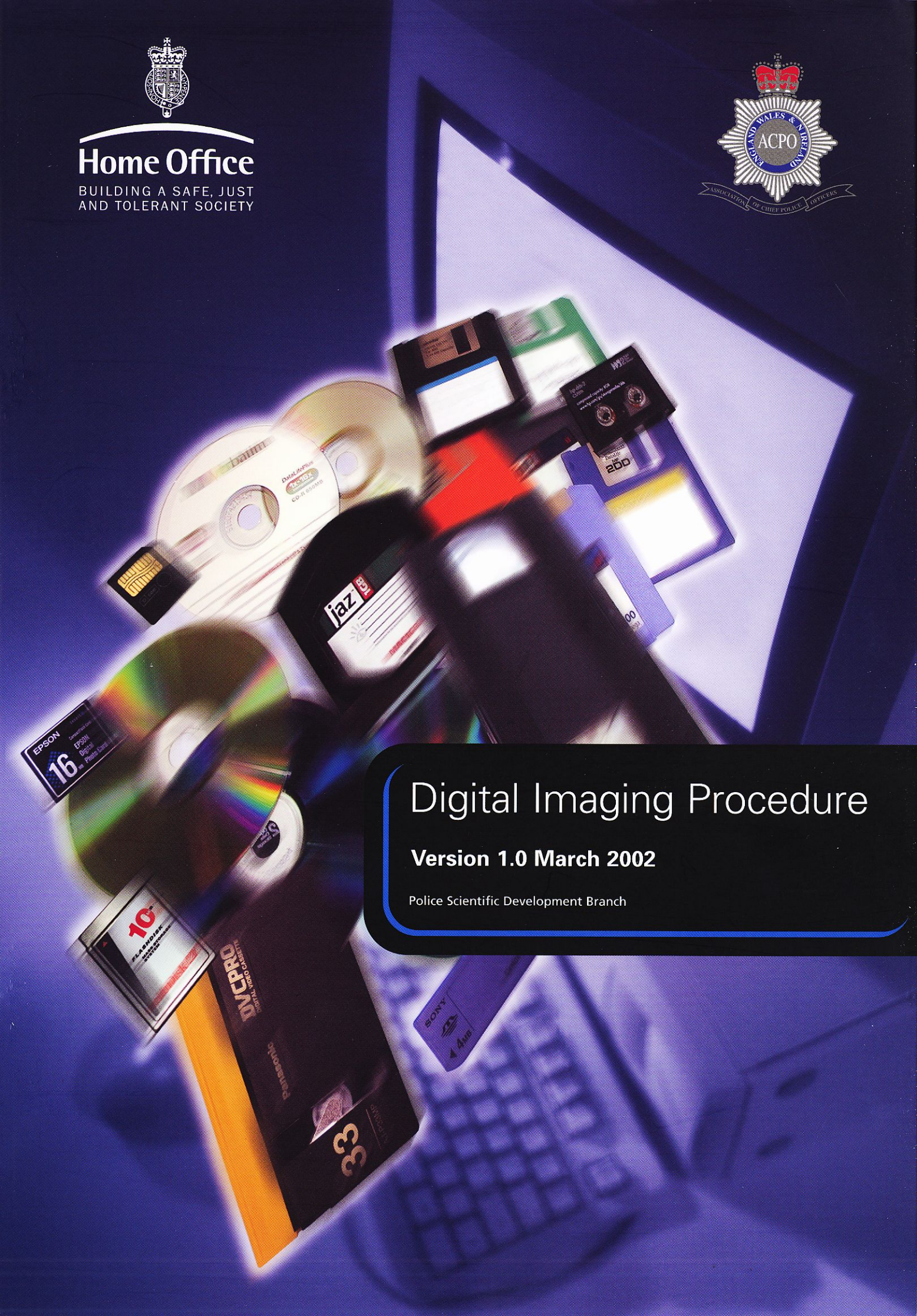

Home Office
BUILDING A SAFE, JUST
AND TOLERANT SOCIETY
ENGLAND WALES & NORTHERN IRELAND
ACPO
ASSOCIATION OF CHIEF POLICE OFFICERS
Digital Imaging Procedure
Version 1.0 March 2002
Police Scientific Development Branch

Acknowledgements

This publication has been produced as a key part of the PSDB project 'Digital Imaging in the Criminal Justice System'.
The editors acknowledge the many organisations and individuals who have contributed through working groups.
These have covered every aspect of policing and included representatives of all UK police forces,
Crown Prosecution Service and other interests within the Home Office and Criminal Justice System.
Industry groups covering the CCTV and the still camera industries have also provided valuable commercial insight.
to the project.
Our thanks to the Project Steering Committee under the Chairmanship of DCC Paul Garvin (Durham Constabulary)

The PSDB editorial team

Jim Aldridge	Project Manager
Neal Skelton	Police Adviser
Leah George	
Sheila Hardwick	
Sheila Slater	
Lauren Doré	

Home Office

BUILDING A SAFE, JUST AND TOLERANT SOCIETY

Digital Imaging Procedure

Version 1.0 March 2002

Police Scientific Development Branch

Contents

Welcome

As a result of the recent development and use of digital image technology it has been necessary to develop a procedure that supports the use of digital images as evidence. The principle purpose of this document is to publish the procedure that details the processes involved in the proper capture and handling of digital images for police applications. This particular document has been produced to enable a wider dissemination of the draft procedure that was included in an earlier and original publication. This document is intended for use by operational, administrative and judicial staff involved throughout all stages of the Criminal Justice System (CJS), and offers guidance on the use of a 'generic' range of camera systems and evidential gathering processes. However, if more detailed information is required 'points of contact' within individual police forces or organisations should be consulted.

The procedure has been developed and agreed by the Police Application Working Groups formed for this project. The procedure mirrors best practice for conventional imaging and other evidence handling requirements. The key is the creation of a Master reference copy, on 'write once read many times' (WORM) media, at the earliest opportunity. It is commonly accepted that digital images can be manipulated to produce a credible product. However, it is very difficult to conceal any manipulation when an analysis of the Master and manipulated files is carried out. More importantly, the procedure reduces the opportunity for malicious manipulation, and enhances the integrity of proper evidential gathering processes.

Digital image technology can and will change the outcome of investigations, as the benefits of transmitting images readily across networks are realised. However, such technology has a price tag; the current quality of telephonically transmitted images is low particularly when transmission time is restricted or networks are busy; in addition many police force networks have neither the capacity nor transmission capabilities to move substantial quantities of image files around their IT infrastructure.

This document contains the findings and recommendations of the Steering Group. We do not present it as a definitive or final report. We appreciate that the full picture of events has yet to emerge. Inquiries currently under way with CJS agency representatives and others will generate further information. We expect that operational implementation and court proceedings will likewise shed greater information. Our own investigations are not closed. However, with the paramount importance of criminal justice very firmly in mind we have decided not to delay production and circulation of this procedure. We fully recognise that as a fuller picture emerges in due time, one or more of the conclusions we now reach, or recommendations we now make, may need amendment.

The information contained in this document has been derived and developed through wide-ranging consultation with practitioners from the Police Service and related CJS organisations, and provides guidance to them. This document represents a body of knowledge drawn from across the range of services for developing the procedure to cope with the introduction of, or transition to, digital technologies and the need to establish an evidential chain. It has not been tested at law but provides a guideline framework; nevertheless I commend it to forces and other organisations for adoption as current 'best practice'.

Paul Garvin
DCC Durham Constabulary

Chair, Steering Group
Digital Imaging in the Criminal Justice System Project

Introduction

This separate publication of the Digital Imaging Proceedure has been produced in response to the demand from the police service for a working version of the procedures with minimal extra information. The data has been extracted from v1.0 of the Digital Imaging in the CJS CD to ease distribution and access. While there are no material changes to the procedures the opportunity has been taken to make some editorial changes and information updates.

It is suggested that these procedures and guidelines are incorporated within force procedures, taking account of any application-specific requirements. Where detailed information is required reference should be made to relevant legislation, Association of Chief Police Officers (ACPO) guidelines and/or individual force procedures.

There are several issues which are not highlighted from the procedure. These are introduced and discussed briefly here to answer frequently asked questions about digital imaging.

What is the 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 presents to the court in support of their case. The images will be presented either as a hard copy or on a screen.

With conventional photography, the negatives are often referred to as the primary or original images and the prints are all made from them. Similarly, with video and analogue recording the first tape is sealed as a Master once the first copy has been made from it. A copy of an analogue tape is always a degraded version because noise is added at each copying. This is compounded by the physical wear and tear of the tape.

However, it is possible to make a bit-for-bit identical copy of a digital image file. In evidential terms there is no distinction of primary or original file because the files are the same and have the same evidential weight. It is not important whether the file is on a stand-alone- or networked-computer, a server, or on any type of storage medium. This assumes the operation of adequate security against unauthorised and unrecorded access.

If no discipline is applied there can be any number of identical files. For evidential purposes it is essential to be able to demonstrate that the images are authentic and have originated from the files captured in the camera and recorded to the first medium.

Digital image files can be used in exactly the same way as conventional photography and video with written audit trails. Electronic audit trails if available can augment the written audit trails.

Digital images should not be thought of as replacements for conventional photographs and videos but alternative technologies. It has to be recognised that digital images are not necessarily better than conventional ones, and that images produced with this new technology may appear different to those we are familiar with. 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 of the image should be fit for the purpose and that the quality is adequate. To this end the use of desktop printers for hard copies of stills and low-resolution video footage must 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.

Is a picture a true representation?

Even in the agreed absence of any deliberate manipulation by anyone, digital images can never be an exact reproduction of the scene. There are two technical points to be appreciated:

- whilst there are digital cameras which have no integral signal processing and the signal is displayed on the screen without processing in the computer, these are used in very specialised applications and are monochrome. Such cameras are used for scientific applications and the Police Scientific Development Branch (PSDB) uses one in its Integrated Rapid Imaging System workstation for fingerprint capture to give extremely high resolution and integrity; and

- most other cameras and all colour cameras use a multitude of complex image processing techniques to combine the signals from the charge-coupled device's (CCD's) pixels into an image of the subject. The image can only ever be an approximation of the subject. Perhaps it is accepted that the output of the camera is somehow 'true' or 'accurate' because the aim of the manufacturer is obviously to produce as 'lifelike' an image as possible within the cost-band of the camera.

However, the image is a representation of the subject in the same way as conventional photographs are. No one questions the chemistry involved in the development of the tiny grains in an emulsion and how the resolution and colour are chemically produced. In video, the images are accepted as being fully electronically processed. Video recordings are admissible as evidence and the digital storage of the images does not alter that.

Compression

There are various compression algorithms used to reduce the amount of data in an image file to reduce both storage capacity and transmission bandwidth requirements. All compression algorithms remove data from the file and some are more effective than others at reconstruction of the data for replay. Generally, the greater the compression ratio, the more seriously affected is the replay.

If an image or video footage is being presented as evidence and illustrates the facts of the offence then it is irrelevant whether the data has been compressed. What is important is the compression algorithm and ratio selected for particular applications.

Some compression algorithms are more suitable for fast movement, some for 'talking heads' scenarios. The compression can produce some artefacts which may mask the information or contaminate it with movement, patterns, outlining, etc. The algorithm must be tested on typical scenes. The image quality must be agreed and performance tests carried out to ensure suitability. Image processing cannot make up for inadequate data. Images should not be excluded because they have been compressed and whilst there may be reasons to prefer some algorithms for reasons of quality, there is no reason to exclude any from evidential material.

File format

Digital data files can have a variety of formats.

The still camera industry is mostly using open formats (TIFF, JPEG) although their highest resolution images are sometimes in their own proprietary format. This means these latter images have to be downloaded in a proprietary software package. The open format allows for the ease of incorporating images into publications, printing and transmitting to others.

Digital handheld video cameras currently record to Mini-DV or Digital8 tape. As the market grows it is likely that more recording media will be introduced. Digital8 camcorders are usually backwards compatible and should be able to play analogue Hi-8 tapes.

The closed circuit television (CCTV) video recorder manufacturers are using a multitude of open, proprietary and mixed compression formats to meet the needs of massive amounts of information versus the cost of storage. Again the format is not relevant to the admission of the evidence, only to the quality.

Preparation

These elements of the procedure 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 authorisations;
- starting an audit trail at the earliest opportunity when it is known that images are to be captured; and
- checking equipment, either routinely or at the commencement of the image capture activity.

Such checks will avoid embarrassment of failure and/or challenges about conformance with an accepted procedure. Digital image capture systems may increasingly be used by non-specialists in operational situations and locations so adherence to an established procedure will assist in safeguarding those captured images.

1 Obtain authority

This instruction applies to all image capturers by virtue of their role or position within the police service. They are empowered to capture images for the purposes of their particular work. Specific roles and responsibilities, for example for a Scenes of Crime Officer or a Collision 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.

However, police forces need to be aware that authorisations do need to be obtained before some images are taken, for example authorisation to permit images to be taken where 'Intrusive Surveillance' is requested under the Regulation of Investigatory Powers Act 2000. That authority must be obtained and recorded within the audit trail of the operation.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

2 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. Currently this will be as a written audit trail, however, as technology improves there may be an increasing availability of 'electronic' audit trails mapping the movement and changes to files on computers.

The procedure relies on the written audit of activities. Where good practice is in place for the collection of evidence, including video and still images, there will be no change in principle. In practice, there probably will be little change in existing procedures with conventional photography except that the operator may receive reusable media to reformat and use; a process familiar to video operators.

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 should include, with the date and time of action:

- details of the case;
- description of shots or footage taken and a log of the media used;
- downloading the data;
- the creation and defining of the Master;
- the storage of the Master;
- any access to the Master;
- any copying that is required to ensure the longevity of the data;
- viewing of the Master;
- use of Master in court; and
- disposal.

The practices may not be familiar where imaging is a new feature of the work and it may be worthwhile to consult the Scientific Support Managers or equivalent adviser.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

3 Check operation of equipment

The correct operation of any equipment is essential to gathering evidence.

In particular it is suggested that checks are made to ensure that:

- operator adjustable settings are made appropriately;
- the time and date settings are correct;
- 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 the equipment manuals.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

Capture

Police-originated images

These steps cover the capture of still or video images onto the chosen medium with due regard for the image quality and integrity of the images.

Third party origination

The procedure diagram should be used to establish the 'point of transfer' at which the responsibility for the handling of third party images transfers to the police. That '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 police audit trail must start from that point. Continuity of image handling should be demonstrated throughout by ensuring that the police audit trail links directly to any audit trail that is available from the third party.

Third party image systems

Town centre CCTV cameras, for example, should follow established and standardised procedures. These systems should allow the police to:

- take evidential recordings away in order to safeguard them;
- replay the recordings in order to view, copy and process them;
- make authentic (not materially different) copies in formats suitable for use by investigators, Crown Prosecution Service (CPS) and the courts; and
- access viewing facilities if the original format recording has to be viewed.

Whichever still or video camera, or format of 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 possibly archived.

4 Take images. Do NOT delete images

Generally digital still or video equipment is used in the same way as conventional cameras. There are two main differences:

- a choice of recorded image quality; and
- the option to delete recorded images.

The image quality setting should be selected appropriate to the operational requirements rather than to minimise the storage capacity. Operators should anticipate their requirements and have sufficient empty storage medium available.

Deletion of images

One crucial aspect of the procedure is that none of the images taken should be deleted without authority. Any deletion of 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 *and be subject to the requirements of the Criminal Procedure & Investigations Act 1996 and Attorney General Guidelines on Disclosure of Evidence.*

Still cameras

On most digital still cameras there is an option to delete image files that have already been saved to the storage medium.

Video – handheld video camcorders

Video recorders are designed to allow deletion by over-recording. Where video footage is recorded directly to tape, images should not be deleted from the recording which will usually become the Master.

CCTV – fixed installations

Where CCTV is recorded directly to hard disc the systems are often designed to over-record automatically after a set period. Before this happens some or all of the images may be transferred onto a back-up tape system. Depending on the design, the back-up may be simultaneous or delayed batch recording. Other systems may not have a back-up system. The standard operating procedures of the system should describe this. When seizing recordings from a hard disc-based system care should be taken when deciding which copy to safeguard, either from the hard disc or back-up tapes. This may need to be done quickly in case the evidence is over-recorded.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

4a Capture still images

Still images can be captured on many different types of cameras using a multitude of memory storage devices/memory cards. The manufacturer's manual should be referred to for instructions on correct use of these types of media.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

4b Capture video images

There are several technologies for capturing video images digitally. Each is illustrated on the procedure:

- magnetic tape – includes digital recording to conventional video tape, special digital video tape and data tape;
- WORM media, for example CD-R and DVD-R;
- reusable, removable, non-tape media, for example discs and memory cards;
- computer hard disc.

Because of the high data rates associated with digital video, the image data is usually compressed in order to:

- reduce the stored data volume;
- reduce the time taken to transmit and/or the transmission channel bandwidth;
- lower the cost of storage media, for example by using low read and write speeds.

Where image sequence(s) have come from a non-removable medium the working copy or copies could be made:

- at the same time as making the Master;
- from the non-removable media after the Master has been made;
- subsequently from copying the Master.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

5a Non-reusable removable medium

Non-reusable removable medium technology includes CDs, DVDs and specially designed WORM devices. They represent the ideal in that once closed the recording on the disc cannot be altered. Other WORM media types may become available.

Video images

To allow ease of current and future use of the recordings for investigations and appeals, etc, the CD/DVD should include:

- the image sequence or sequences clearly identified;
- an easily-read textfile stating any requirements for special hardware or software for replay;
- all associated metadata (time and date should be bound to the relevant images);
- licence-free software enabling the sequences to be viewed correctly;
- licence-free software enabling the sequences to be directly copied;
- clear instructions on making copies of video to VHS detailing changes which may occur to the sequence when viewed side-by-side with the digital image; and
- licence-free software enabling editable copies of the sequences to be made.

Other items that could be included:

- text data about the originating camera or system;
- audit trails;
- authentication or verification software; and
- short test sequence to confirm that the recorded image sequences are being replayed correctly.

Still images

In general, still images are stored in open format and there is no need for viewing software to be stored with images but where proprietary formats are used then the software should be included on the media in line with the information given above for sequences.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

5b Reusable removable medium

These include CompactFlash, SmartMedia, Memory Stick or any other reusable media such as floppy discs. These are currently used for transferring individual frames or sequences of a few images. Evolving technology may allow significant amounts of video footage to be recorded.

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. SmartMedia cards can also have a physical protective seal to prevent all the images being deleted accidentally but this does not prevent the card from being reformatted if the seal is then removed.

Once images are transferred to the Master, the reusable medium is reformatted to remove all of the previous image files in preparation for reuse. This reformatting should be carried out in preparation for the work ahead and the officer should have sufficient empty media for such purposes.

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 card cannot always be formatted in one type of camera, placed in another make and be expected to work.

The cost of reusable media needs to be a consideration when procuring equipment since adequate stocks of replacement media must be readily available for operational work. The initial outlay is high but the cost is insignificant when averaged over the lifetime of the medium. A typical 64Mb media card can be used between 100,000 and 300,000 times. It is likely that the cost of these media will reduce due to market forces whilst the storage capacity is likely to increase.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

5c Removable tape medium

There are several types of tape onto which digital video can be recorded. In the case of a handheld digital camcorder the two most common types at present are MiniDV and Digital8.

These are principally designed for domestic use although their small size, ease of use and cost make them attractive for police applications. The growth of the market may mean that more types will be introduced.

Other formats of digital video tape recording include the professional formats:

- DVCAM and DVCPRO; and
- Digital Betacam.

and those aimed more at the domestic market:

- DVHS; and
- SVHS-D.

Where the video footage has been recorded onto a digital tape in a handheld camcorder then this video tape will usually become the Master.

In the case of CCTV the images may be recorded onto a data tape format. Digital Audio Tape (DAT) is one example. Whilst these tapes are removable it may not be feasible for the police to see the evidence without first transferring the data to another more convenient removable medium.

Where hard disc recording systems use tapes for back-up the recording format may be non-standard to accommodate time lapse and multiplex recordings. These recordings will require special playback and copying facilities.

Analogue VHS copy recordings can usually be made from digital recordings.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

5d Non-removable medium

These are usually in the form of hard disc drives and mainly used for direct storage of video but sometimes for large file-size still images, for example fingerprints.

Because of the high cost and limited capacity of hard drives, images stored on them will usually be erased after a preset time or after the images have been transferred (backed-up) to some other medium for transport or archive. The back-up might be selective, by automatic or manual selection. It may be necessary to bring in specialists to ensure that the data is safeguarded.

Any difficulties with obtaining evidential material should be referred to the force TSU or video units. These systems should be treated as computer systems and reference made to the *ACPO Good Practice Guide for Computer Based Evidence*.

The normal mechanism for erasing data recorded on hard discs is to delete the directory entry only. The computer controlling the hard disc then reallocates the space ready for a fresh recording. The new recording will then erase the previous recording by writing over the top of it and a new directory entry will be made.

If it is essential to erase recordings in any other way then advice should be sought from IT professionals.

When an incident or offence has occurred and there is a requirement to take information from the hard disc as evidence:

- check whether the required data has already been copied to a back-up medium;
- check that what is needed is not being over-recorded while arrangements to save the data are being made;
- stop the recording process if necessary to preserve the data – this may put the system out of action until the data transfer can be completed;
- be prepared to seize the hard disc if necessary;
- transfer the data in a file format with software for accurate replay that can be used by the police; and
- transfer to a recording medium suitable for play by the police.

If it is necessary to seize more than a small amount of data this may take a considerable time and require many units of back-up media (for example CDs).

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

Protection

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

Accidental alteration or erasure could be detected by noting image number sequences and prevented by:

- designating the image file as read only;
- activating the mechanical write protect mechanism; and
- transferring to WORM media.

Protection can also be achieved by controlling access to the file or media by electronic password and/or controlling the viewing of the images by electronic encryption.

With CD media, still image files can be protected using camera functions. If an image is 'deleted', it is only the address in the directory which is deleted. The image is simply not accessible therefore the capacity on the disc is not increased and this shows that an image has been 'deleted'.

The procedure does not rely on any form of 'electronic' protection but neither does it preclude its use. There are several methods for 'electronically' authenticating an image file. Once applied, any change to the pixel values will be detected although the nature and location of the changes may not be indicated.

Authentication techniques

If a 'hash' function is applied to an image a unique numerical value is calculated for the whole image. The number is embedded in the metadata of the image file. A change in pixel value causes the 'hash' function value to change. This is the basis for most 'authentication' software.

Watermarking

Watermarking describes visibly insignificant changes made to the pixel values to incorporate information which changes if the image file is altered. The watermark may then become visible on the picture or even make it unreadable.

The primary use for watermarking is to protect the intellectual property rights of the photographer or film maker. Its use may lead to claims that the image is not authentic because the pixels have been changed.

Encryption

The image file is encrypted so that the file cannot be opened except with the correct decryption key. 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 unrecoverable.

The use of electronic protection is mandatory in the digital imaging used for roadside cameras where there is unattended capture, the image is the only evidence of an offence having taken place and the images are transmitted from the roadside to a central facility. Refer to Home Office and ACPO Traffic, *Outline Requirements and Specification for Automated Traffic Enforcement Systems*, S Lewis, PSDB 3/96.

Handling

Images should also be protected from accidental deletion by the careful handling of media. Media should be stored in clean, dry environments and kept away from strong magnetic fields, strong light and chemical contamination.

Some media such as CDs and SmartMedia will be damaged by allowing to become dirty or scratched.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

6a Close WORM medium

WORM medium must be closed to prevent any of the image data files being subsequently changed and further data being written to the disc.

Compact disc recordable (CD-R) must be 'finalised' or 'closed' in the camera or CD-writer before the disc is removed otherwise the images may not be viewable on a computer.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

6b Copy to WORM

Images on reusable medium should be copied from the initial storage medium in the original format onto a WORM medium, for example CD-R. Once the images and associated data have been copied onto the CD-R and it has been closed, they cannot be overwritten or altered.

The preparation of the WORM copy should be carried out as soon as possible after the capture to reduce the time and opportunity for the accidental or malicious alteration to images.

In most cases WORM copies should relate to the relevant prosecution in case papers to facilitate the storage, retrieval and eventual disposal of case material.

In evidential value there is no difference between bit-for-bit copies on the Master, Working Copies and the images on the storage medium as bit-for-bit copies are regarded as having equal evidential weight. This does not remove the necessity to protect the Master as an exhibit in case of the event of challenges to evidence handling procedures or image manipulation.

Video sequences may be downloaded to WORM, for example DVD or CD for convenience of storage and replaying.

The software required for viewing proprietary formats must be available otherwise the images will be inaccessible. It is advisable to copy any replay software onto each WORM recording to assist with the correct viewing of the files.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

6c Activate write-protect mechanism

As soon as a tape containing evidence has been removed from its recording device, the write-protect mechanism should be activated where available. On a video tape this is usually in the form of a tab with two positions or a tab that can be broken out preventing the recorder from switching to the record mode. For instance Mini-DV cassettes have a switch which can be in one of two positions marked REC and SAVE. Placing the tab in the SAVE position guards the tape from being accidentally erased by over-recording but will not prevent damage or erasure due to careless handling, proximity to magnetic fields or poor storage conditions, etc.

Product manuals/instructions should be referred to along with relevant legislation, ACPO guidelines and/or individual force procedures.

6d Download to removable medium

Transferring images from digital systems may not always be straightforward. In some cases the images may have been backed-up onto a removable medium such as digital tape which can be seized or copied by the police in the same way as conventional tapes.

Substantial costs may be incurred if the expensive media used on some of these systems is seized as evidence and replaced with new on each occasion. However, the understanding that bit-for-bit copies have equivalent evidential value allows the copying onto cheaper alternatives and the reuse of the original.

Unfortunately problems have been encountered because some systems:

- have no output other than a screen and possibly a printer;
- have no connections to allow external devices for copying to be used;
- use encryption therefore decryption keys are required for the viewing;
- produce image or file formats that are incompatible with police facilities; and
- cannot download images and record new data simultaneously.

Any difficulties with obtaining evidential material should be referred to the force Technical Support Unit (TSU) or video units. These systems should be treated as computer systems and reference made to the *ACPO Good Practice Guide for Computer Based Evidence*.

Large non-video images may be stored directly to a hard drive, for example the images of fingerprints captured with large array, high bit still cameras. Ideally such images will be simultaneously stored locally, as the Master in full resolution, and transferred directly to a centralised computerised identification system.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

Use

The Master is defined and will be documented as such. It will then be stored securely pending its production at court as an exhibit. Only in the event of any doubt being cast upon the integrity of the images will the Master be viewed.

A Working Copy is usually produced simultaneously, or immediately after the Master is defined. The Working Copy, as its name implies, is the version that will be used for investigation and to assist in the preparation of the prosecution file.

Where it is believed that images relate to any crime or incident pending civil or criminal proceedings they must be retained ensuring compliance with the Criminal Procedure and Investigations Act 1996, the Data Protection Act 1998 and other relevant legislation. Offence type and sentences determine the length of time that they must be retained on conviction. The circumstances of their retention should ensure that their integrity is maintained in the event of appeals against sentence, civil claims and/or retrials.

All use and movement of the Master will be logged in the audit trail. Similarly any significant use, enhancement 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 when the image files and any analogue copies are destroyed.

Where detailed information is required reference should be made to the relevant legislation, ACPO guidelines and/or individual force procedures.

7 Define Master and produce Working Copy

The core of the procedure is the production, definition and storage of a Master which can be examined if required by the court to confirm the authenticity of the images. The Master should be:

- on removable medium;
- labelled (with due care to longevity of label and readability of medium);
- stored in a form and manner, with software if required, so that the images may be viewed in the future;
- kept in accordance with exhibit protocol; and
- never used, except to make further copies together with appropriate audit trail, or by order of the court to establish authenticity.

Force policies should be developed to cater for such eventualities.

Image files should be in the same format as:

- first captured on medium in/or attached to camera; and
- as recorded after transmission from camera.

Still images

The first WORM copy is usually the Master.

Video images

Video is often recorded to tape and existing best practice procedures for tape define the original tape recording as the Master. In other cases a Master needs to be defined. When video is recorded to a hard disc it needs to be transferred to a removable medium. This can be done by:

- making two copies simultaneously and defining one as the Master and the other the Working Copy;
- making two copies, consecutively, from the hard disc and defining one as the Master and the other the Working Copy; and
- making one copy, the Master, and making a Working Copy from that Master.

Where video footage is stored on the hard disc of a computer with no effective means of downloading the data the computer may need to be seized in order to safeguard the data until arrangements for download can be made. Any difficulties with obtaining evidential

material should be referred to the force TSU or video units. These systems should be treated as computer systems and reference made to the *ACPO Good Practice Guide for Computer Based Evidence*.

Produce Working Copies

Working Copies can be in many forms. The files can be copied onto any suitable medium or e-mailed for circulation to the investigating officers, CPS or defence lawyers. Issues of quality control, security and resource management need to be considered.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

8 Document and secure storage of Master

The Master is defined, will be documented as such and retained in secure storage as an exhibit for court purposes.

Local force policies need to be established to ensure that the integrity of the images is maintained throughout the storage, to include the period before, during and after any court proceedings during which the images might be used.

There will be times when the Master may need to be viewed and/or a fresh Working Copy produced. Force policy needs to be developed concerning the actual process of opening the exhibit and any seal that has been used to protect the images. At the present this storage is on a physical, separate piece of medium such as a tape or disc. If electronic storage on a computer system is proposed then procedures will need to be reviewed. The location and any access to the Master or movement of the Master should be recorded in the audit trail.

Whatever form the Master takes it is essential to label it adequately, protect it from physical damage and contamination and store it securely. Whether this is a room or locked cabinet it should have a clean dry atmosphere with temperature variations limited to normal room temperatures to prevent condensation. Where long-term storage is needed expert advice should be sought.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

9 Retain as exhibit

The Master should be labelled, protected and stored in accordance with force procedures in order to fulfill statutory requirements.

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. Retention of images should conform to the Data Protection Act 1998 and the Criminal Procedure and Investigations Act 1996. Media containing images should be kept in a suitable environment and catalogued for accessibility.

Where detailed information is required reference should be made to the relevant legislation, ACPO guidelines and/or individual force procedures.

10 Produce Working Copies

Once the Master is defined and stored, all use of images should be from a Working Copy. Bit-for-bit copies should be used for further reproduction of additional Working Copies or where precise detailed analysis is to be carried out or when images are to be enhanced.

The Master should never be used, except to produce additional Working Copies when no other Working Copies are available to copy, or by order of the court to establish authenticity. Force procedures will need to detail the circumstances and the relevant processes involved. All actions will need to be entered in the audit trail.

Working Copies produced for the investigation, technical investigation, briefings, circulation, and preparation of prosecution evidence and defence can be in any of the forms described:

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

At present the CPS and courts are normally only equipped to handle hard copy stills and VHS format video recordings.

The copying and distribution of Working Copies should be in accordance with force procedures with appropriate audit trails as required.

The production of copies on media such as CDs, DV tapes and prints requires specialist equipment. The copying of files within a computer is easy and so needs to be disciplined to prevent unnecessary files being produced.

Management of images will be subject to the Attorney General 'Disclosure of Evidence' guidelines and any processing or enhancements of the Working Copy must be documented. These will also be subject of 'Disclosure of Evidence' guidelines also, and must be documented. Working Copies will be physical items, however, in the future, these may be 'electronic' files as technology, storage, transfer and access control improve.

It is not suggested that all Working Copies should require individual audit trails, however, certain application specific situations and/or enhancement processes may require audit trails to be maintained for additional Working Copies. Where this happens these need to commence and records kept contemporaneously.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

11 Prepare prosecution file

Administration of Justice Departments or their equivalents may receive images in many file and media formats and from a variety of sources – both police and third party originated.

The appearance of images may differ depending on the means of display. Administration of Justice Departments should define how the image is to be viewed to ensure evidentially significant material is visible.

The introduction of different formats for digital recording makes it unlikely that Administration of Justice Departments will have all the facilities to view digital video evidence. Currently the CPS and the majority of courts only have facilities for VHS replay so for ease of use digital video is usually converted to analogue VHS. Some courts may be equipped with digital facilities during 2002 but not all formats will be accommodated. The CPS is being equipped to handle CD format in the medium term and may need to rely on police facilities for the time being for other formats.

Similarly some digital still images may have to be printed for the time being as the facilities to view various formats may not be available.

If evidence can only be appreciated when replayed in the digital form then arrangements need to be made for replay and viewing facilities.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

12 Present exhibits for court

Currently the preferred format in UK courts for presenting still images is hard copy and full frame rate VHS format for video footage. In most circumstances this will not affect the content or quality of the images submitted for evidential purposes in prosecution cases. However, all images should be presented so that the evidential content is not compromised. If there is pertinent material that can only be seen when the image is viewed in digital form then provision should be made for appropriate playback equipment to be provided in court. It is generally accepted that the police should provide this equipment.

The report: *Criminal Justice: The Way Ahead* includes a commitment that all the main criminal justice organisations (police, probation, CPS, courts and prisons) will be able to exchange case file information electronically by 2005. In the meantime pilot studies are being conducted in selected courtrooms of electronic equipment and if successful it is feasible that individual courts will be equipped before the target date.

The specifications for the equipment will allow the display of digital images from a number of media.

It should be understood that images may look different depending on the equipment used. In particular, images viewed on different screens may differ from one another. An accurate replay facility should be provided wherever possible.

Concerning the presentation of images in court, PSDB is

- liaising with the Home Office, Justice and Victims Unit; Criminal Justice System Information Technology Unit; Court Service Division, and the Lord Chancellor's Department;
- representing the police requirements to these bodies; and
- advising the police service on the selection of compatible hardware, software and media to facilitate effective case handling.

Where detailed information is required reference should be made to relevant legislation, ACPO guidelines and/or individual force procedures.

13 Retain for statutory period

Sentences determine the period of time that evidence must be retained, and images must be stored in a manner that their integrity is maintained pending appeals, retrials and/or civil claims.

Force 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 developed. This is of extreme importance for appeals in cases where long custodial sentences have been imposed.

CDs, DVDs, digital tapes, etc, are designed for short-to-medium term storage periods. To ensure the integrity of the data the files need to be transferred to new media regularly, possibly as often as every five years, or transferred to professionally managed data management archive systems.

Where detailed information is required reference should be made to the relevant legislation, ACPO guidelines and/or individual force procedures.

14 Dispose of exhibits and complete audit trail

Each force needs to consider mechanisms for the disposal of images once the statutory periods of retention are completed. Currently, the images are produced as prints from negative film or VHS tapes, and the records are paper documents but an equivalent system for the destruction of all electronic files will be required.

All copies of images should be disposed of when they have no further evidential value, in accordance with force procedures and statutory requirements, and an appropriate entry made in the audit trail.

Where Working Copies have audit trails these should also be closed.

Where detailed information is required reference should be made to the relevant legislation, ACPO guidelines and/or individual force procedures.

Capture and preservation of evidential images from digital still and video recordings.

Preparation

1 Obtain authority

2 Start audit trail

3 Check operation of equipment

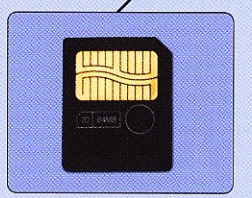
Capture

4 Take images. Do NOT delete images

4a *Capture still images*

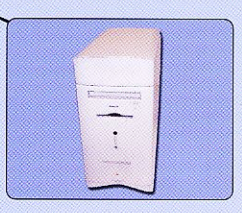
4b *Capture video images*

5a Non-reusable removable medium e.g. CD-R



5b Reusable removable medium e.g. flash card

5c Removable tape medium e.g. MiniDV, DAT



5d Non-removable medium e.g. hard disc

Protection

6b Copy to WORM e.g. CD-R

6d Download to removable medium **5a, 5b, 5c**

6a Close WORM medium

6c Activate write-protect mechanism

Use

7 Define Master and produce Working Copy

Master

Working Copy

8 Document and secure storage of Master

10 Produce Working Copies

9 Retain as exhibit

11 Prepare prosecution file

12 Present exhibits for court

13 Retain for statutory period

14 Dispose of exhibits and complete audit trail

For further explanation use accompanying notes and refer to force policy

Police Scientific Development Branch

Sandridge, St Albans, Hertfordshire AL4 9HQ
digital_imaging@homeoffice.gsi.gov.uk

ISBN 1840 82 7343