

Contents

WELCOME	4	STEP 2 - CAPTURE	16
INTRODUCTION	5	2.1. Capture	16
ACKNOWLEDGEMENTS	6	2.1.1. Accurate Representation of the Evidence	16
ABBREVIATIONS	7	2.1.2. Third Party Capture	16
KEY RECOMMENDATIONS	8	2.1.3. Documentation	17
MANAGING THE DIGITAL IMAGE PROCESS	9	2.2. File Formats	17
Image Evidence	9	2.2.1. Common File Formats	17
Image Management in Large-Scale Incidents	10	2.2.2. File Sizes	17
THE DIGITAL IMAGE PROCESS	11	2.3. Authority to Delete Images	19
STEP 1 - PREPARATION	12	2.4. Capture and Storage Media	19
1. Preparation	12	2.4.1. Non-reusable removable medium	20
1.1. Training, Quality and Validation	12	2.4.2. Re-usable Removable Medium	21
1.1.1. Personnel	12	2.4.3. Non-removable Medium	21
1.1.2. Quality Management Programs	12	2.4.4. Secure Digital Storage System (secure server)	22
1.1.3. Accreditation	12	2.4.5. Transmission	22
1.1.4. Validation	13	2.4.5.1. Access to Third- party Networks	22
1.1.5. Awareness Program	13	STEP 3 - USE	23
1.2. Obtain Authority	13	3.1. Continuity	23
1.3. Equipment	14	3.1.1. Verification Techniques	23
1.4. Start Audit Trail	14	3.1.2. Encryption	23
		3.1.3. Watermarking	23
		3.1.4. Handling and Storage Conditions	24
		3.2. Legal Considerations	24

Contents continued

3.3. Use of the Image	24	STEP 4 - RETENTION AND DISPOSAL	29
3.4. Defining the Original Image and the Production of Working Copies	24	4.1. Retain for Statutory Period	29
3.4.1. Defining the Original Image	24	4.1.1. Record Storage	
3.4.2. Secure Storage and Documentation of Original Images	24	Considerations	29
3.4.2.1. Security	25	4.2. Dispose of Exhibits and Finalise Audit Trail	30
3.4.2.2. Storage Environment	25	GLOSSARY OF COMMON TERMS	31
3.4.2.3. Documentation	25	BIBLIOGRAPHY	34
3.4.3. Production of Working Copies	25	Further reading	34
3.5. Digital Image Processes	25	APPENDIX A	35
3.5.1. Image Enhancement	26		
3.5.2. Image Restoration	27		
3.5.3. Image Analysis	27		
3.5.4. Image Syntheses	27		
3.5.5. Image Compression	27		
3.5.5.1. Lossy vs Lossless Compression	28		
3.5.5.2. Cautions with Compression	28		
3.6. Presentation in Court	28		

Welcome

The Australia New Zealand Policing Advisory Agency National Institute of Forensic Science (ANZPAA NIFS) in conjunction with the Senior Managers of Australia and New Zealand Forensic Science Laboratories (SMANZFL) seeks to advance forensic science and related technologies.

The rapid uptake of next-generation digital imaging and related technologies across the community creates significant challenges and opportunities for forensic science service providers, clients and stakeholders.

The convergence of digital imaging that now uses an ever increasing range of image capture devices, with new communication technologies, hardware systems, software applications, and large scale data storage capabilities, creates a very complex technological operating environment.

The need for consistent national guidelines regarding the use of these technologies in forensic science for practitioners is perhaps even more crucial than ever before.

The development and adoption of methods of best practice with respect to the gathering and presentation of digital evidence remains essential to ensure that such evidence can be relied upon by the courts.

It is also important that the methods employed are constantly reviewed and improved to keep pace with the ongoing advances in technology.

Digital imaging itself is now a widely accepted source of secondary physical evidence within the judicial system. However, digital images can be easily duplicated, manipulated, contaminated, or altered.

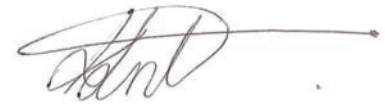
Thus it remains imperative that forensic science practitioners can validate the origin and integrity of digital images through the procedures employed in their capture, storage, transmission, processing, analysis and reporting of this type of evidence.

The Electronic Evidence Specialist Advisory Group (EESAG) has revised the National Guidelines for Digital Imaging Processes issued in 2004.

The resultant 2013 Guidelines contained in this document are a positive reflection of EESAG's endeavours to actively involve a wide range of industry practitioners in the revision process.

It is hoped that this document will provide valuable guidance for police and forensic laboratories in the enhancement of their digital imaging procedures.

Accordingly, ANZPAA NIFS and SMANZFL are pleased to endorse the guidelines contained within this document and encourage laboratories to adopt the principles outlined herein.



Karl Kent OAM BSc. A.Dip.For.Inv

EESAG Mentor

Senior Managers Australian and New Zealand Forensic Laboratories (SMANZFL)

Introduction

The 2013 revision of the 2004 *Australia and New Zealand Guidelines for Digital Imaging Processes* document continues the mission of the Electronic Evidence Specialist Advisory Group (EESAG) established under the auspices of the Senior Managers of Australian and New Zealand Forensic Laboratories (SMANZFL) and the Australia New Zealand Policing Advisory Agency National Institute of Forensic Science (ANZPAA NIFS), in providing strategic policy advice and guidance on cross-jurisdictional policing initiatives to facilitate the introduction and integration of digital imaging technologies within Australia and New Zealand law enforcement and forensic organisations.

This document was developed in response to the demand from the forensic community in Australia and New Zealand, for a review of the 2004 document. Through consultation with subject-matter experts and an international body of knowledge across a range of forensic disciplines, as well as the UK Home Office Centre for Applied Science and Technology (formerly Home Office Scientific Development Branch) and Scientific Working Group for Imaging Technologies (SWGIT, USA), they represent world's best practice across a range of disciplines that utilise digital imaging technologies in their workflows.

This version encompasses current and emerging technologies in capture, storage and transmission of images, as well as advancements in forensic practices that integrate these technologies into a modern workflow.

The use of digital images in the criminal justice system bears the same onus on the witness as previous imaging technologies as to the depiction of the image to being a true (fair¹) and accurate representation of what it purports to depict².

The authentication requirement is still primarily with a witness, through testimony, that the image:

1. was captured by that person
2. is a depiction of a subject that the witness is capable of advising the court on, and/or qualified to verify its accuracy
3. was captured by a device that has been validated by an expert witness as to its correct operation.

The susceptibility to either abuse or misuse of digital images lies within one of their key benefits - the ability to produce an identical (bit-for-bit) copy of a recording or image. The safeguards lay with the security of the storage medium, the testimony of the witness, and the verification that the copies have originated from the Primary or Original Image.

By adhering to robust and accepted work practices that maintain the integrity of the image, the evidential value will not be compromised.

The principles outlined here may apply to other disciplines, such as computer forensic, and audio/video signal processing.

These fields may also utilise guidelines, techniques and terminology that are similar to but distinct from the image-specific guidelines in this document.

The fundamental principle of Primary and Original Images and the associated practices are directly applicable to any digital recording to be used in evidence, whether it be digital evidence, visual, or audio material.

While all appropriate steps have been taken to standardise terminology and nomenclature within these guidelines to correlate to local usage, some jurisdictions are bound, either by legislation or interdependent policy, to use equivalent or similar terminology.

Agencies are to equate terminology within this document to locally-used terminology in order to establish an equivalency in meaning that will still enable the formulation of local policy and procedures within this framework.

Clarification within locally-produced documents should refer to the terminology used in these guidelines and their correlation to the local nomenclature.

These guidelines provide guidance and advice on the steps involved in the digital process – from initial capture through the processing stages, to presentation in court and the eventual retention and/or disposal.

They serve as a framework for agencies to develop and adapt local policies that are compliant with current 'good practice'.



Darren Bails

Forensic Services Branch, South Australia Police

Chair, Digital Imaging Scientific Working Group, EESAG, 2013

When reading and applying these guidelines, consideration must be given to other applicable and relevant legislation, accreditation guidelines (e.g. ISO 17025, NATA and ASCLD/LAB), and interdependent organisational procedures.

1. Scientific Working Group on Imaging Technology (SWGIT) Section 13 'Best Practices for Maintaining the Integrity of Digital Images and Digital Video' Version 1.1 2012.01.13.

2. ALMOND v. THE STATE, 274Ga. 348, 553 S.E.2.d 803 (Georgia, USA 2001).

Acknowledgements

The *2013 Australia and New Zealand Guidelines for Digital Imaging Processes* are the second revision of the document drafted in 1998 by the Working Party for Imaging Technologies on behalf of the ANZPAA NIFS and SMANZFL.

This revision was developed by members of the Electronic Evidence Specialist Advisory Group, Digital Imaging Scientific Working Group 2010-11.

Sergeant Darren Bails - South Australia Police
Senior Sergeant Stuart Cross - Queensland Police Service
Acting Senior Sergeant Chris Flight - Victoria Police
Senior Sergeant Mike Whitaker - New Zealand Police
Senior Sergeant Alex Wells - Western Australia Police
Senior Constable Matthew Ward - Western Australia Police
Dion Sheppard - ESR – New Zealand
Jason Barr - ESR – New Zealand
Shaun Ellis - Australian Federal Police
Graeme Kinraid - Australian Federal Police
Sergeant Brian Barnes - New South Wales Police Force
Senior Sergeant Arnold Jansen - New South Wales Police Force
Ellen Pocock - Northern Territory Police
Senior Sergeant Kerrie Whitwam - Tasmania Police
Senior Sergeant Troy O'Malley - Queensland Police Service

The contributors to the previous development of these guidelines consist of:

1998 Working Party for Imaging Technologies

Inspector Adrian Freeman, Chair - Queensland Police Service
Sergeant Darren Bails, Secretary - South Australia Police
Senior Sergeant Troy O'Malley - Queensland Police Service
Associate Professor Gale Spring - RMIT University
Greg Humphries - RMIT University
Kerry Wilson - New South Wales Police Force
Hermann Metz - Victoria Police
Peter Williams - Executive Officer NIFS, 1998

2003 Working Group

Senior Sergeant Troy O'Malley, Chair - Queensland Police Service
Sergeant Darren Bails - South Australia Police
David Chadwick - Australian Federal Police
Dean Catoggio - Victoria Police
Sarah Donnelly - ESR - New Zealand
Associate Professor Gale Spring - RMIT University
Greg Humphries - RMIT University
Anna Davey - Executive Officer NIFS

Thanks must also go to ANZPAA NIFS for their continued support, in particular Dr Linzi Wilson-Wilde and all the representatives from Specialist Advisory Groups and Scientific Working Groups providing information, opinions and feedback for discussions on the implication and application of these guidelines to their respective disciplines.

Due recognition and thanks must go to the Association of Chief Police Officers (ACPO - UK) and the Home Office Centre for Applied Science and Technology (formerly Home Office Scientific Development Branch), for permission to use Version 1 of the Digital Imaging Procedure, as the major reference for the source document in 2004 (current version 2.1 November 2007).

They, in conjunction with the UK National Policing Improvement Agency must also be recognised for their publications and invaluable research dedicated to the improvement of policing.

Recognition must also go to the Scientific Working Group for Imaging Technologies (SWGIT - USA) for their support, significant publications, and research, since 1997.

They have been the major drivers to inform and educate the international law enforcement community in matters relating to digital imaging and electronic evidence, and are an invaluable source of information.

Abbreviations

ASCLD/LAB	American Society of Crime Laboratory Directors / Laboratory Accreditation Board (Int)
ACPO	Association of Chief Police Officers (UK)
ANZPAA NIFS	Australia New Zealand Policing Advisory Agency – National Institute of Forensic Science (AUST/NZ)
ASTM	American Society for Testing and Materials (USA)
DSD	Defence Signals Directorate (Department of Defence) (AUST)
EESAG	Electronic Evidence Specialist Advisory Group (AUST/NZ)
HOCASST	Home Office Centre for Applied Science and Technology (UK) - formerly the Home Office Scientific Development Branch (UK)
ISO/IEC	International Standards Organisation/International Electrotechnical Commission (Int)
NATA	National Association of Testing Authorities (AUST)
NIST	National Institute of Standards and Technology (USA)
NPIA	National Policing Improvement Agency (UK)
SMANZFL	Senior Managers Australian and New Zealand Forensic Laboratories (AUST/NZ)
SWGIT	Scientific Working Group on Imaging Technology (USA)
SWGDE	Scientific Working Group on Digital Evidence (USA)

Key Recommendations

The 2004 guidelines made key recommendations for organisations adopting the use of digital imaging practices. Those are still applicable to the current use of digital images in the forensic context.

The following key recommendations are summarised from the *2013 Australia and New Zealand Guidelines for Digital Imaging Processes*. Further clarification and information can be obtained from the expanded discussion of these points within this document.

1. These guidelines are intended to standardise all practices of digital image processing and safeguard digital media from adverse legal criticism.
2. The process of the digital image is addressed as the following stages, preparation, image capture, use of the image (storage, processing, analysis, output, transmission and presentation), and retention and disposal.
3. An image captured by any device capable of capturing a digital image should be archived and maintained in an original state.
4. The integrity of the Original Image must be preserved and should not be subjected to processes that cause permanent alteration.
5. Where any type of image processing is to take place this should be performed on a Working Copy of an Original Image.
6. The word 'manipulation' should not be used in law enforcement and forensic contexts, relating to digital processing applications.
7. The digital imaging processes that are in place within the organisation should be validated.
8. All personnel utilising digital imaging technologies should be trained in the application of those technologies and their assessments documented if working within an accreditation framework.
9. Personnel and organisations within the law enforcement and forensic communities that are utilising digital imaging processes should be aware of the standards and practices commonly referred to within the process and should strive to conform to, or exceed those standards and practices.



Managing the Digital Image Process

Digital evidence can be susceptible to either abuse or human error, either by ignorance and/or inexperience in the management of this evidence. Procedures should be implemented to validate forensic digital imaging processes and safeguard those digital images from adverse criticism.

Agencies, or part thereof, within or associated with the legal system, in particular law enforcement and forensic agencies that are engaged in the capture, storage, processing, analysis, transmission, or output of digital images, should ensure that their images and imaging processes are governed by documented policies and procedures.

This document provides a set of broad guidelines for the development of standard operational procedures within these agencies.

The process of digital imaging is addressed as the following steps.

1. **Preparation.**
2. **Capture** – Creation of the Primary Image. Includes storage and transmission.
3. **Use** – Defining the Original/Working Images. Includes image processing, compression, analysis, output and presentation.
4. **Retention and Disposal.**

Within all these steps of the digital image process the integrity of the Original Image must be maintained.

The status of the image as it moves through the digital management process is defined below:

Primary Image

The first instance in which an image is recorded onto any media that is a separate identifiable object or objects³.

Original Image

The Primary Image or an exact binary copy of the Primary Image.

- There can be any number of Original Images.
- The file name may be changed depending on jurisdictional policies but the actual image data must remain exact.

Working Copy

A copy of the Original or Primary Image.

- This may involve applying processes that change the file format or Original Image data in any way. (Including enhancement, compression, processing, filtering, cropping etc).

Throughout this document, the terms 'Working Copy' and 'Working Image' should be taken as interchangeable and meaning the same.

Image Evidence

Evidence, in terms of a still image or video footage, is the presentation of visual facts about the crime or an individual that the prosecution or defence presents to the court in support of their case. The images will be presented either as a hard copy or on a screen.

Images deemed for 'intelligence purposes' are not included in the processes outlined in this document. The adherence to these guidelines is concerned with those images deemed for 'evidentiary purposes'.

It is possible to make a binary (bit-for-bit) identical copy of a digital image file. In evidential terms there is no distinction between the content of Primary or Original files because they are the same and have the same evidential weight⁴.

It is not important whether the file is on a stand-alone or networked-computer, a server, or on any type of portable storage medium. This assumes the operation of adequate security against unauthorised and unrecorded access. It also allows for the existence of multiple Originals taken from the first binary copy of the Primary Image.

As stated before, the **Primary Image** is the first instance in which data is recorded in memory and from which the image can be generated. This is normally the image recorded on the memory card of a digital camera. It follows then that the **Original Image** is any bit for bit duplication of the data, irrespective of the media.

There can be any number of Original Images; however for evidential purposes it is essential to be able to demonstrate to a court that they are identical to the Primary Image. This fundamental principle and the associated practices are directly applicable to any digital recording to be used in evidence, whether it is visual or audio material.

3. Scientific Working Group on Imaging Technology (SWGIT) Section 1 'Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System' Version 3. 3 2010.06.11.

4. House of Lords, Science and Technology Select Committee, Fifth Report entitled 'Digital Images as Evidence' 3 February 1998. Chapter 2.

Digital image files can be used in exactly the same way as film-based photography and video, with written and/or electronic audit trails used to track and verify the veracity of the file.

Digital images should not be thought of as replacements for conventional (hard-copy) photographs and videos, but alternative technologies.

It has to be recognised that digital images are not necessarily better than hard copies, and that images produced with digital technology may appear different to those from an analogue source.

Some lower resolution digital images displayed on a computer screen or as hard copy might not appear very lifelike but then neither do many simulations.

The important and overriding factor is that the content and quality of the image should be fit for the purpose and that the process has been validated.

To this end, the use of desktop printers for hard copies of stills and low-resolution video footage should not be ruled out. It is not always necessary or feasible to produce the highest quality images to demonstrate the facts required for the evidence.

Image Management in Large-Scale Incidents

It is recommended that in large-scale incidents that involve imaging as part of the investigation or repatriation process (e.g. major disaster involving Disaster Victim Identification, Counter-Terrorism, CBRN incidents etc), that specific consideration be given to assigning appropriate staff and resources to an image and information management role.

This can be as part of, or separate to, a file management capability, but the ability to successfully undertake either role should not be compromised by the other.

Given the transition to primarily digitally-based images, the importance of suitably trained and skilled personnel to manage the gathering, cataloguing, storage and security of images (including video), captured or collected in relation to the incident, should not be under-estimated.

Appropriate resources should also be allocated to ensure the efficient and effective execution of this role.

The required skills for this position should include:

- a high level of computer literacy
- working knowledge of photographic, imaging and video issues
- working knowledge of the *2013 Australia and New Zealand Guidelines for Digital Imaging Processes* and their application to investigation
- knowledge of the IT requirements for an effective image management system
- good communication (written and oral), organisation and file management skills
- knowledge of local jurisdictional policies in image and records management.

On selecting the suitable personnel to manage images in sensitive or particularly graphic incidents, the welfare of the assigned person/s should be monitored closely and relief provided where necessary.

The Digital Image Process

This diagram summarises the Digital Imaging Process as outlined in these guidelines. The 'Digital Image Process Workflow' diagram (Appendix A) shows a visual representation of the whole digital image management process.

1.1 Training, Quality and Validation
1.2 Obtain Authority
1.3 Equipment
1.4 Start Audit Trail

2.1 Capture
2.2 File Formats
2.3 Authority to Delete
2.4 Storage Media <ul style="list-style-type: none">• Non-reusable, removable medium (WORM media -CD- R/DVD-R)• Reusable, Removable Medium (memory cards, video tape)• Non-removable Medium,(hard drive, solid state memory)• Secure Digital Storage System (secure server)• Transmission.

3.1 Continuity
3.2 Legal Considerations
3.3 Use of Image
3.4 Defining the Original and the Production of Working Copies
3.5 Digital Image Processes <ul style="list-style-type: none">• Image Enhancement• Image Restoration• Image Analysis• Image Synthesis• Image Compression
3.6 Presentation in Court

4.1 Retain for Statutory Period
4.2 Dispose of Exhibits and Finalise Audit Trail

Step 1 - Preparation

1. Preparation

These sections of the guidelines include the preparatory steps before images are captured. This may be directly before the images are taken, or at an earlier stage or date where work can be anticipated. The steps identify the importance of:

- obtaining relevant training and maintaining competency in the skills required for the digital imaging processes that are to be used
- obtaining relevant training and instruction in local procedures, including system validation and quality management practices
- obtaining relevant authorisations
- checking equipment, either routinely or at the commencement of the image capture activity
- starting an audit trail at the earliest opportunity, when it is known that digital images are to be captured.

Such checks will minimise risk of failure and/or avoid challenges about conformance with accepted local procedures.

Due to advancements in the integration of digital capture systems into more common devices, non-specialists in operational situations and locations may increasingly use these devices, so adherence to an established procedure will assist in safeguarding those captured images.

1.1. Training, Quality and Validation

1.1.1. Personnel

All personnel utilising digital imaging technologies in the forensic context should be trained and assessed for competency, with regard to the particular organisation's standard operating procedures and the operation of the relevant imaging technologies.

All training and competency assessment programs need to be documented in accordance with the organisation's procedures. Where organisations have an accredited quality management system, the competence assessment and subsequent documentation must be in accordance with the system.

The Scientific Working Group on Imaging Technology (SWGIT) produce a number of guideline and best practice documents that deal with specific areas of forensic imaging, including training and the specific application of digital imaging to forensic applications e.g. field photography equipment, recording footwear impressions, image analysis, and training. These can be found at the SWGIT website⁵.

1.1.2. Quality Management Programs

All organisations that utilise images and imaging technology in the forensic context should implement quality management programs that safeguard images against accidental and illegal practices. The electronic process that is in place within the organisation should be able to validate the end results.

The quality management system should contain scheduled and documented performance reviews, calibrations, audits, and corrective actions to ensure results achieved are consistent and reliable. The National Association of Testing Authorities (NATA) has produced a number of Application Documents and Technical Circulars that deal with specific aspects of the application of ISO/IEC 17025 for forensic facilities, including training and accreditation. Access to these documents can be arranged through individual organisation's quality management sections.

Standards Australia are producing a series of Australian Standards under AS 5388 Forensic Analysis that deal with various aspects of the forensic evidence collection, analysis and recording process⁶. This includes the capture and validation of forensic evidentiary images and digital evidence.

1.1.3. Accreditation

Jurisdictions, organisations and facilities working within an accreditation framework to ensure competence and compliance of testing and calibration functions and equipment, all base their processes on the requirements of ISO/IEC 17025.

Facilities accredited under an approved accreditation body must comply with requirements in relation to training and competence of staff, facility security, document control, audits, quality management, method validation, equipment calibration and health and safety.

5. www.swgit.org

6. At the time of publication, ISO/IEC Draft Standards AS 5388 and 2nd CD 27037 were still in the approval and comment process.

Step 1 - Preparation continued.

In Australia and New Zealand, the two main compliance agencies are the National Association of Testing Authorities, Australia (NATA), and the American Society of Crime Laboratory Directors/Laboratory Accreditation Board - International (ASCLD/LAB-International).

The guidance documents that relate to Australia and New Zealand jurisdictions are:

- National Association of Testing Authorities, Australia - ISO/IEC 17025 DRAFT Field Application Document - Supplementary Requirements for Accreditation - June 2011⁷ (Australia)
- American Society of Crime Laboratory Directors/ Laboratory Accreditation Board (International) – Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories – April 2011⁸ (New Zealand).

These guidelines should form part of an agency's policy on digital image management and applied in accordance with the requirements specified by that agency's accreditation and any other standards applicable to the disciplines employed at that facility.

1.1.4. Validation

It is recognised that forensic digital imaging is used for a variety of purposes and examinations with a wide range of accuracy and/or quality requirements. The quality of a digital image is affected at capture by three main factors:

- spatial resolution (size of the image/number of pixels)
- bit depth (amount of grayscale and colour information able to be recorded)
- compression (file size reduction through software processing).

The quality of an Imaging System is dependent on its parts and includes the capture, storage and output stages. Image quality must be agreed and validation tests carried out to ensure suitability for the intended purpose.

Validation is the developmental process used to acquire the necessary information to assess the ability of the Imaging System to obtain a result reliably, to determine the conditions under which such results can be obtained and to determine the limitations of the Imaging System.

The validation process identifies critical aspects of the system that must be carefully controlled and monitored⁹. Each forensic discipline and/or organisation should determine the accuracy and precision requirements for imaging equipment and set its calibration/verification program accordingly. It should also be noted that similar items of equipment used for different functions may have different calibration/verification requirements.

1.1.5. Awareness Program

Personnel and organisations within the law enforcement and forensic communities that are using digital imaging technology should be aware of the standards commonly followed within these disciplines and should strive to conform to, or exceed, these standards.

This can be done by:

- maintaining good practices in digital imaging processes
- pursuing continuing education courses in imaging
- being aware of legal developments relating to the use of imaging technologies.

The following stakeholders would benefit from an awareness program regarding the capabilities and limitations of emerging specific imaging technologies:

- law enforcement personnel
- forensic practitioners
- legal representatives (defence and prosecution)
- judiciary
- personnel involved in the administration of justice.

1.2. Obtain Authority

This instruction applies to all individuals responsible for capturing images by virtue of their role or position within the organisation. They are empowered within their appointed role to capture images for the purposes of their particular work. Specific roles and responsibilities, e.g. for a Crime Scene Investigator, will be written into their job descriptions, training and instructions, together with any verbal instructions. Obtaining authority is not necessarily required for each separate operational task.

7. National Association of Testing Authorities, Australia, ISO/IEC 17025 DRAFT Field Application Document – Supplementary Requirements for Accreditation – June 2011.

8. American Society of Crime Laboratory Directors/Laboratory Accreditation Board (International) – Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories (Corresponds to ISO/IEC 17025: 2005) – April 2011.

9. National Association of Testing Authorities, Australia, ISO/IEC 17025 DRAFT Field Application Document – Supplementary Requirements for Accreditation – June 2011.

Step 1 - Preparation continued.

However, organisations need to be aware that specific authorisations may need to be obtained before some images are taken, e.g. authorisation to permit images to be taken where an intimate forensic procedure is conducted. Where this is the case, it should be recorded within the audit trail or case file notes of the operation.

1.3. Equipment

The correct operation and maintenance of any equipment is essential to a robust forensic imaging system. It is also imperative that operators are familiar with the features and operation of the equipment.

All equipment utilised in imaging should be maintained in accordance with the manufacturer's specifications and recommendations, as contained under warranties and operating manuals. All maintenance should be documented and performed by authorised technicians. This maintenance log may form part of the audit trail for an examination or larger operation.

On a regular basis, and if a modification is made to the system, an end to end check must be performed to ensure the consistency is maintained within the specific system parameters.

If a process or piece of equipment does not meet required standards* or needs to be repaired, that piece of equipment must be removed from the process until the fault is rectified. Evaluation of equipment and system checks should be documented, inclusive of corrective action. If applicable, calibration schedules of capture equipment, hardware or software should be followed.

In particular it is suggested that prior to using any equipment for image capture, checks are made to ensure that:

- operator-adjustable settings are made appropriately
- the time and date settings are correct (and any inconsistencies are documented)
- there are adequate supplies of recording media
- the media should either be new, reformatted or erased in an approved manner
- any media protection settings will not prevent recordings being made
- if the equipment is battery operated, there are sufficient fully charged batteries available
- a scheme of checks is carried out before deployment particularly for equipment that is used less frequently.

This list is not definitive and detailed information should be obtained from appropriate equipment or user manuals.

**Note: While image capture equipment may not fall under the equipment calibration schedule provided under the NATA ISO/IEC 17025 DRAFT Field Application Document - Supplementary Requirements for Accreditation - June 2011 (or respective ASCLD/LAB reference), provision for repairs, maintenance, and checking (including calibration, if required), of capture equipment should form part of any agency implementation.*

1.4. Start Audit Trail

One of the fundamental requirements of digital imaging is the need to safeguard the integrity of images. Part of this process involves an audit trail being started at the earliest stage. This can be in written or electronic format.

The audit trail for the images is usually part of the audit trail for the larger operation or examination being carried out. Consideration should be given to the audit trail, before the capture of any police-originated images. The audit trail for digital images commences with the metadata embedded in the Primary or Original Image file from the capture device. For this reason, it is imperative that the time/date recording in the capture device is accurate and verified by the operator.

The person who captures the Original Image, or was present at the time the Original Image was captured, should make documentation to support oral testimony as to its origin and integrity as being a fair** and accurate representation of the scene or evidence.

The audit trail should include or be linked to records which include the date and time of action and:

- details of the case
- description of shots or footage taken and a log of the media used
- if the image is third-party generated, information about the source of the image and its status as an Original Image or Working Copy
- details regarding downloading of the Primary Image
- the creation and defining of the Original Image
- the creation and defining of additional Original Images or Working Copies
- details and reasons for any selective capture or retrieval
- storage details of the Original Image

Step 1 - Preparation continued.

- details of any access to the Original Image in a manner that could affect the integrity of the image, including the time/date of access and details of any person accessing the image(s)
- details of any copying that is required to ensure the longevity of the Original Image
- use of Original Image in court
- disposal and/or retention details.

The level of documentation undertaken should be commensurate with the complexity of the processes applied to the image, and in accordance with relevant legislation, accreditation guidelines^{10,11} and/or individual organisation procedures.

***See Section 2.1.1. in relation to discussion on the terminology used here.*

10. National Association of Testing Authorities, Australia, ISO/IEC 17025 DRAFT Field Application Document – Supplementary requirements for Accreditation – June 2011.

11. American Society of Crime Laboratory Directors/Laboratory Accreditation Board (International) – Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories (Corresponds to ISO/IEC 17025:2005) – April 2011.

Step 2 - Capture

2.1. Capture

Capture is the process of recording (acquiring) data, such as an image or video sequence¹². The purpose and requirements of the end product drive the selection of image acquisition device (camera, scanner and recorder).

Therefore, the final use of the image should determine the choice of capture device, whether it be digital or analogue. The image quality setting of evidentiary digital images should be selected and validated relating to the end requirements of the image rather than to minimise the storage requirements.

2.1.1. Accurate Representation of the Evidence

The image capture device should be capable of producing an accurate representation of the evidence being recorded.

Even in the agreed absence of any deliberate malicious alteration by anyone, images can never be an exact reproduction of the scene. Digital image capture devices use a multitude of complex image processing techniques to convert the signals from the imaging sensor into picture elements (pixels) that form an image of the subject. The image can only ever be an approximation of the subject.

It is commonly accepted that the output of the camera is 'true/fair'* or 'accurate', because the aim of the manufacturer is to produce as 'lifelike' an image as possible within the cost-band of the camera. The image quality must be agreed and validation tests carried out to ensure suitability for the intended purpose.

The variables within images that contribute to this accuracy include factors such as:

- exposure
- colour accuracy
- focus
- distortion
- size (or relative size)
- compression
- relationship within the scene.

Various forensic applications will dictate different standards of accuracy and require validation of the capture device and method used. At a minimum, the following criteria should be considered when selecting appropriate capture devices to ensure the quality and integrity of images.

- Characteristics of the scene or evidence (size, location, detail required etc).
- Any requirements established by the source agency in relation to capture settings or parameters e.g. resolution.
- Lighting of the items of interest.
- Dynamic range of the scene.
- Time or weather constraints.
- Required end products or output (including use in other systems e.g. ICSR or NAFIS).

**Note: The traditional terminology relating to admissibility criteria was 'a true and accurate representation', due to the fact that no imaging system can reproduce the human visual system exactly and images are only ever an approximation and not actually a true record. SWGIT and the courts in the USA are using a description leaning towards 'accurately and fairly depict' as the criteria.*

While not intending to dilute the court requirement that an image must be a 'true and accurate' representation of the subject as captured, it is more realistic to represent images as being a 'fair and accurate' representation, given the technologies being used and processes applied to the image in-camera.

2.1.2. Third Party Capture

Digital images are not always captured by organisations that have adopted the *Australia and New Zealand Guidelines for Digital Imaging Processes* or similar standards. Where this third party capture occurs, the digital workflow diagram (Appendix A) should be used to establish the 'point of transfer' at which the responsibility for the handling of third party images is transferred to the organisation (i.e. Primary, Original or Working Copy).

The 'point of transfer' will depend on the nature of images being transferred, the recording format, and equipment used by the third party. At whatever stage this 'point of transfer' occurs, the audit trail must start from that point and compliance with the processes outlined in these guidelines commence. Continuity of image handling should be demonstrated throughout by ensuring that the audit trail links directly to any audit trail that is available from the third party.

Whichever medium is chosen for the capture and initial storage of images, effective means must be available for transferring the images to the computer system where they are to be used and archived.

12. SWGIT – Section 1 – Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System – Version 3. 3 2010.06.11.

Step 2 - Capture continued.

2.1.3. Documentation

Documentation should be made by persons involved in the image capture and handling processes to assist in the authentication of the origin and integrity of the image, and to support oral testimony that the image portrays what it is alleged to portray.

The documentation may be in electronic or hard-copy format and should be appropriately filed with relevant information from the case or securely attached to the relevant case notes.

2.2. File Formats

Digital data files can have a variety of formats. The file format is the structure by which data is organised into a file and relates to the application(s) able to open and view the file. The file format may include inherent compression to reduce the size of the file. Metadata (data in the file in addition to the image data), captured at the time of the image or during the post-processing of the image, is often present and able to be analysed.

Digital images can be stored using open or proprietary formats. This means these latter images may have to be processed in a specialised software package to enable viewing or further processing. The choice of format is a consideration for the ease of incorporating images into publications, viewing or printing, and transmitting to others.

It should be noted that file extensions are the common way for the file format to be identified, but as these can be easily changed, should not be the sole method of identifying the actual file format. Changing a file extension may create problems in reading or opening files. The use of some image editing programs may alter metadata from the original files.

The choice of file format is not relevant to the admission of the evidence, only to the quality, impact on storage and replay requirements, and may be a consideration in the retrieval of long-term archived images. Organisations need to maintain versions of specialised software packages to enable this retrieval in the future.

2.2.1. Common File Formats

Parts of the following list of common image file formats are reproduced from the SWGIT document 'Section 19 - Issues Relating to Digital Image Compression and File Formats Version 1.1 2011.01.15'. It is not an all-inclusive list but provided for basic information about the common formats encountered and their inherent characteristics.

JPEG Variants

JPEG (Joint Photographic Experts Group) is a digital compression and coding standard developed in 1992 for continuous-tone still images and bound by ISO/IEC IS10918-1 to ensure all files developed under this format are compatible. There are a number of common variants under this format. JPEG uses a redundancy (discrete cosine transform) method to calculate what information in the image can be discarded in the compression process whilst maintaining image quality (see 3.5.5. Image Compression for additional information about terms used in this section).

- **JFIF** - JPEG File Interchange Format (JFIF) is a common file format that stores JPEG-compressed information. This file format uses the file extensions .JPG or .JPEG. This leads to confusion between JPEG, which is a compression algorithm and JFIF that is a file format. Depending on the level of compression applied, the artefacts visible in the image may or may not be visible to the naked eye.
- **EXIF** - Exchangeable Image File format is a format designed to record and standardize the exchange of images with image metadata between digital cameras and editing and viewing software. It is a file standard similar to the JFIF format with TIFF extensions and incorporated in the JPEG-writing software used in most cameras. Each image has its metadata embedded in the image data and it records variables such as the camera model, time/date the image was taken, camera settings (shutter speed/aperture/white balance etc), compression, and image size. The EXIF data can be displayed when images are viewed or edited by image editing software and can also be used to document changes to the image.
- **JP2** - is the file format created for the JPG 2000 compression algorithm. This format was created by the Joint Photographic Experts Group committee in 2000 to supersede the JPEG standard and standardised under ISO/IEC 15444. It is based on wavelet compression.

TIFF - Tagged Image File Format is a flexible open format that can be compressed or uncompressed. TIFF images from digital cameras tend to be large because they are limited on the amount of compression applied and have all of the colour 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 (see 3.5.5. Image Compression).

Step 2 - Capture continued.

While the most common algorithms associated with the TIFF format are lossless, one cannot assume this with every image. TIFF files are also a much larger file than compressed formats, so storage considerations could be an issue.

PSD - Photoshop Document is a proprietary format specific to Adobe software. In addition to the image information, all layer information is retained. It can also contain embedded information about the history of image processing applied to the image within Adobe applications.

It is useful for working within Photoshop but images cannot be used in most other applications. Due to their large size and proprietary nature, mechanisms should be in place for retrieval if archiving PSD files, and they are not recommended as an archival format for these reasons.

RAW Variants

The RAW file format is not a specific file format but a class of formats and refers to the unprocessed data from the camera sensor. 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. As it is a data file rather than an image file, typically, cameras are packaged 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 may 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.

RAW files are also a much larger file than compressed formats, so storage considerations may also be an issue. With over 20 different RAW file formats available, three of the more common formats used in forensic areas are explained here:

- **DNG** - Adobe Photoshop's Digital Negative format is a royalty-free RAW image format designed by Adobe systems. DNG is based on a TIFF format and mandates the use of metadata. DNG was a response to demand for unifying camera RAW file formats. Many common camera RAW files can be converted to DNG format.
- **NEF** - Nikon Electronic Format is a proprietary RAW image format used by Nikon. It is based on the TIFF format and includes metadata.
- **CRW/CR2** - Canon Raw (Version 2) format is a proprietary RAW image format used by Canon. It is based on the TIFF format and includes metadata.

PNG - Portable Network Graphics format was designed for transferring images on the internet, not for high-quality print applications. It does not support metadata or non-RGB colour spaces, such as CMYK. It is raster-based and an open format.

GIF - Graphics Interchange Format is now an open format originally developed by CompuServe for internet applications. It is an 8-bit file format that has a reduced colour set, and supports animation, transparency and LZW compression. It also supports a non-rectangular image.

BMP - Bitmap is a very basic format designed by Microsoft that supports data compression, alpha channels, and colour profiles, and allows most applications to open the image and store it using a different format.

PICT - Picture File 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 onsite.

Step 2 - Capture continued.

These systems should be avoided as their future compatibility cannot be guaranteed like a format that is bound by an international standard.

2.2.2. File Sizes

Apart from the quality of the image, the file format chosen in capture has an impact on the file size and its storage requirements, and is a major consideration for any agency when implementing a digital imaging program.

A rough guide to the comparison of file size ranges on a Nikon D800 (36.3 megapixel camera) is below. Variations between camera models and brands will exist due to sensor size, compression options and proprietary technologies but this provides an indicative comparison of the file size ranges achievable on higher-end SLR cameras. File size may also vary within the same format and setting (in brackets), dependent on the subject¹³.

RAW 13.2Mb (DX 12-bit compressed) to 74.4Mb (FX 14-bit uncompressed)

JPEG 700Kb (DX Basic Small) to 16.3Mb (FX Fine Large)

TIFF 12.5Mb (Small) to 108.2Mb (Large)

2.3. Authority to Delete Images

One crucial aspect of the procedure is that none of the Primary or Original Images taken should be deleted without authority. Any deletion of Primary or Original Images, intentionally or accidentally, may be subject of a 'challenge' or legal debate during any prosecution. Where such authority is given, deletions must be recorded in the audit trail or on separate recording systems.

Any authority for in-camera deletion of Primary Images must be specifically referred to in organisational policy or procedures.

2.4. Capture and Storage Media

While the format of Primary Image digital capture media (memory card formats, in-built hard drive), has remained relatively constant, the transition away from optical media as an organisational long-term image storage medium has resulted in a move towards secure server storage as the preferred method of evidentiary image storage for many jurisdictions.

Issues relating to longevity of optical media, migration from obsolete systems and formats, and ease of storage and retrieval, have prompted many agencies to move to server-based systems for their image data storage.

While organisational secure server storage prompts its own set of issues, overall if managed appropriately, it is a more robust storage method to preserve the integrity of images and ensure accessibility well into the future.

The UK Home Office Centre for Applied Science and Technology has published a comprehensive technical document that provides guidance and covers aspects relating to the storage, replay, and disposal of evidential images. This document includes information and references to research on the longevity and storage of optical media as well as providing background on all other storage options¹⁴.

Once images are captured onto any form of re-usable media, they should be transferred from the capture media onto secure media and the Original Image defined as soon as practicable after the capture. This will limit the time and opportunity for accidental or alleged malicious alteration to the images.

Care and Handling of Optical Media

Although no independent body exists to certify the longevity of optical media, high (archival)-quality optical media is recommended for the preservation of Original Images for an extended period of time because of their proven quality, durability, permanence and reliability.

They include Write Once Read Many (WORM) e.g. Compact Disc-Recordable, Digital Versatile Disc (DVD) Recordable and data storage systems. Examining the results of the manufacturer's longevity tests of that media with full disclosure of all factors involved in interpreting those tests is currently the only method of assessing media quality and longevity.

Environmental factors such as light, heat, airborne pollutants, and moisture can damage optical media to the extent that they may become unreadable. Care should be taken before and after recording on optical media to avoid damage and corruption due to external factors. The United States National Institute of Standards and Technology (NIST) have published a care and handling guide of CD's and DVD's for librarians and archivists¹⁵.

13. Nikon D800 User's Manual – 2011.

14. Home Office Scientific Development Branch – 'Storage, Replay and Disposal of Digital Evidential Images' – Publication No. 53/07 – St. Albans: HOSDB-2007.

15. Byers, F. R. – 'Information Technology: Care and Handling of CDs and DVDs – A Guide for Librarians and Archivists' – NIST Special Publication 500-252 – October 2003.

Step 2 - Capture continued.

This care and handling guide outlines recommendations about proper handling of optical media to maximise their useful life, as well as provide an information reference to the structure and longevity of optical media formats.

The storage of optical media in unsatisfactory or unstable environments can significantly reduce the longevity of the media and thus its suitability for use as a long-term storage format. Quoted maximum lifetimes are developed through intensive shortened test periods and under normal usage conditions.

Image Recovery from Storage Media

Image recovery is the process of salvaging digital image data from damaged, failed, deleted, corrupted, formatted, or unreadable storage media when it is unable to be accessed or viewed normally. This could be from corruption, damage, or user error prior to the Primary or Original Image(s) being binary copied across to secure storage media, or might be from third-party storage media where images have been purposefully deleted.

Storage media most commonly encountered in this process include re-usable removable media (e.g. media cards), and non-removable media (e.g. hard disc drives or solid state devices).

Data recovery tasks are commonly the responsibility of organisational Computer Forensic (recovery from media) or Information Technology (recovery from backup) areas. Data recovery tasks should be conducted in accordance with your jurisdictional policies and are likely to involve consultation or referral to staff with the appropriate specialist skills. Agreed and documented procedures should be followed to ensure the integrity of the recovered data and veracity of the methods used in the recovery process. Processes should be documented and an audit trail maintained.

Information Security

It is mandatory requirement of the Australian Government, for all State and Federal Government Agencies to conform to the Australian Government Protective Security Policy Framework (PSPF)¹⁶ and Defence Signals Directorate's (DSD) Australian Government Information Security Manual (ISM)¹⁷, in implementing policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats) which match their value, importance and sensitivity.

The PSPF clearly outlines the requirements for protective security programs to ensure Government agencies can function effectively in the face of disruption while sharing appropriate sensitive information, instil public confidence, safeguard Government resources and information, and safeguard employees and clients of Government from foreseeable risks. It employs a security classification model and is based on principles of accountability, transparency and openness, efficiency, and leadership within the public sector.

2.4.1. Non-reusable Removable Medium

Non-re-usable removable media includes WORM media such as CD-R and DVD-R, or any other media format that is designed to be removed from the capture device and once written, cannot be altered or deleted. Once written to this format, the integrity of the images is managed through the same physical security requirements as any other physical exhibit, but the environmental storage requirements are more demanding.

To allow ease of current and future use of the recordings for investigations and appeals etc, the CD-R/DVD-R should include clearly identified image data files, including all available metadata (time and date should be bound to the relevant images).

Generally WORM media is designed for short-to-medium term storage periods (e.g. 5-10 years), so organisational procedures should be developed to ensure that the media bearing the images or their data does not degrade and that the medium can be replayed in the future when equipment and technology has progressed. A migration strategy for images requiring retention beyond this time frame should be developed.

Agencies need to address specific issues with WORM media, including:

- the compatibility between the original media and evolutionary systems
- verifying the accuracy of the copy
- using the 'finalise' option to ensure compatibility with all systems
- the encoding format or standard
- damage to the media (e.g. ball point or corrosive markers)

16. Australian Government – Attorney-General's Department – Australian Government Protective Security Policy Framework (PSPF) V1. 4 – September 2011.

17. Australian Government – Department of Defence – Defence Signals Directorate (DSD) – Australian Government Information Security Manual (ISM) 2012.

Step 2 - Capture continued.

- the quality and longevity of the media
- physical storage requirements – space, environment, indexing, retrieval.

2.4.2. Re-usable Removable Medium

Re-usable removable media includes Compact Flash, SmartMedia, Memory Stick, Secure Digital, digital video tape, or any other media format that is designed to be removed from the capture device for further use, erased and re-used. For storage or transport of captured images, this also includes CD-RW and DVD-RW formats.

In the case of media cards, once the image files are copied to the removable medium, they may be locked via the menu functions on the camera so that accidental deletion is prevented. Some re-usable removable media can also have a physical protective seal to prevent all the images being deleted accidentally.

This does not prevent the card from being reformatted if the seal is then removed, and it will not protect the images from corruption by external factors e.g. magnetic fields, therefore the transfer to secure storage should occur as soon as practicable after capture.

In the case of tape-based media, copy protection must be activated, if available, prior to any copying or transfer of data from the tape media to WORM or secure digital storage system. Similarly, protection from corruption by external factors should be instigated.

Once the Primary Images are binary transferred from the re-usable medium, they are defined as the Original Image(s). Once the Original Images are verified, the re-usable medium may then be reformatted to remove all of the contents of the media in preparation for re-use. If re-usable, removable media is used to store Primary or Original Images, physical exhibit storage protection (i.e. access control, secure storage), shall be used.

Re-usable, removable media is acceptable for the temporary storage of Primary or Original Images, but care must be taken to avoid loss of data and integrity. This is especially relevant if the practitioner relies on this media e.g. Compact Flash cards, over an extended period of time, as these media formats have a finite life and no indication is usually given of impending failure.

Media cards may have to be formatted in the particular camera prior to use otherwise they may not accept the images to be stored.

A media card cannot always be formatted in one type of camera, placed in another type, and then be guaranteed to work. Likewise, images taken on one make or model of camera may not be visible if the media card is placed in another camera, even though the images exist on the card.

The cost of re-usable media needs to be a consideration when procuring equipment since adequate stocks of replacement and backup media must be readily available for operational work. A typical media card has a finite life and the manufacturer's specification should be used as a guide.

Agencies need to be aware of the security issues surrounding the disposal or distribution to outside agencies, of media cards that have been used for evidential purposes. Unless specifically erased with a forensically-robust process designed to over-write all data on the card, deleted images may still be able to be recovered using data recovery processes. This may permit the recovery of sensitive or confidential images by non-authorized persons.

2.4.3. Non-removable Medium

These are usually in the form of hard disc drives (HDD) or solid-state memory in the capture device, and are mainly used for direct storage of image data

As these are non-removable media within the capture device, the Primary Images must be binary copied to another secure storage medium as soon as practicable after capture.

When the Primary Images have been transferred from the original medium and verified, they are defined as the Original Image(s). The non-removable medium may then, if required, be returned to the owner, erased or reformatted to remove all of the contents of the device in preparation for re-use.

The use of standalone hard drives or PC's as a storage medium have their own set of issues that must be addressed prior to the use of the medium for long-term storage. The finite capacity of a single hard drive, combined with the risk of data loss, will require a backup and data migration strategy. The application of appropriate security measures to the drive and data will also be required.

Where evidential third-party images have been provided to organisations on non-removable media (HDD), they may take considerable time to copy across to WORM media or secure server.

Appropriate data protection measures should be implemented prior to commencing this transfer of data to ensure the integrity of the data is not compromised.

Step 2 - Capture continued.

Advice should be sought from jurisdictional computer forensic practitioners to ensure the appropriate processes are followed when transferring evidential third-party data or images to WORM or secure servers.

2.4.4. Secure Digital Storage System (Secure Server)

These are usually a computing environment, in the form of hard disc drives or arrays, controlled and secured by an Operating System, that are used for the storage of image and other data.

Such systems should employ file redundancy as a protection against data loss in the case of drive failure or corruption, as well as virus and power-out protection.

As this is a computer-based storage system, the Primary Images must be binary copied from another storage medium. When the Primary Images have been transferred from the original medium and verified, they are defined as the Original Image(s). If used, any non-removable medium may then, if required, be returned to the owner, erased or reformatted to remove all of the contents of the device in preparation for re-use.

The design of the evidential server storage should take the following attributes into consideration.

- Minimum retrieval time for images of various ages.
- Retention and management of metadata associated with images.
- Security requirements in line with a security risk assessment and the categorisation (may be mixed), of the data, images or information contained on it (also see 2.4.5. Transmission for references relating to government information security classifications and protection of information assets).
- Long-term ability to view and replay images, especially if the retention period of the data exceeds the safe lifetime of the physical media or longevity of the media format.
- Migration requirements to ensure maximum future compatibility, longevity and access.
- Viability of off-site archiving to provide a further level of data loss protection than single-site storage.

2.4.5. Transmission

The transmission of images over private networks (wired or wireless), or common communication lines may occur in some jurisdictions.

With the possible sensitivity and security classification of this content, consideration must be given to the appropriate use of these networks for this purpose and requirement for the application of security measures to protect the transmitted content.

Agencies must ensure any processes that employ wired or wireless transmission methods have the appropriate level of security applied to them, or the content is controlled to a level appropriate to its security classification, particularly if the internet forms any part of the transmission network.

The Defence Signals Directorate (DSD) is the Commonwealth authority on the security of information.

They work closely with the ICT industry and provide advice and other assistance to federal and state authorities on matters relating to the security and integrity of information.

They also provide government with a comprehensive understanding of sophisticated cyber threats against Australian interests, in addition to coordinating and assisting operational responses to cyber events of national importance across government and systems of national importance.

All state governments should have an information security management framework in place that assists agencies to manage their ICT requirements.

For further information on government system security, ICT system forensics and specialist assistance, vulnerability assessments, education and awareness, and system vulnerability mitigation, refer to the Defence Signals Directorate.

2.4.5.1. Access to Third-Party Networks

Where direct access to third-party networks is granted to investigators, the application of appropriate security processes must be considered and documented. Advice should be sought from jurisdictional computer forensic practitioners to ensure the appropriate processes are followed.

The images retrieved from the third-party network must be binary copied to another storage medium at the earliest opportunity. This will be considered the 'point of transfer' for evidentiary purposes.

When the images have been transferred from the third-party network and verified, they are defined as the Original Image(s) and the responsibility for the storage, handling and continuity of the images is transferred to the organisation.

Step 3 - Use

3.1. Continuity

Continuity of the Original Image must be maintained at all times in accordance with the individual agency's evidence handling procedures. The National Association of Testing Authorities (NATA) or American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) accreditation requirements for Forensic Science Laboratories can be consulted for procedures relating to evidence handling, quality assurance and technical requirements within forensic science laboratories^{18,19}.

All images must have documentation to identify the custody and control of the image from the point of capture to being defined as an Original Image. Once the image has been defined as an Original Image, continuity shall be maintained by records identifying the persons who had access to those Original Images.

There are various media on which images can be captured, both re-usable and non-re-usable. Irrespective of their nature, early transition from 'capture' to 'defining the Original Image' phase is extremely important. The integrity of images needs to be protected at the earliest stage as this reduces the opportunities for challenges in court.

Protection can be achieved by controlling access to the file or media by electronic password and/or controlling the viewing of the images by electronic encryption. The important element of visually recorded evidence is to ensure that the Original Image is preserved, so that the integrity of that image is maintained.

The Original Image should not be subjected to processes that cause permanent alteration. Where processing and/or analysis are required, the relevant procedures should be performed on a Working Image, which in effect can be a verified binary copy of the Original Image.

The Original Image shall be archived (which includes authorised destruction) in compliance with the various state or agency archival legislative requirements or policies.

3.1.1. Verification Techniques

There are several methods for 'electronically' verifying a binary copy of a data file.

These methods include 'hash verification'²⁰ and digital signatures. If a 'hash' function is applied to an image, a unique numerical value is calculated for the whole image. A change in pixel value causes the 'hash' function value to change and when compared to the original, will show variation. This is the basis for most verification software.

Digital signatures allow the source of a digital file to be attributed to an individual when used in conjunction with a hash verification process.

3.1.2. Encryption

The image file is encrypted (i.e. the content is modified or it is contained within an encrypted or protected file container), so that the file cannot be opened except with the correct decryption key or password. This has particular value if images are to be transmitted to or from remote sites. Loss or corruption of either the key or the data may make the files un-recoverable and all encryption methods should be validated prior to use. Encryption can be used with other verification processes.

3.1.3. Watermarking

The image file content is modified to incorporate visibly insignificant information that changes if the file is altered. If a watermarked file is modified, the watermark may then become visible, or introduce other effects such as the locking of the image from viewing. As the watermarking process modifies the Original Image content in order for it to operate, this method is not recommended for evidentiary images.

3.1.4. Handling and Storage Conditions

Images should be protected from accidental deletion by the careful handling of storage or transport media. Physical media should be stored in clean, dry environments and kept away from strong magnetic fields, strong light and chemical contamination. Allowing media to become dirty, scratched, or subjected to other environmental factors such as physical stress, warping or heat, will damage some media such as CD/DVD's and Smart Media²¹.

18. National Association of Testing Authorities, Australia, ISO/IEC 17025 DRAFT Field Application Document – Supplementary Requirements for Accreditation – June 2011.

19. American Society of Crime Laboratory Directors/Laboratory Accreditation Board (International) – Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories (Corresponds to ISO/IEC 17025:2005) – April 2011.

20. ISO 10118:2000 – Information Technology – Security techniques – Hash functions ('hash'). House of Lords, Science and Technology Select committee, Fifth Report entitled 'Digital Images as Evidence' 3 February 1998.

21. Byers, F. R. – 'Information Technology: Care and Handling of CDs and DVDs – A Guide for Librarians and Archivists' – NIST Special Publication 500-252 – October 2003.

Step 3 - Use continued.

3.2. Legal Considerations

Primary Images on a re-usable medium should be binary copied from the re-usable medium onto an archival medium or secure digital storage system as soon as practicable after capture.

If WORM media is chosen, once the images and associated data have been copied onto the media it should be finalised so it cannot be overwritten or altered.

WORM image storage media should be labelled with appropriate case numbers or other information to enable them to be linked to the correct case and facilitate the storage of evidence and eventual disposal. This is particularly important if copies of image files are provided to prosecution or defence counsel.

In evidential value there is no difference between binary copies of the Primary Image, defined as the Original Image/s or Working Copies created by binary copy. This does not remove the necessity to protect the Original Image as an exhibit in case of allegations of inadequate evidence handling procedures or malicious alteration of the image²².

3.3. Use of the Image

The Original Image, once defined, shall be stored securely pending its production at court as an exhibit. An Original Image should not be subjected to analysis unless the veracity or integrity of the Original Image, or subsequent Working Images, cannot be verified.

A Working Copy is a binary copy, usually produced simultaneously, or immediately after the Original Image is defined. A Working Copy may also be produced immediately prior to any image processing being undertaken. The Working Copy, as its name implies, is the version that will be used for investigation, processing, forensic examination and ultimately, presentation in evidence. Where the Working Copy is a binary copy of the Primary Image and is supported by an audit trail it may be produced in evidence as an Original Image.

Generally, offence type and circumstances, jurisdictional records disposal and archiving legislation, sentences, and organisational policy determine the length of time that images must be retained after or pending any court action or determination. The circumstances of their retention should ensure data and image integrity is maintained (See Step 4 – Retention and Disposal).

All use and movement of the Original Image will be logged in an audit trail. Similarly any significant use, processing and distribution of Working Copies should be logged. The aim is to support the presentation of evidence through legal proceedings.

All audit trails should be closed and audit documentation retained by the organisation in compliance with agency or government records retention criteria when the Original Image file is destroyed.

3.4. Defining the Original Image and the Production of Working Copies

The core of the guidelines is the production, definition and storage of the Original Image to protect its integrity.

3.4.1. Defining the Original Image

Original Image files **must** be in the same format as the Primary Image. This is the product of the binary copy process.

In the case of third-party images, the Original Image should be in the same format as received at the point of transfer.

The Original Image should be:

- archived and permissions set to 'read-only'
- stored on labelled medium (with due care to longevity of label and readability of medium)
- stored in a form and manner, with software if required, such that the images may be viewed in the future
- kept in accordance with the organisation's exhibit protocols and evidence control system, with appropriate access control
- used to make subsequent Original Images or Working Copies together with appropriate audit trail entries.

3.4.2. Secure Storage and Documentation of Original Images

Whatever form the Original Image takes, it shall be labelled adequately, protected from physical damage, corruption and contamination and stored securely. Local organisational policies should ensure that the integrity of Original Images is maintained throughout the storage, to include the period before, during and after any court proceedings during which the images may be used.

22. House of Lords, Science and Technology Select Committee, Fifth Report – 'Digital Images as Evidence' – 3 February 1998. – Sect.2.

Step 3 - Use continued.

The Original Image should be labelled, protected and stored in accordance with organisational procedures in order to fulfil statutory requirements.

3.4.2.1. Security

There will be times when the Original Image may need to be viewed and/or a new Working Copy produced. Organisational policy should address the actual process of accessing images stored on computer storage systems or the opening of an exhibit or removal of seals that have been used to protect the images.

3.4.2.2. Storage Environment

The Original Image media should be stored in a clean dry atmosphere with temperature variations limited to normal room temperatures to prevent degradation of the storage medium (see Section 2.4. Capture and Storage Media). For further information regarding the storage of digital images on various media refer to The National Archives of Australia 'Standard for the Physical Storage of Commonwealth Records'²³, the Archives New Zealand 'Guide to Best Practice in Storage'²⁴ and the UK National Archives guide 'Care, Handling & Storage of Removable Media'²⁵.

3.4.2.3. Documentation

Audit trails started at the outset of the image capture process should be completed and documented contemporaneously. A similar process may be necessary for those Working Copies that may be produced as evidence.

The location and any access to or movement of the Original Image should be recorded in the audit trail. Documentation of movement and/or access to files can be on a physical, separate medium such as a tape or disc, or stored electronically on a computer system. Media containing images should be kept in a suitable environment and catalogued for accessibility.

3.4.3. Production of Working Copies

Working Copies are sourced from an Original Image and the continuity of Working Copy images, depending on their purpose, may or may not be maintained. Working Copies produced for the investigation, technical investigation, briefings, circulation, and preparation of evidence can be in many forms, and may not necessarily result in an image of the same format as the Original Image.

They can be:

- tapes or digital media in available-equipment form
- hard-copy stills from still or video cameras
- edited video
- enhanced still or video in electronic or hard-copy format.

The Working Copy files can be copied onto any suitable medium for further processing, retention, or electronic distribution to other parties e.g. investigating officers. Issues of quality control, security and resource management need to be considered and comply with organisational procedures.

Organisations should determine when it is appropriate to include an audit trail and when it is not. If audit trails for Working Copies are maintained, they should be made contemporaneously and relate to the specific situation or image processing circumstance with appropriate levels of detail to ensure repeatability²⁶.

3.5. Digital Image Processes

In practice, when a digital process is applied to a digital image it forms a digital result such as a new image (with enhancements or differences to the original), or a list of extracted data.

Image processing techniques may be considered as subjective or objective.

Subjective image processes are dependent on the skill and experience of the practitioner. They are generally applied to a digital image at the discretion of the practitioner to produce the detail necessary for the required task, e.g. contrast enhancement, colour balancing, etc.

23. The National Archives of Australia – 'Standard for the Physical Storage of Commonwealth Records' – December 2002.

24. Archives New Zealand – 'Guide to Best Practice in Storage' – Recordkeeping Guide G16 – June 2009.

25. The National Archives (UK) – Digital Preservation Guidance Note 3 – 'Care, Handling & Storage of Removable Media' – August 2008 – Issue 2.

26. Scientific Working Group on Imaging Technology (SWGIT) – Section 11 – 'Best Practices for Documenting Image Enhancement' – Version 1.3 2010.01.15.

Step 3 - Use continued.

Objective image processes are applied based on known distortions to the Original Image and cannot be used without concise electronic measurement to improve the Original Image e.g. correcting for image distortion from a camera lens, inverse filtering etc.

Forensic digital image processing tasks should be approached in a methodical and structured manner. All digital image processing tasks should be documented in sufficient detail to allow independent repeatability of the processes employed²⁷.

It is important when referring to such images, to qualify when a Working Image has been subjected to image processing (e.g. processed image, synthesised image etc.).

The principles of digital evidence handling and use of the most appropriate validated processing methods should be understood when applying any digital processing to evidential images.

The three fundamental evidentiary principles of Relevance, Reliability and Sufficiency are important for the evidence to be admissible in a court of law.

The processing methods used should then comply with the requirements for effective digital evidence handling – being Auditability, Repeatability, Reproducibility, and Justifiability²⁸.

The word 'manipulation' should not be used in the forensic field, as it refers to enhancement processing techniques which do not apply to ethical practices within forensic digital imaging processes.

As generally defined; **Manipulate** – handle, manage, or use, especially with skill, in some process of treatment...; manage or influence by artful skill, or deviousness; to adapt or change to suit one's purpose or advantage²⁹. In relation to digital images, use of this term may indicate an implication of purposeful alteration of digital images to produce a desired outcome.

Digital image processes can be broadly grouped into five fundamental categories³⁰:

- image enhancement
- restoration
- analysis

- synthesis
- compression.

Practitioners in this field should be familiar with these principles and their representative operations. This will ensure consistent identification of the processes used and remove ambiguity of processing terms that may otherwise be misinterpreted.

The application of image processing to an Original Image shall not be carried out prior to the image being saved to long-term storage media. Image processing (including minor enhancements), shall only be performed on Original or Working Copies of images once the Original Images have been safeguarded.

3.5.1. Image Enhancement

Image enhancement operations are a subjective operation in most cases designed to improve the qualities of the image or subjects within the image. Common techniques, such as cropping, dodging and burning, brightness and contrast adjustments, and colour balancing that are used to achieve an accurate recording of an incident or object, are standard processing steps.

When the results of these steps are visually verifiable, specific documentation of such steps is not considered mandatory other than a standard operating procedure that describes the typical enhancement processes.

Advanced enhancement processes can include: colour processing, sharpening, spatial filtering, frequency domain filtering, edge enhancement and noise reduction. These processes have been accepted as valid forensic processes by the forensic community and judicial system after wide use and acceptance in the scientific community as long as the following criteria are met³¹:

- the original image is preserved
- processing steps are documented when appropriate (see SWGIT document 'Section 11 - 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

27. Scientific Working Group on Imaging Technology (SWGIT) – Section 12 – 'Best Practices for Forensic Image Analysis' – Version 1.7 2012.06.07

28. ISO/IEC Draft Standard 27037 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence – 2nd Committee Draft 2011-06-16.

29. Macquarie Essential Dictionary 2006.

30. Baxes, Gregory A., Digital Imaging Processing Principles and Applications, John Wiley and Sons, Canada 1994. pp. 20-35.

31. ASTM Standard E2825 – 12, Standard Guide for Forensic Digital Image Processing. ASTM International, West Conshohocken, Pennsylvania, USA, 2012, DOI: 10.1520/E2825-12.

Step 3 - Use continued.

- the end result is presented as a processed or working copy of the image
- the other recommendations in relation to image processing and documentation of image enhancement are followed.

SWGIT provides guidance in documenting image enhancement by categorising images according to their end use, allocating basic and advanced techniques, and recommending levels of documentation according to the processes applied and intended end use of the image³².

There is no requirement to document exploratory enhancement operations or retain test/intermediate images that are not incorporated into the final image. Organisations are advised to consider the SWGIT recommendations when formulating local policy on image enhancement and the documenting of such.

3.5.2. Image Restoration

Image restoration processes are objective processing operations designed to improve the qualities of an image but based on known, measured, or accurately surmised degradation or improvement of the Original Image. They can be conducted in the spatial and/or frequency domains.

There are limitations to the restoration process in that noise in the image may inhibit the process, and where information has been totally lost it cannot be replaced. Often the partial restoration of an image may be a better option where total restoration cannot be achieved. Processes involving image restoration can include photometric correction, geometric correction, inverse filtering, defocusing, warping and blur removal.

3.5.3. Image Analysis

Image analysis operations generally do not produce pictorial results but use the application of image science and domain expertise to examine and interpret the content of an image and/or the image itself. Analysis operations may produce other information, e.g. numerical or graphical data, based on the characteristics of the Original Image.

Processes in this category can include Fast Fourier Transform, spatial measurement and statistics, image segmentation, feature extraction and object classification.

3.5.4. Image Syntheses

Image synthesis operations create images from other images or non-image data. These operations are used when a desired image is either physically impossible or impractical to acquire, or does not exist in physical form at all. It is important to note that the operations in this category are not limited to the qualities of the Original Image.

Processes in this category can include visualisation, composite image (Comfit, FACE), 3D scene construction (virtual reality and animated scenes), and Interactive Crime Scene Recording.

3.5.5. Image Compression

Image compression operations reduce the data content necessary to describe an image. Compression is used to reduce storage and transmission bandwidth requirements. Decompression is required to retrieve or rebuild the compressed data into a usable state. All compression algorithms remove data from the file and some are more effective than others at reconstruction of the data for replay.

Many programs and cameras provide user adjustments in the level of compression to be applied. Some compression formats like JPEG compression can apply increasing levels of compression that result in degradation commensurate with the amount of compression applied and respective effect on the file size, i.e. high amount of compression = high level of degradation + smaller file size.

Any use of compression to Original Images should be validated to ensure the level of compression and end effect on the image is fit for purpose, i.e. the final use of the image should determine the choice of compression.

Compression may be classified as either 'lossless' or 'lossy', and it can be applied either at the time of capture or during processing and saving.

Note: Re-saving a compressed image in an uncompressed format will not reconstitute any lost data.

32. Scientific Working Group on Imaging Technology (SWGIT) – Section 11 – 'Best Practices for Documenting Image Enhancement' – Version 1.3 2010.01.15.

33. Scientific Working Group on Imaging Technology (SWGIT) – Section 19 – 'Issues relating to Digital Image Compression and File Formats' – Version 1.1 2011.01.15..

Step 3 - Use continued.

3.5.5.1. Lossy vs Lossless Compression

Lossless image compression techniques preserve the exact data found in the Original Image. No information is lost but fewer bits are used to store the original data. All of the original data is reconstructed on re-opening the image. Lossless compression commonly has a 2:1 compression ratio, reducing the file size by half.

Operations in this class include run-length encoding and lexicographic encoding, and produce file formats such as TIFF (Lempel-Ziv-Welch) and Targa.

Lossy image compression techniques do not exactly represent the data of the Original Image but strive only to maintain a particular level of subjective image quality. Information is lost or re-organised and cannot be retrieved. Greater compression ratios in excess of 2:1 can be achieved. The JPEG (Joint Photographics Expert Group) compression algorithm is the most common format for still images and uses quantisation encoding to map multiple values to a single replacement value.

Lossy compression introduces artefacts into the image that are not part of the Original Image. These can manifest themselves in an image as blocking, banding in gradients, local colour distortion, and loss of fine detail.

Multiple re-saves of a compressed file may magnify the artefacting but opening, viewing and closing a file without saving will not further compress or degrade the image. Images intended for analysis should not be compressed using a lossy process.

An advanced version of JPEG compression, JPEG2000 uses other mathematical functions (wavelet compression), to achieve higher levels of compression while maintaining image quality. The ultimate aim of all compression schemes is to achieve smaller file sizes with less image degradation.

Other operations in the class of lossy compression include operations such as Fractal, and Wavelet (which can be either lossy or lossless).

3.5.5.2. Cautions with Compression

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 make the image unrecognisable or unusable.

Imaging management programs may alter metadata from the original file.

New algorithms are developed constantly that may not be valid. When implementing a new algorithm ensure a validation process is conducted.

3.6. Presentation in Court

Practitioners may receive images in many file and media formats and from a variety of sources, including images captured by a third party. It is at the discretion of the courts to determine the presentation format of digital images used in civil or criminal proceedings.

Organisations shall provide digital images in a format so as to not compromise the evidential content that will enable presentation and viewing in courtrooms preferably without the need for specialised equipment. If evidence can only be clearly presented when replayed in the digital form, arrangements need to be made for replay and viewing facilities within the courtroom or wherever replay is to take place.

Images may appear different depending on the equipment used. In particular, images viewed on different screens may differ from one another. A calibrated or visually accurate replay facility should be provided wherever possible. Digital images may be required to be printed for presentation in court where no facilities to view various digital formats are available.

In preparing files for court presentation, liaison should take place with the prosecutor to determine:

- the full manifest of evidence being held
- the disclosure schedules for evidence and associated audit and maintenance logs, if required
- explanation of the processes and systems used in the capture and post-processing of the evidence, where relevant
- the preferred format for court presentation
- whether any additional arrangements for replay and viewing are required
- whether conversion or copying to a different format from the Original Image format will significantly reduce the quality of the image by introducing artefacts, affecting the metadata, or distorting the colour, detail or resolution of the image
- the requirement for any additional expert evidence to clarify or rebut any technical issues anticipated in relation to processes or systems used.

Step 4 - Retention & Disposal

4.1. Retain for Statutory Period

A range of factors including state legislation and organisation policy will determine the period of time that evidence must be retained. Images must be stored in a manner that protects their integrity.

Within the limits of known data about the media, organisational procedures should be developed to ensure that the media bearing the images or their data does not degrade and that the medium can be replayed in the future when equipment and/or technology changes³⁴. The longevity of data is of importance when dealing with lengthy judicial processes.

Generally CD-R, DVD-R, digital tapes, etc, are designed for short-to-medium term storage periods – 30 to 100 years under optimum storage conditions but more likely to be in the vicinity of 5-10 years. To ensure the integrity of the data the files should be transferred to new media regularly, or transferred to professionally managed data management archive systems.

The differing perspectives of the organisation's Imaging and IT departments must be taken into account when formulating policy, establishing responsibilities, and defining requirements for forensic image and data management. Imaging departments are concerned with ensuring image integrity and quality is maintained, while IT departments are concerned with security and storage³⁵.

Mutually-agreeable solutions should be provided that allow for the evidential content and integrity of images to be preserved through data migration and archiving processes. These solutions should also consider reverse compatibility and interoperability when data migration or upgrades to hardware or software are planned³⁶.

Australian Standard ISO 15489: Information and documentation - Records management — Part 1: General and Part 2: Guidelines provide information and guidance on the standardisation of records management policies and procedures to ensure that appropriate attention and protection is given to all records, and that the evidence and information they contain can be retrieved more efficiently and effectively, using standard practices and procedures.

4.1.1. Record Storage Considerations

AS ISO 15489.2-2002: Records management - Guidelines deals with points that organisations should consider when planning for a record/image storage capability.

In summary, the section 4.3.7.1. (reproduced below) highlights decisions that must be made when establishing record storage³⁷.

“The decision to capture a record implies an intention to store it. Appropriate storage conditions ensure that records are protected, accessible and managed in a cost-effective manner. The purpose served by the record, its physical form and its use and value will dictate the nature of the storage facility and services required to manage the record for as long as it is needed.

It is important to determine efficient and effective means of maintaining, handling and storing records before the records are created and then to reassess storage arrangements as the records' requirements change. It is also important that storage choices be integrated with the overall records management programme.

Organisations may do this by conducting a risk analysis to choose the physical storage and handling options that are appropriate and feasible for their records. The selection of storage options should take into account access and security requirements and limitations in addition to physical storage conditions. Records that are particularly critical for business continuity may require additional methods of protection and duplication to ensure accessibility in the event of a disaster.

Risk management also involves development of a disaster recovery plan that defines an organised and prioritised response to the disaster, planning for the continuance of regular business operations during the disaster and making appropriate plans for recovery after the disaster.

The following are some of the important factors you should consider when selecting options for storage and handling.

- 1. Volume and growth rate of records.** Projected growth rates may eliminate some storage facilities from consideration if their growth capacity is not sufficient. Similarly, digital storage media for electronic records should be assessed as to storage capacity. The choice of media should be matched to the presumed volume and growth rates of the records.

34. Home Office Scientific Development Branch – 'Storage, Replay and Disposal of Digital Evidential Images' - Publication No. 53/07 – St. Albans: HOSDB-2007.

35. Ibid.

36. Scientific Working Group on Imaging Technology (SWGIT) - Section 15 - Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System - Version 1.1 2012.01.03.

37. Australian Standard ISO 15489.2-2002: Information and documentation – Records Management – 2002.

Step 4 - Retention & Disposal continued.

2. **Use of records.** The various uses of the record will determine the necessary levels of protection against loss or damage. For electronic records, use of reliable systems and media that have greater and more robust life spans will be indicated. In addition, the ease with which backups can be rotated and protected is a key consideration in the selection of storage options for electronic records.
3. **Records security and sensitivity needs.** Some records require limitations on access to them for reasons of confidentiality, proprietary nature of the information or due to legal protections.
4. **Physical characteristics.** These factors will influence records storage: weight, floor space required, need for temperature and humidity controls, and the particular physical preservation requirements of the record's media (for example, paper, digital storage, microform). Records in electronic form may need to be converted or migrated. Digital storage media may need to be refreshed. Records will need to be protected from fire, flood and other risks according to local circumstances.
5. **Records use as reflected in retrieval requirements.** Retrieval of records is a major consideration. Records that are accessed more frequently will require easier access to the storage facility. Electronic records may be stored in a variety of ways that make their retrieval easier or faster.
6. **Relative cost of record storage options.** Cost considerations may affect decisions about outsourcing of physical and/or electronic storage and the media selected for storage of electronic records.
7. **Access needs.** A cost-benefit analysis of on-site storage vs. off-site storage may indicate that multiple storage facilities, system, and/or equipment may be necessary to fully support the organisation's needs."

When organisational procedures and statutory requirements permit the disposal of images, an appropriate entry must be made in the audit trail.

All audit trails (including any audit trails of Working Copies) must be closed and audit documentation retained by the organisation when the Original Image file is destroyed, in compliance with the agency's disposal policies.

4.2. Dispose of Exhibits and Finalise Audit Trail

Each organisation needs to consider mechanisms for the disposal of images once the statutory periods of retention are completed. Prior to the transition to digital imaging, the images were produced as prints from negative film or VHS tapes and the records were physical documents.

An equivalent system for the destruction of all electronic files is required. Consideration needs to be given to a situation where images identified for destruction and images identified for retention reside on the same physical media.

Glossary of Common Terms

Analogue Image	An image created from a signal that is continuously variable in its level and recorded as a variation in some physical property.
Analysis	see: Image Analysis.
Archive	Long-term storage.
Archive Image	An image that is on media suitable for long-term storage.
Artefact	Any information inadvertently introduced by image processing, which is not present on the Original Image.
Audit	A systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives (ISO 8402:1994 – 4.9).
Audit Trail	Step by step documentation to support the continuity and/or integrity of an image.
Authentication	The process of substantiating that an image is an accurate representation of what it purports to be, and that the origin and integrity of the image are proven to be intact and as purported.
Binary Copy	A bit for bit duplication of digital data from one location to another.
Bitmap	1. A method of describing an array or map of bits within a rectangular grid of pixels or dots. 2. Also an image file format (.bmp).
Blu-Ray	Optical disc format using blue-violet laser developed for recording and playback of high-definition video and storing large amounts of data.
Capture	The process of recording an image.
Capture Device	A device used to record image data. Includes flatbed scanners, drum scanners, film scanners, digital cameras and other multi-function devices e.g. mobile phones, PDA's, laptops. They traditionally use a charge-coupled device (CCD) or complementary metal oxide semiconductor (CMOS) image sensor to capture images.
CCTV	Closed Circuit Television.
CD	Compact Disc. A disk to which data can be written but not erased.
CD-R	Compact Disc Recordable. Format that allows CD writers to record data to a blank CD-ROM disc.
CD-ROM	Compact Disc Read-Only Memory. Storage medium using compact discs to store data.
CD-RW	Compact Disc Re-Writeable. Format that allows a recordable compact disc to be re-written several times.
CCD	Charge-Coupled Device. A device, consisting of an array of light sensitive photo cells, that converts light into a corresponding electrical charge.
Colour Management	System ensuring colour uniformity across input and output devices so that the final printed results match the Original Images or images viewed on screen. Colour management can be achieved using hardware, software, or methodology.
Compression	The process of reducing the size of an electronic file, accomplished through software processing. This is used to reduce the required storage space or reduce transmission times.
Digital Image	An image that is captured digitally and stored in a numerical form.
Digital Camera	Any camera system that is capable of converting an analogue image into a digital signal.
Digital Printer	Any printing device that is capable of translating digital data to a hard copy output.
DPI	Dots Per Inch. The unit of measure used to describe the resolution of printers. The measure of distinct pixels that a printer can place either horizontally or vertically in one inch.

Glossary of Common Terms continued.

DVD	Digital Versatile/Video Disc. A data storage media type that has a higher data density than CD and thus a higher capacity.
Dynamic Range	The difference between the highest (highlights) and lowest (shadows) values in an image.
Encryption	Encoding a file through the use of software programs so that others cannot gain access to its content without a password key.
Film	A medium used to record images via a light sensitive emulsion on transparent backing material. Can be negatives (negatives used to produce photographic prints) or positives (slides).
Finalised	The process of closing a CD/DVD burning session to enable the reading of the disc in any standard reader.
Hash Verification	The use of mathematical algorithms to test the validity of an electronic record (data or images), and ascertain whether the record has been altered from its original state.
Hybrid Imaging	Electronic imaging systems that mix traditional silver halide technologies with digital imaging technologies.
Image Analysis	The application of image science and domain expertise to examine and interpret the content of an image and/or the image itself.
Image Output	The means by which an image is presented.
Image Processing	<ol style="list-style-type: none">1. An operation applied to a digital image to form a digital result.2. Adjusting the technical properties of the image and modifying the actual content to improve or change some quality of the image³⁸.
Image Synthesis	Any process that renders an image, using computer graphics techniques, for illustrative purposes (i.e. age progression, facial reconstruction, accident/crime scene reconstruction).
Image Transmission	The act of electronically moving or copying images from one location to another over dedicated networks or communication lines.
Image Verification	The process of confirming the accuracy of an image to its original or confirmation that the application of a tool, technique or procedure performs as expected ³⁹ . See: Hash Verification.
Interpolation	A sampling technique generally used to increase (or decrease) the size of an image file by modifying the number and relationship of pixels in an image and increasing (or decreasing) the apparent resolution of an image. Interpolation examines the existing pixel information and creates additional pixels through image processing.
Lossless Compression	Any compression technique where smaller file sizes are achieved without the loss of Original Image data values. The image can be retrieved in its original form.
Lossy Compression	Any compression technique where image data is irretrievably lost in the compression process. The effects of the compression may or may not be visible, but the original data cannot be restored.
LPI	Lines Per Inch. Measure of halftone screen resolution (offset printing).
Metadata	Image information that is embedded within the electronic image data.
Native File Format	The original format of the Primary Image.
Negative	See: Film.

37. Scientific Working Group on Digital Evidence/Scientific Working Group on Imaging Technology – SWGDE/SWGIT'Digital and Multimedia Evidence Glossary' - Version 2.5 – January 13, 2012.

38. Association of Chief Police Officers (ACPO)/NATIONAL Policing Improvement Agency (NPIA) – 'Practice Advice on Police Use of Digital Images' – 2007.

39. SWGDE/SWGIT – loc. Cit.

Glossary of Common Terms continued.

Open File Format	File format able to be read by a number of other manufacturer's applications.
Optical Media	Data storage media that hold content in digital form e. g. CD or DVD, that are read and written by a laser disc on which digital data may be read with reflected laser light that bounces off the surface of the disc.
Original Image	For film and analogue video, the Primary Image is the Original Image. For digital images, the Original Image is an accurate and complete bit-for-bit copy of the Primary Image, irrespective of media.
Output	See: Image Output.
Pixel	The smallest discrete element of a digital image.
PPI	Pixels Per Inch. The number of pixels per inch in an image – measures image information density, primarily in screen resolution.
Positive	See: Film.
Primary Image	The first instance in which an image is recorded onto any media that is a separate, identifiable object or objects.
Processing	See: Image Processing.
Proprietary File Format	File format native to a specific manufacturer's application and used exclusively by that application.
Quantise	To measure or record data that can only have discrete values.
Raster Image	An image composed of lines of pixels in a grid layout or bitmap.
Resolution	The amount of digital information within a given area. It can refer to the density of pixels in an image or the number of dots per inch a device can achieve.
Scanner	An electronic capture device that creates digital files from original photographs, film or artwork.
Secure Server	A computing environment in the form of hard disc drives or arrays, controlled and secured by an operating system, that are used for the storage of image and other data.
Selective Capture	The decision by an operator to switch on or off a capture device during the capture process (not to be confused with the editing process).
Selective Retrieval	The decision by an operator (made in consultation with an investigating officer), to retrieve identified incidents of interest from a capture system.
Server	The control computer on a local area network (LAN), controlling the software, printer access, and other parts of the network.
Synthesised Image	See: Image Synthesis.
Transmission	See: Image Transmission.
Verification	See: Hash Verification or Image Verification.
Validation	Developmental process used to acquire the necessary information to assess the ability of the imaging system to obtain a reliable result, to determine the conditions under which such results can be obtained, and to determine the limitations of the imaging system.
Watermark	An embedded image, electronic data or function that is included as a security feature or to denote copyright of an image.
Working Copy	See: Working Image.
Working Image	Any image created for, and subjected to image processing.
WORM media	Write Once Read Many. Storage media that can be written to once only, but read or accessed any number of times.

Bibliography

- ALMOND v. THE STATE., 274 Ga. 348, 553 S.E.2.d 803 (Georgia, USA 2001).
- American Society of Crime Laboratory Directors/Laboratory Accreditation Board (International) – Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories (Corresponds to ISO/IEC 17025:2005) – April 2011.
- ASTM Standard E2825 – 12, Standard Guide for Forensic Digital Image Processing. ASTM International, West Conshohocken, Pennsylvania, USA, 2012, DOI: 10.1520/E2825-12.
- Archives New Zealand – 'Guide to Best Practice in Storage' – Recordkeeping Guide G16 - June 2009.
- Association of Chief Police Officers (ACPO) / National Policing Improvement Agency (NPIA) – 'Practice Advice on Police Use of Digital Images' – 2007.
- Australian Government - Attorney-General's Department - Australian Government Protective Security Policy Framework (PSPF)V1. 4 – September 2011.
- Australian Government - Department of Defence - Defence Signals Directorate (DSD) - Australian Government Information Security Manual (ISM) 2012.
- Australian Standard ISO 15489: Records Management - 2002.
- Baxes, Gregory A., Digital Imaging Processing Principles and Applications, John Wiley and Sons, Canada 1994.
- Byers, F. R. – 'Information Technology: Care and Handling of CDs and DVDs – A Guide for Librarians and Archivists' - NIST Special Publication 500-252 – October 2003.
- Home Office Centre for Applied Science and Technology (formerly the Home Office Scientific Development Branch) – 'Digital Imaging Procedure' – Publication No. 58/07 - Version 2.1 November 2007.
- Home Office Centre for Applied Science and Technology (formerly the Home Office Scientific Development Branch) – 'Storage, Replay and Disposal of Digital Evidential Images' – Publication No. 53/07 – St. Albans: HOSDB - 2007.
- House of Lords, Science and Technology Select Committee, Fifth Report entitled 'Digital Images as Evidence' 3 February 1998.
- <http://www.swgit.org>
- ISO/IEC Draft Standard AS 5388 Forensic Analysis.
- ISO/IEC Draft Standard 27037 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence – 2nd Committee Draft 2011-06-16.
- ISO 10118:2000 – Information technology – Security techniques - Hash functions ('hash').
- Macquarie Essential Dictionary 2006.
- National Archives of Australia – 'Standard for the Physical Storage of Commonwealth Records' – December 2002.
- National Archives (UK) – Digital Preservation Guidance Note 3 – 'Care, Handling & Storage of Removable Media' - August 2008 – Issue 2.
- National Association of Testing Authorities, Australia, ISO/IEC 17025 DRAFT Field Application Document - Supplementary Requirements for Accreditation - June 2011.
- Nikon D800 User's Manual - 2011.
- Scientific Working Group on Imaging Technology (SWGIT) Section 1 'Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System' Version 3.3 2010.06.11.
- Scientific Working Group on Imaging Technology (SWGIT) – Section 11 – 'Best Practices for Documenting Image Enhancement' – Version 1.3 2010.01.15.
- Scientific Working Group on Imaging Technology (SWGIT) – Section 12 – 'Best Practices for Forensic Image Analysis' – Version 1.6 2007.01.11.
- Scientific Working Group on Imaging Technology (SWGIT) – Section 13 – 'Best Practices for Maintaining the Integrity of Digital Images and Digital Video' Version 1.1 2012.01.13.
- Scientific Working Group on Imaging Technology (SWGIT) - Section 15 – 'Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System' Version 1.1. 2012.01.13.
- Scientific Working Group on Imaging Technology (SWGIT) - Section 19 – 'Issues relating to Digital Image Compression and File Formats' - Version 1.1 2011.01.15.
- Scientific Working Group on Digital Evidence/Scientific Working Group on Imaging Technology – SWGDE/SWGIT 'Digital and Multimedia Evidence Glossary' – Version 2.5 – January 13, 2012.

Further Reading

7Safe/Association of Chief Police Officers - (ACPO)– 'ACPO Good Practice Guide for Computer-Based Electronic Evidence'.

Appendix A

DIGITAL WORKFLOW PROCESS DIAGRAM

Capture and preservation of digital evidential images

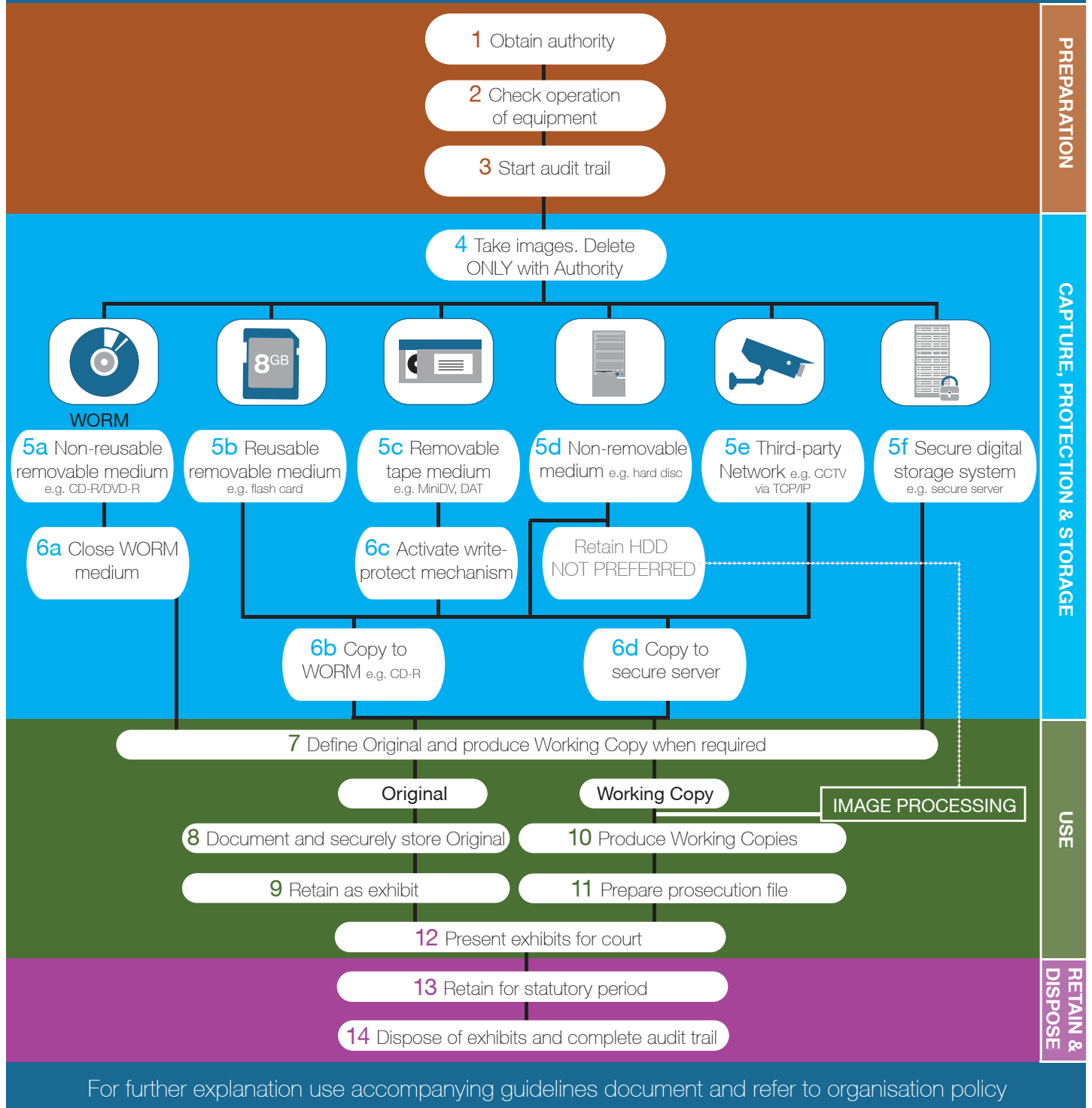


Image Credits

Photos courtesy of:

- New South Wales Police Force
- Queensland Police Service
- South Australia Police
- Tasmania Police
- Victoria Police
- Western Australia Police Public Affairs



Level 6, Tower 3, World Trade Centre
637 Flinders Street, Docklands Victoria 3008
DX 210096 Melbourne

T +61 3 9628 7211
F +61 3 9628 7253
E secretariat.nifs@anzpaa.org.au
W www.anzpaa.org.au