view.

Forensic
The use or application of scientific knowledge to a point of law, especially as it applies to the investigation of crime.

Forensic Audio
A subdiscipline of Digital & Multimedia Evidence, which involves the scientific examination, analysis, comparison, and/or evaluation of audio.

Forensic Cloning
The process of creating a bit stream duplicate of the available data from one physical media to another.

Forensic Image
(c) See "Image".

Forensic Photogrammetry
The process of obtaining dimensional information regarding objects and people depicted in an image for legal applications.

Forensic Video Analysis
See "Video Analysis".

Forensic Wipe
A verifiable procedure for sanitizing a defined area of digital media by overwriting each byte with a known value.

Format
(verb) The process of preparing a hard disk and/or removable media for data storage. This is not a replacement for a forensic wipe.

(noun) The structure by which data is organized on a device.
(v) One or several combined elements that may be used to describe the video recording method. These include tape width (e.g. 8mm, ½ inch, ¾ inch, 1 inch), signal form (e.g. composite, Y/C, component), media (e.g. VHS tape, DVD, CD), data storage type (e.g. analog/digital, AVI/MPEG), and signal standard (e.g. NTSC, PAL, SECAM).

Format Conversion
(a,i,v) To transfer audio and/or video information from one media type to another and/or from one recording method to another.

Frame
(v) Lines of spatial information of a video signal. For interlaced video, a frame consists of two fields, one of odd lines and one of even lines, displayed in sequence. For progressive scan (non-interlaced) video, the frame is written through successive lines that start at the top left of the picture and finish at the bottom right.

Free Space
Data storage areas available for use by the computer. The area may already contain previously stored information. Also referred to as Unallocated Space.

Gaussian Blur
(i,v) A function typically used to reduce image noise and detail using a specific mathematical function known as the "Gaussian Kernel" or "bell-curve". The visual effect of this technique is a smoothing of image features as if viewing the image through a translucent filter.

Geotag
GPS coordinates added to files as metadata.

GPX
GPS exchange format. An XML scheme designed for a common GPS format for software applications.

Hash or Hash Value
Numerical values, generated by hashing functions, used to substantiate the integrity of digital evidence and/or for inclusion /exclusion comparisons against known value sets.

Hashing Function
An established mathematical calculation that generates a numerical value based on input data. This numerical value is referred to as the hash or hash value.

Image
(i,v) An imitation or representation of a person or thing, drawn, painted, photographed, etc.
(c) A bit stream copy of the available data. The result may be encapsulated in a proprietary format (e.g., E01, 001, etc.).

Image Analysis
The application of image science and domain expertise to examine and interpret the content of an image, the image itself, or both in legal matters.

Image Averaging
(i,v) The process of averaging similar images, such as sequential video frames, to reduce noise in stationary scenes.

Image Comparison (Photographic Comparison)
(i) The process of comparing images of questioned objects or persons to known objects or persons or images thereof, and making an assessment of the correspondence between features in these images for rendering an opinion regarding identification or elimination.

Image Content Analysis
(i) The drawing of conclusions about an image. Targets for content analysis include, but are not limited to: the subjects/objects within an image; the conditions under which, or the process by which, the image was captured or created; the physical aspects of the scene (e.g., lighting or composition); and/or the provenance of the image.

Image Data Recovery
(i) The process of retrieving viewable image(s) from a data set.

Image Enhancement
(i,v) Any process intended to improve the visual appearance of an image or specific features within an image.

Image Output
(i) The means by which an image is presented for examination or observation.

Image Processing
(i) Any activity that transforms an input image into an output image.

Image Processing Log
(i) A record of the steps used in the processing of an image.

Image Restoration
See "Restoration".

Image Synthesis
(i,v) Any process that renders an image, using computer graphics techniques, for illustrative purposes (i.e. age progression, facial reconstruction, accident/crime scene reconstruction).

Imaging Technology
(i,v) Any system or method used to capture, store, process, analyze, transmit, or produce an image. Such systems include film, electronic sensors, cameras, video devices, scanners, printers, computers, etc.

Image Transmission
(i,v) The act of moving images from one location to another.

Integrity verification
The process of confirming that the data presented is complete and unaltered since time of acquisition.

Intermediate Storage
Any media or device on which data is temporarily stored for transfer to permanent or archival storage.

Interlaced Scan
(v) A technique of combining two television fields in order to produce a full frame. The two fields are composed of only odd and only even lines, which are displayed one after the other but with the physical position of all the lines interleaving each other, hence interlace. [*CCTV*, Vlado Damjanovski, Butterworth-Heinemann. 2000]

Interpolation
(i,v) A method of image processing whereby one pixel, block, or frame is displayed or stored based on the differences between the previous and subsequent pixel, block, or frame of information. [Taken from the *Encyclopedia of Photography* 3rd Edition] This is often done to increase the apparent clarity of an image.

Log File
A record of actions, events, and related data.

Logical Acquisition/Copy
(c) An accurate reproduction of information contained within a logical volume (e.g. mounted volume, logical drive assignment, etc).

Lossy Compression
Compression in which data is lost and cannot be retrieved in its original form.

Lossless Compression
Compression in which no data is lost and all data can be retrieved in its original form.

Media
Objects on which data can be stored.

Media Characterization
The process of inspecting, identifying, and noting the properties of the media.

Memory Smear
(c) The modification of data by a running system during the memory acquisition process.

Metadata
Data, frequently embedded within a file, that describes a file or directory, which can include the locations where the content is stored, dates and times, application specific information, and permissions.

Mobile Device
A portable device that has an embedded system architecture, processing capability, on–board memory, and may have telephony capabilities (e.g., cell phones, tablets, and smartphones).

Mobile Phone Forensics
For legal purposes, the utilization of scientific methodologies to recover data stored by a cellular device.

Multiplexer/Demultiplexer
(v) A device used to combine multiple video signals into a single signal or separate a combined signal. These devices are frequently used in security and law enforcement applications for recording and/or displaying multiple camera images simultaneously or in succession.

Multimedia Evidence
Analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein.

Native File Format
The original form of a file. A file created with one application can often be read by others, but a file's native format remains the format it was given by the application that created it. In most cases the specific attributes of a file (for example, fonts in a document) can only be changed when it is opened with the program that created it. [*Newton's Telecom Dictionary*]

Noise
(i,v) Variations or disturbances in brightness or color information in an image that do not arise from the scene. Sources of noise include film grain, electronic variations in the input device sensor and circuitry, and stray electromagnetic fields in the signal pathway. It frequently refers to visible artifacts in an image.

Nominal Resolution
(i,v) The numerical value of pixels per inch as opposed to the achievable resolution of the imaging device. In the case of flatbed scanners, it is based on the resolution setting in the software controlling the scanner. In the case of digital cameras, this refers to the number of pixels of the camera sensor divided by the corresponding vertical and horizontal dimension of the area photographed.

Normal Lens
(i,v) A lens designed to approximate the field of view of the human eye without magnification or reduction. The focal length of a normal lens is based on the sensor size in the camera.

NTSC
National Television System Committee also referred to as National Television Standards Committee.

NVR (Network Video Recorder)
A network based surveillance video recording system, typically utilizing Internet Protocol (IP) cameras and Internet connectivity that allows for remote access through a web client or mobile application.

Original Image
(i) An accurate and complete replica of the primary image, irrespective of media. For film and analog video, the primary image is the original image.

Original Recording
(a) The first manifestation of sound in a recoverable stored format.

PAL
Phase Alternation Line. [*European Broadcast Union*]

Partition
User defined section of electronic media.

Password Recovery
The process of locating and identifying a series of characters used to restrict access to data.

PCB
Printed Circuit Board. A board used in electronics.

Peer Review/Technical Review
An evaluation conducted by a second qualified individual of reports, notes, data, conclusions, and other documents.

Photogrammetry
The art, science, and technology of obtaining reliable information about physical objects and the environment through the processes of recording, measuring, and interpreting photographic images and patterns of electromagnetic radiant energy and other phenomena. [*The Manual of Photogrammetry*, 4th Edition, 1980, ASPRS]
In forensic applications, Photogrammetry, sometimes called "*mensuration*," most commonly is used to extract dimensional information from images, such as the
height of subjects depicted in surveillance images and accident scene reconstruction. Other forensic photogrammetric applications include visibility and spectral analyses. When applied to video, this is sometimes referred to as "videogrammetry".

Photometry
The measurement of light values of objects in an image.

Physical Copy
(c) An accurate reproduction of information contained on the physical device.

Physical Image/Acquisition
(c) A bitstream duplicate of data contained on a device.

Pixel
Picture element, the smallest component of a picture that can be individually processed in an electronic imaging system [*The Focal Encyclopedia of Photography*, 4th Edition 2007].

Playback Optimization
(a,v) The process of determining the most suitable equipment and settings for analyzing the output signal.

Playback
Recorded material viewed and heard as recorded, facilitated by camcorder, cassette recorder, or other device.

Preview
(c) A sub-process of triage where a cursory review of items is performed to assess the need for collection and/or further examination.

Primary Image
(i,v) Refers to the first instance in which an image is recorded onto any media that is a separate, identifiable object. Examples include a digital image recorded on a flash card or a digital image downloaded from the Internet.

Processed Image
(i,v) Any image that has undergone enhancement, restoration or other operation.

Production Switcher
(a,v) A device and/or software used to mix video and/or audio signals from two or more sources (e.g. cameras, videocassette recorder/players, character generators) for dissolves, wipes, and other transition effects.

Proficiency Test
A test to evaluate analysts, technical support personnel, and the quality performance of an agency. (*Four examples are provided)*

1. **Open test** - the analyst(s) and technical support personnel are aware they are being tested.
2. **Blind test** - the analyst(s) and technical support personnel are not aware they are being tested.
3. **Internal test** - conducted by the agency itself.
4. **External test** - conducted by an agency independent of the agency being tested.

Progressive Scan
(v) Display scan pattern where each line of the frame is scanned out sequentially.

Proprietary File Format
Any file format that is unique to a specific manufacturer or product.

Quality Assurance
Planned and systematic actions necessary to provide sufficient confidence that an agency's/laboratory's product or service will satisfy given requirements for quality.

Quantitative Image Analysis
(i,v) The process used to extract measurable data from an image.

Reconstruction
The process of repairing damaged media in order to allow the retrieval of data.

Reference Materials
Refers to items such as published literature, hardware and software documentation, hash sets, header sets, etc.

Reliability
The extent to which information can be depended upon.

Reproducibility
The extent to which a process yields the same results on repeated trials.

Residue
(c) Data that is contained in unallocated space or file slack.
(a) The residue of a filtered signal is the algebraic difference between the filter output and its signal input. [*Diamond Cut Users Manual*]

Resolution
(i,v) The act, process, or capability of distinguishing between two separate but adjacent parts or stimuli, such as elements of detail in an image, or similar colors. [Taken from the *Encyclopedia of Photography,* 3rd Edition]

Resolving Power
(i,v) See "Achievable Resolution".

Restoration
(i,v) Restoration is any process applied to an image that has been degraded by a known cause (e.g., defocus or motion blur) to partially or totally remove the effects of that degradation.
(c) The process of restoring data from an image.

Route
A series of waypoints.

Routing Switcher
(a,v) A device and/or software used to direct the path of one or more signals into one or more devices.

Sharpening
(i,v) A process used to emphasize edge detail in an image by enhancing the high frequency components.

Signature Wiped
Media that has been securely wiped in accordance with acceptable standards, such as those by NIST, utilizing a sector character signature that is unique.

Skimmer
A magnetic card reader used for illegal purposes.

Standard Conversion
(v) The transformation of one television system signal to another. For example, NTSC to PAL.

Source Code
The list of instructions written in a programming language used to construct a computer program.

Storage Media
Any object on which data is preserved.

S-Video
(i,v) A signal in which the luminance and chrominance are separate.

Technical/Peer Review
An evaluation conducted by a second qualified individual of reports, notes, data, conclusions, and other documents.

Time-base Corrector (TBC)
(v) An electronic device used to correct timing inconsistencies and stabilize the playback of the video signal for optimum quality. It also synchronizes video sources allowing image mixing.

Timed Expiry
(v) A feature of DVRs that allows the equipment to adhere to data retention policies that may be mandated in certain parts of the world which results in video data becoming inaccessible after a certain date. This may happen even when the unit is switched off.

Time Lapse Video Recording
(v) Process by which images are recorded at less than the standard rate of frames per second (NTSC – 29.97; PAL – 25.00) thus extending the period of time that can be covered by the storage medium.

Timeline Sequence Reconstruction
The process of relating images, audio, or other data to one another in a chronologically ordered succession.

Track Log
A complete list of trackpoints that a GPS device has created.

Trackpoint
A location automatically created and stored by a GPS device without user interaction as a record of where it has been.

Traditional Enhancement Techniques
(i) Techniques that have direct counterparts in traditional darkrooms. They include brightness & contrast adjustment, color balancing, cropping, and dodging & burning.

Transcode
To convert between formats or encoding methods.

Triage
(c) The process by which items considered for collection or analysis are prioritized to determine the order in which they should be collected and/or analyzed, if at all.

Trusted Media
(c) Media of a known state and risk to the examination.

Unallocated Space
(c) Data storage areas available for use by the computer. The area may already contain previously stored information. Also referred to as *Free Space*.

Validation
The process of performing a set of experiments, which establishes the efficacy and reliability of a tool, technique or procedure or modification thereof.

Validation Testing
An evaluation to determine if a tool, technique or procedure functions correctly and as intended.

Variable Focal Length Lens (Zoom)
(i,v) A lens that the focal length can be continuously changed between set limits. It can range from wide angle to telephoto.

Vectorscope
(v) An electronic device that measures a video signal's chrominance (color) performance.

Verification
1. The process of confirming the accuracy of an item to its original.
2. Confirmation that a tool, technique or procedure performs as expected.

Video
The electronic representation of a sequence of images, depicting either stationary or moving scenes. It may include audio.

Video Analysis
The scientific examination, comparison, and/or evaluation of video in legal matters.

Video Distribution Amplifier
(v) A device used to divide single video signals, while boosting their strength for delivery to multiple video devices.

Video Enhancement
Any process intended to improve the visual appearance of video sequences or specific features within video sequences.

Video Security Recording System
One or more cameras connected to a recording device capable of storing analog or digital video information.

Video Stabilization
(v) The process of positioning individual frames so that a selected object or person will remain in the same location as the video is played.

Waveform Monitor
(v) An electronic device that provides a graphic display of a video signal.

Waypoint
A location that is stored by a GPS device based on user interaction.

Work Copy
A copy or duplicate of a recording or data that can be used for subsequent processing and/or analysis.

WORM (storage)
Write Once, Read Many. A storage technology that allows media to be written only once but read an unlimited number of times.

Write Block/Write Protect
Hardware and/or software methods of preventing modification of media content.

SWGDE Digital & Multimedia Evidence Glossary

History

Revision	Issue Date	Section	History
1.0	07/25/2005		Original Release created by SWGDE and the Scientific Working Group on Imaging Technology (SWGIT)
2.0	01/10/2006	Added Image Data Recovery (i), Image Content Analysis (i), Digital CCTV Retrieval (v), Demonstrative Comparison (v), Video Stabilization (v)	Revision of document by SWGDE and SWGIT. Revision number change.
2.1	06/08/2007	Updated Demonstrative Comparison (v) definition	Revision of document by SWGIT and SWGDE. Revision number change.
2.2	11/1/2007	Removed definition Digital Image (c), Added Forensic Image (c)	Revision of document by SWGIT and SWGDE. Revision number change.
2.3	05/22/2009	Added Aspect Ratio (i,v), Image Restoration (i,v) Sharpening (i,v), Noise (i,v), Deblurring (i,v) Gaussian Blur (i,v), updated Photogrammetry definition, and updated Restoration definition	Revision of document by SWGIT and SWGDE. Revision number change.
2.4	01/14/2011	Added Achievable Resolution definition, Nominal Resolution (i,v), Competency Test, Reference for Peer Review, Forensic Wipe	Revision of document by SWGIT and SWGDE. Revision number change.
2.5	1/13/2012	Added Format, Timed Expiry and Mobile Phone Forensics definitions, modified logical copy to include logical acquisition, modified physical image to include physical acquisition and deleted the word physical	Revision of document by SWGIT and SWGDE. Revision number change.
2.6	6/8/2012	Changed Peer Review to Peer/Technical Review and used same definition as Technical/Peer Review , added Acquisition (c), Extraction (c,i,v), Codec (i,v), Composite Video Signal (i,v), Downloading/Exporting (i,v), DVR (i,v), Enhancement (a,i,v), Fixed Focal Length Lens (i,v), Focal Length (i,v), Normal Lens (i,v), S-Video (i, v), Variable Focal Length Lens (Zoom) (i,v)	Revision of document by SWGIT and SWGDE. Revision number change.

Revision	Issue Date	Section	History
2.7	4/8/2013	Added definitions: Cellular Network Isolation Card (CNIC), Forensic Cloning, Image (c), Pixel, Trusted Media (c), WORM	Revision of document by SWGIT and SWGDE. Revision number change.
2.8	05/27/2015	Added the following definitions: Clean Room/Chamber, Data Smear, Geotag(s), GPX, Memory Smear, Mobile Device, Original Recording, PCB, Preview, Route, Signature Wiped, Skimmer, Track Log, Trackpoint, Transcode, Triage, Waypoint	Revision of document by SWGIT and SWGDE. Revision number change.
3.0 – Draft	02/08/2016	This document was originally created and released in collaboration with SWGIT and titled, SWGDE/SWGIT Digital & Multimedia Evidence Glossary. This update retitled the document, SWGDE Digital & Multimedia Evidence Glossary, and changed the formatting to match SWGDE formatting. Added the following definitions: Forensic Analytical Photogrammetry, NVR (Network Video Recorder), Photogrammetry, Video Security Recording System Modified the following definitions: Image Analysis, Video Analysis Removed the following definition: Photogrammetric Analysis	Revision of document by SWGDE for Draft for Public Comment. Version number change pending release as Approved.
3.0	06/23/2016	Added term “Forensic Video Analysis” and pointed to existing definition for “Video Analysis”.	SWGDE voted to release as an Approved document.

Scientific Working Group
Imaging Technology

As of May 2015, SWGIT has terminated operations

The Scientific Working Group on Imaging Technology (SWGIT) would like to thank the forensic community for the continued support, involvement, and participation in making this group and the documents we have provided over the last 18 years so very successful. The mission of the SWGIT has been to facilitate the integration of imaging technologies and systems within the criminal justice system (CJS) by providing best practices and guidelines for the capture, storage, processing, analysis, transmission, output, and archival of digital evidence. This mission has served our community well since the inception of the group in 1997. The SWGIT documents have been essential to developing laboratory and law enforcement best practices and guidelines across the United States as well as internationally. The documents have been used to demonstrate reliable scientific principles and methods in court and Daubert hearings.

The current economic climate has impacted the continued work of SWGIT. **Due to a lack of funding revenue,** SWGIT has made the decision to terminate operations. SWGIT's website and social media will remain available as a continued valuable resource for all questions involving Forensic Video, Image Analysis, and Forensic Photography.

SWGIT documents will remain in effect and available on the SWGIT website, www.swgit.org. SWGIT has addressed concerns important to all members of the community including first responders, laboratory examiners, and managers of criminal justice organizations. Our website contains more than 20 recommendations and guidelines detailing procedures for digital photography, video and image processing, CCTV installations, documentation of image enhancement, and several other topics important in the current forensic environment. SWGIT was instrumental in the publication of two of our documents as ASTM standards, "Standard Guide for Image Processing" and "Standard Terminology for Digital and Multimedia Evidence Examination."

As the forensic community moves forward, a goal of SWGIT is to continue to engage the entire law enforcement imaging community in the development of guidelines, best practices, and standards. In remaining true to that goal, SWGIT strongly encourages the members of our forensic disciplines to continue to support other professional groups that strive to provide such information.

SWGIT will continue to have an active web presence at www.swgit.org and on social media. Please see the social media links provided on our website.

Thank you again for making SWGIT such a long-standing success.

Melody Buba, Chair
Federal Bureau of Investigation

Cory Winar, Vice Chair
Eugene Police Department