Home Office

Scientific
Development Branch

Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0

Publication No. 66/08

N Cohen
K MacLennan-Brown

Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0

N Cohen
K MacLennan-Brown

Publication No. 66/08

2.0

Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0

N Cohen
K MacLennan-Brown

Publication No. 66/08

2.0

ISBN: 978-1-84726-832-7

FIRST PUBLISHED 2006

REVISED AUGUST 2008

Home Office Scientific Development Branch
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051
Fax: +44 (0)1727 816233
E-mail: hosdb@homeoffice.gsi.gov.uk
Website: http://science.homeoffice.gov.uk/hosdb/

Foreword

CCTV is increasingly commonplace in our society and has proved to be an invaluable tool in the investigation of crime ranging from petty theft to terrorism. However, the proliferation of different CCTV systems, together with the transition from analogue to digital recording technology has required a change in practices for the recovery and processing of video evidence. This is particularly evident in the increased level of technical knowledge required for retrieval of video evidence from the diverse range of digital CCTV systems in use.

It is therefore vital that the police have clear procedures and guidance to follow when retrieving video and processing images from digital CCTV systems, and maintain the integrity of the evidence.

We are confident that this procedure provides a sound framework within which to effectively gather and present evidence from digital CCTV systems.

Alan Pratt

Alan Pratt

Director

HOSDB

Gerrard.

Graeme Gerrard

DCC Cheshire Constabulary

Chair ACPO CCTV/Video Working Group

Contents

Figures

Acknowledgments

We are grateful for the assistance of the following organisations during the preparation of this document:

Metropolitan Police Video Laboratory

ACPO CCTV/Video Working Group

Video Evidence Analysis Users' Group

National High-Tech Crime Unit

Crown Prosecution Service

Management Summary

This document has been designed to provide a procedure and supporting guidance to police technical staff wishing to identify the most appropriate method for retrieving video from any digital CCTV system. It also provides guidance on methods for the production of working copies in non-native file formats, where this is necessary to facilitate further processing or replay in court.

The first part of the document covers methods for the retrieval of video in its native file format from digital CCTV systems, leading to the creation of a master copy of the evidence. It presents a checklist of actions that should be followed when retrieving data to ensure that all relevant information is captured and evidential integrity is maintained. It also contains a flowchart to help the user select the most appropriate retrieval method to use for any given CCTV system. Explanatory notes are provided for each option and guidance given for assessing the practicality and suitability of each technique.

The second part of the document covers the production of working copies, specifically where this involves a conversion between video formats. The various routes available for format conversion are presented in a chart, which also shows the different options available for final storage of the working copy. Information is given as to the suitability of each conversion technique and storage medium, so that appropriate choices can be made to best minimise the potential degradation in image quality.

This edition of the document has been updated to take account of the revised guidance on capture and handling of digital images for police applications given in the HOSDB publication 58/07 *Digital Imaging Procedure v2.1* and the *NPIA Practice Advice on Police Use of Digital Images 2007.*

1 Introduction

Digital CCTV installations vary greatly in terms of the recording methods used and picture export facilities provided. There are many manufacturers operating in the CCTV marketplace and each offers a slightly different solution with different capabilities and functionality. This makes the task of retrieving and replaying data increasingly complex for police technical staff, who have to develop a familiarity with a broad range of systems and export technologies.

This publication is designed to guide technical staff in the selection of methods for effective retrieval and subsequent processing of digital CCTV. It is essential that the selected method allows evidential integrity to be maintained and that maximum picture information is retained.

The document is divided into two parts, each of which consists of a procedure, flow chart and associated guidance notes. The first part covers the retrieval of video data in its native file format from digital CCTV systems, leading to the creation of a master copy of the evidence. The second part focuses on methods for the creation of a working copy of the data, particularly where a format conversion is required. This is usually because the native file format does not permit the processing or editing that is required to analyse or present the video evidence.

2 Retrieval of Video Evidence

2.1 Introduction

This procedure is designed to enable police technical staff to select the most appropriate method for retrieving recorded video from a digital CCTV system. It is aimed at video content investigators, rather than computer systems analysts, and is intended to facilitate extraction of video sequences (and associated metadata, e.g. time and date) from digital video recording equipment, rather than to forensically examine the entire system. There are key differences between most CCTV and computer forensic investigations; e.g. it is often the case with CCTV that the owner/operator of the system is not a suspect and the recording is not seized under PACE.

Forensic computer investigators are advised to refer to the relevant ACPO guidelines for computer based evidence:

http://www.acpo.police.uk/policies.asp

Having received a request for assistance, a technician is required to assess the request against the functionality provided by the CCTV system. The selection process is based around a flow chart (see section 2.4), which seeks to address four fundamental questions:

1. Is the request reasonable?

2. What export methods are available?

3. Is the method practical?

4. Does the method lead to the creation of an evidential master copy?

Priority is given to techniques that permit video data to be extracted in the native file format and satisfy the requirements for master copies as described in HOSDB publication 58/07 *Digital Imaging Procedure v2.1.* The preference for extraction of data in the native file format is to assist with maintaining evidential integrity and retaining picture quality.

Options such as recording to videotape (analogue or digital) via an analogue video output or scan conversion of the VGA signal from the CCTV system are not recommended for the creation of a master copy; these do not result in exact copies of the original picture data, potentially resulting in a reduction in picture quality (i.e. loss of information) and evidential weight. In circumstances where it is not possible or practical to extract the data in the native format, alternative methods (such as recording to videotape and scan conversion) may be justifiable, but their use should be approved by the SIO or nominated representative.

2.2 Download Checklist

The list of actions below should be followed when retrieving video data to ensure that all relevant video and information about the system is gathered. This is essential to permit future viewing and maintain evidential integrity, whilst minimising any potential disruption to the premises where the CCTV system is installed.

(a) **Contemporaneous notes** should be kept, detailing the course of action taken, to provide an audit trail.

(b) **Note the make and model** of the CCTV system, and the number of cameras. Take photographs of the system if possible, particularly if the recorder is unfamiliar or the manufacturer uncertain.

(c) **Note the basic system settings** (e.g. current record settings and display settings), so that if changes have to be made to facilitate the retrieval, it is then possible to return the system to its original state. (Taking photographs of the system can assist, particularly if cable connections are changed during retrieval).

(d) **Time check** – compare the time displayed by the CCTV system with that given by the speaking clock. Any error between the system time and real time should be recorded in the audit trail and compensated for when conducting the retrieval. This will ensure that the correct section of data is copied.

(e) **Determine time period required** in conjunction with SIO, if this has not already been specified in the request.

(f) **Determine which camera views are required**, and whether they can be retrieved separately. It is good practice to draw a plan of the camera views to facilitate further decision making processes. Depending on the nature of the incident, there might, for example, be a requirement to retrieve all cameras with external views. Some systems permit video from individual cameras to be downloaded, but some do not, in which case data from all cameras will need to be taken. The decision taken and the reasons for it should be documented in the audit trail.

(g) **Replay Data.** Check that the requested video exists on the system.

(h) **Check storage / overwrite time** – to determine how long the relevant data will be retained on the system. This is particularly important if the retrieval cannot be carried out immediately, or needs to be prioritised against other tasks. A maximum time period can then be determined within which the retrieval must be carried out before data is lost.

(i) **Obtain system password,** if necessary. Be aware that the standard user password may provide only limited functionality and an administrator password may be necessary in order to enable data retrieval.

(j) **The recording should not be stopped during the retrieval process** unless (i) this is an unavoidable feature of the system or (ii) there is an immediate risk that important data will be overwritten before it can be retrieved.

(k) **Protect data**. Some systems allow write-protecting a selected video sequence to prevent it from being overwritten before it can be retrieved; however, it should not be assumed that this facility will be present.

(l) **Confirm that the data can be retrieved in its native file format**. It is preferable to extract the CCTV sequence in its native format in order to maintain image quality and provide best evidence, even where this file format is proprietary to the CCTV manufacturer. Some systems may provide an option to write the sequence to AVI file, which may seem to be an advantage in that the video will be replayable using standard software; however the generation of the AVI file often requires the video to be recompressed, resulting in a loss of quality, and so this method should be avoided. Metadata such as time and date information may also be lost, along with any stored bookmarks. (Note that when copying data files manually via Windows Explorer, the metadata and index files may be stored in a separate directory to the video files.)

(m) **Replay software**. Is the data format proprietary? If so, it is necessary to retrieve a copy of the replay software alongside the data. Some CCTV systems provide this facility, but others do not, and the software has to be obtained separately, e.g. from the manufacturer's website. It should be established that the facility exists to replay the data before leaving the scene and allowing the system recording to be overwritten.

(n) **Confirm success of retrieval.** The retrieved data should be checked before leaving the scene (or immediately on returning to the lab) to confirm that (i) the retrieval process was successful and (ii) that any associated replay software functions correctly. This check should be done on a machine other than the original recorder to ensure that replay is not device specific.

(o) **Restart the CCTV system** (if necessary). Ensure that video is being recorded onto the system as well as being displayed as a live view. Confirm in the presence of the owner/operator that it is operating as it was originally and obtain a signature.

(p) **Complete evidence sheet.** The following information should be included with the evidence to assist the investigator with subsequent replay and analysis:

- Make and model (important when trying to identify suitable replay software or hardware)
- Error in display time and date
- Time period covered by download
- Map of camera locations and coverage
- Include replay software if available

(q) **Media handling.** Media should be packaged to minimise the likelihood of damage in transit. CDs and DVDs should be kept in individual cases rather than on a spindle, flash cards should be stored in their original protective packaging and particular care should be taken to protect hard drives removed from systems. These should preferably be stored in individual boxes with foam inserts. All evidence should be bagged and labelled according to established procedures, and the label on the box should contain sufficient information to link it to the evidence sheet that contains the full details. Also, if there are multiple discs, the labels should identify the correct order for replay.

2.3 Equipment

A range of equipment will be needed to enable a technician to be able to deal with the variety of systems that are likely to be encountered. The following is a suggested list of equipment that should permit the most common systems to be dealt with and retrieval methods to be undertaken:

- Appropriate forms for documenting the audit trail
- Toolkit (plus torch, mirror, pens and labels for cable marking)
- Blank media, e.g. CD-R, DVD-R, DVD+R, DVD-RAM
- External CD/DVD writer
- USB hard drives (capacity 200GB+)
- Replacement hard disk drives (range of sizes 80-400GB)
- Laptop, with USB and network connectivity. (A selection of proprietary replay software could be installed, to enable the downloaded data to be checked).
- Memory card reader
- Network cables (crossover and patch)
- Extension cables (e.g. 4-way power distribution cables)
- Digital camera – to record cabling, connections and settings before disconnecting system
- Analogue/digital video monitor
- Replacement (loan) DVR units

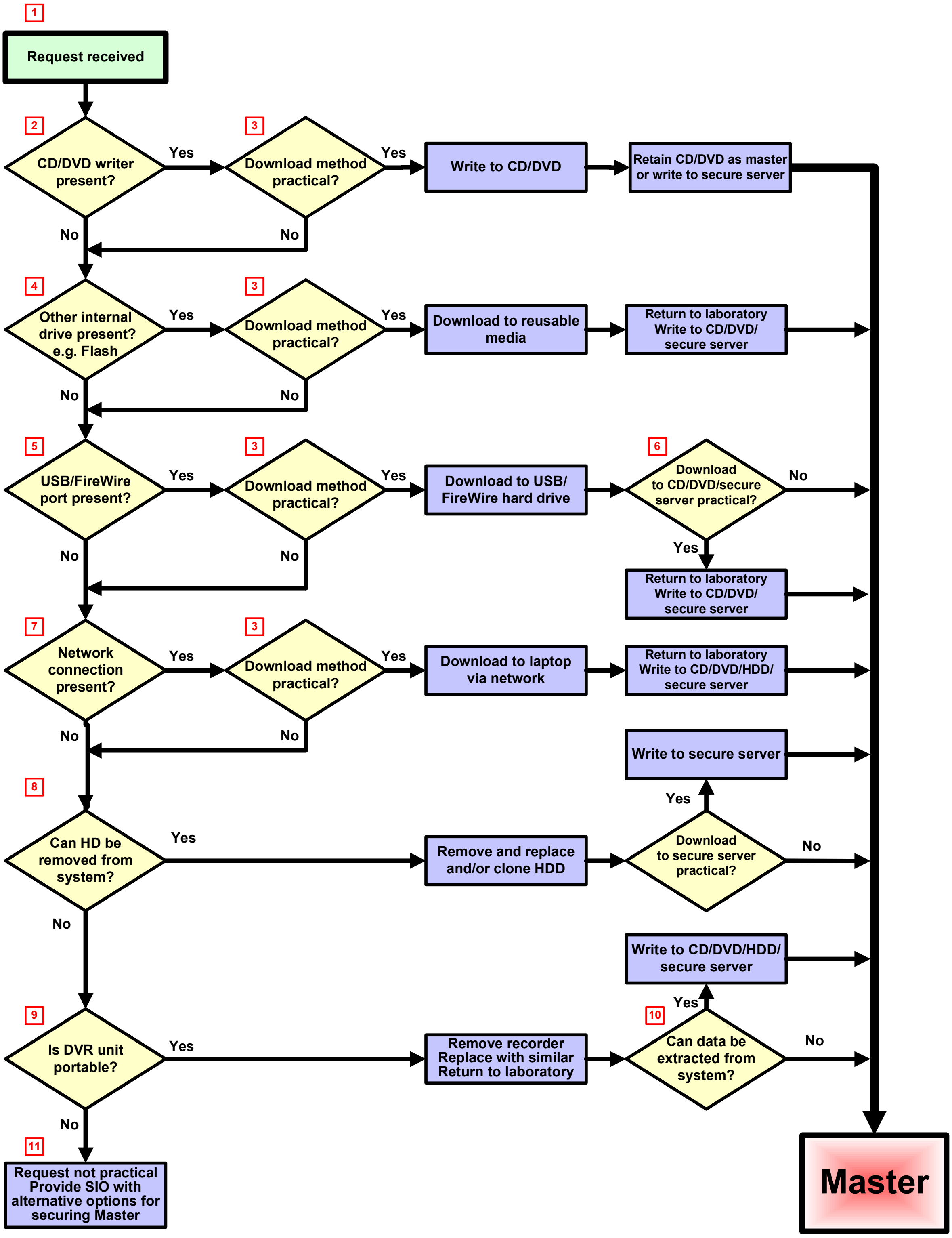
2.4 Selecting Method for Video Retrieval from Digital CCTV Systems

The chart presents the various options available for downloading data in its native file format, starting with those methods that are the most straightforward to implement and will minimise potential disruption to the CCTV installation. Explanatory notes are provided for each option and guidance given for assessing the practicality and suitability of each technique.

Most of the techniques described are relatively straightforward and could be undertaken by a competent and experienced user of computers and/or DVRs. The part of the procedure that deals with removal and replacement of hard drives, however, requires a higher level of technical competence and familiarisation with other issues, such as health and safety. It is not recommended that this be undertaken by staff without the appropriate knowledge. More in depth information and guidance can be found in chapter 3 of HOSDB publication 20/02 *Video Processing and Analysis Manual*.

Each technique results in the production of a master copy, although some master copies may be the result of a copy of a copy to a write-protected medium. This is acceptable under best evidence rules, but the weight a court will place on the evidence will be determined by how it has been handled. It is therefore essential that ‘chain-of-evidence’ is maintained and documented.

PROCEDURE FOR SELECTING METHOD FOR VIDEO RETRIEVAL FROM DIGITAL CCTV SYSTEMS


1
Request received
2
CD/DVD writer present?
Yes
No
3
Download method practical?
Yes
No
Write to CD/DVD
Retain CD/DVD as master or write to secure server
4
Other internal drive present? e.g. Flash
Yes
No
3
Download method practical?
Yes
No
Download to reusable media
Return to laboratory Write to CD/DVD/ secure server
5
USB/FireWire port present?
Yes
No
3
Download method practical?
Yes
No
Download to USB/ FireWire hard drive
6
Download to CD/DVD/secure server practical?
No
Yes
Return to laboratory Write to CD/DVD/ secure server
7
Network connection present?
Yes
No
3
Download method practical?
Yes
No
Download to laptop via network
Return to laboratory Write to CD/DVD/HDD/ secure server
Write to secure server
Yes
8
Can HD be removed from system?
Yes
No
Remove and replace and/or clone HDD
Download to secure server practical?
No
Write to CD/DVD/HDD/ secure server
Yes
9
Is DVR unit portable?
Yes
No
Remove recorder Replace with similar Return to laboratory
10
Can data be extracted from system?
No
11
Request not practical Provide SIO with alternative options for securing Master
Master

2.5 Explanatory Notes for Chart

1 Request received

An initial assessment should be made to determine whether the request seems reasonable, i.e. is the volume of data asked for appropriate to the nature of the incident being investigated. If a general request has been submitted for all available video from a site, then an attempt should be made, in conjunction with the SIO, to narrow down the period of interest before starting the download.

It should also be confirmed that alternative routes for obtaining the data have already been explored before requesting technical support, i.e. has the owner been asked to undertake the download, or is help available from the installer or manufacturer of the CCTV system?

2 CD/DVD writer present?

Many digital CCTV systems have a built-in CD/DVD writer for downloading data, in which case there should be an option within the CCTV software to facilitate the back-up of the selected video sequences (in the native file format). There may also be the option to include the replay software on the disc along with the data. Write-once discs should be used, even if the intention is to use the CD/DVD as a transport medium and store the master evidence on a secure server – please see the glossary for a definition of secure server.

3 Download method practical?

The practicality of a particular export method is determined by the resource (e.g. staff hours), cost (e.g. media/hardware), time (e.g. data transfer time), and quality implications for the volume of data to be retrieved. Before an export method is chosen it should be assessed against each of the criteria to determine whether it is appropriate.

For example:

- An internal CD writer may be present, but long sequences of video from multiple cameras may require an impractically large number of CDs for storage. The download process may also take several hours to complete. Archiving to a USB hard drive or via a network connection may be a more practical option than the use of a CD writer, as no regular changing of discs is required during the download process.
- It may be more time-efficient to replace the hard drives or remove the DVR and undertake the download in the laboratory, although this may be more expensive in replacement hardware/media cost.

To assess whether downloading to CD is time-efficient for large downloads, the time taken to create one CD should be checked, and the percentage of the required video that fits on this disc noted. From this information, the total number of discs required and the total archiving time can be calculated.

For other download methods such as USB hard drive and network, the file transfer rate should be monitored and the total transfer time estimated.

4 Other internal drive present?

If the facility exists to back-up data to memory cards/sticks such as compact flash, this may be utilised for extracting short video sequences. The storage capacity for compact flash is approximately the same as a CD (albeit increasing with time) and therefore similar problems may be encountered if archiving large volumes of data.

Memory cards are not the ideal medium for storing master copies as cards are more expensive than CDs and less stable, which could cause difficulties in accessing data for playback. Thus if a memory card is used to extract data from a CCTV recorder, it is recommended that this is used as a transport medium only, and the data files are then copied to the master medium e.g. CD/DVD or direct to secure server.

5 USB or FireWire[1] port present?

It may be possible to connect a USB (or FireWire) hard drive to the CCTV system for data retrieval. Archiving data to USB hard drive may be the preferred option in several scenarios, for example:

- For downloading smaller quantities of data where there is no other easy option (e.g. CD writer). The USB drive in this case is just a transport medium, and the data may then be copied to optical disc or secure server later, at the lab, to make the master copy.
- For downloading large quantities of data, where it is quicker or more practical than writing to several CDs. When copying large quantities of data, it may be more efficient to exit the CCTV system software (which may be possible on a Windows PC-based system) and copy the required files directly using Windows Explorer. This may also be necessary if the CCTV software does not recognise the addition of the USB device and consequently offers no suitable menu option. (For older operating systems it may be necessary to install a USB driver for the device being attached.)

6 Download to CD/DVD/Secure server practical?

Where a USB hard drive has been used to download the data at the premises, either for convenience or out of necessity, it is strongly recommended that a master copy is then made from this on a secure server or on a write once medium such as optical disc. Copying the data is more cost-effective than retaining the USB drive permanently as evidence and also the lifespan of stored hard drives is currently unknown. The USB drive can then be wiped using a suitable protocol and reused.

If very large volumes of data have been extracted (several tens of GB), it may be deemed impractical to archive to CD/DVD, in which case if a secure server is not available a decision could be made to retain the USB drive as the master. This should then be stored and handled accordingly.

[1] FireWire is Apple’s brand name and iLink is Sony’s brand name for the IEEE 1394 interface created by Apple.

7 Network connection present?

Where CCTV software provides for network connectivity, a laptop could be linked to the system using a crossover cable and IP address specified to create a local network and allow transfer of data.

DVR-based systems often require remote viewer software to first be installed on the laptop, although this can sometimes be downloaded directly from the DVR via a web browser. For a PC-based CCTV system it may be possible to exit from the CCTV software and create a connection to a laptop via Windows. Video data can then be downloaded to the hard drive on the laptop or to a USB hard drive connected to it, and a master copy then created from this on an appropriate medium.

Some systems may provide a remote network connection for off-site monitoring or data download. Before using this facility the network speed should be checked and it should be confirmed that the transmitted video is of the same quality as that which is stored locally. More detail on network connections can be found in chapter 3 of the HOSDB publication 20/02 *Video Processing and Analysis Manual.*

8 Can hard drive be removed from system?

The direct replacement of hard drives can be a quick method for extracting large volumes of data from a system. The recorder may be equipped with a removable hard drive in a caddy, or the casing of the unit may need to be opened and the storage drives extracted and replaced. Depending on the system, the hard drive could be replaced with a blank (the quickest option) or a clone could be taken and the original drive replaced. Once the drive has been removed or cloned either the data can be written to a secure server or the drive can be retained. Retaining the hard drive is not recommended for the reasons given in point 6.

There are several risks with this approach, however, and it should only be attempted with caution, and by an experienced engineer.

- It should first be clearly established that it will be possible to replay the data from this hard drive in the laboratory. A DVR may have a fully removable hard drive for storing data, but this drive may not be compatible with anything other than the original recorder.
- Where the casing of the DVR needs to be removed to access the drive, care must be taken to follow appropriate health and safety procedures, particularly with regard to potential exposure to electricity. The possibility of invalidating the manufacturer's warranty or damaging the storage media by undertaking this procedure also needs to be considered.
- A hard drive removed from a standalone DVR may not be in Windows compatible format, and therefore the data files will not be accessible via connection to a PC. It may be possible to replay the data from the hard drive by fitting it to another similar CCTV recorder (e.g. if there is a unit in stock from a previous job), but in the worst case scenario the hard drive will be locked to a specific CCTV recorder and will only play on that one machine.
- The data may appear to be contained on a removable hard drive in a caddy which is thus easy to extract. However, there may be a second

hidden data drive within the DVR, which is only accessible by removing the case.

- The DVR may not recognise any replacement drive fitted, even a clone of the original.

9 Is DVR unit portable?

In circumstances where all other retrieval options have been rejected as either impractical or impossible then the decision may be made to remove the recording unit itself. This assumes that it is physically possible to do so, and that removal is justified by the significance of the incident being investigated. For example, where the volume of data required is very large, it may be time-efficient to temporarily remove the recorder and undertake the download in the lab, rather than wait at the site for a download to complete. Alternatively, for some systems, there may no straightforward method for extracting the required video (e.g. no CD writer or data output ports and a hard drive that cannot be replayed in another machine). In this scenario, it may be necessary to take the recorder and retain the unit as evidence.

If the DVR is removed, the implications (legal, insurance, etc.) of this should be considered, and a decision taken as to whether a replacement recorder should be provided, or other arrangements made in order to maintain security at the premises.

10 Can data be extracted from system?

If a DVR unit has been removed from the premises because it was more time efficient to do so than to wait while the video was downloaded, then the data should be transferred to a suitable master format on returning to the lab, and the DVR then returned. For those systems where it is impossible to extract the data in a replayable format, the DVR unit itself may need to be retained as evidence.

11 Request not practical. Refer back to SIO

Where it is impractical or not economically viable to download the required data and the CCTV recorder is too large or complex to be removed, the request should be referred back to the SIO for a policy decision.

The SIO should be presented with alternative options to enable data to be retrieved. For example:

- It may be possible to reduce the volume of data required by reconsidering the time period of interest or the number of cameras needed. By reducing the volume of data, it may then be possible to use some of the methods that had previously been rejected.

- It may at this stage be necessary to consider using other techniques such as recording of the system analogue output, or scan conversion, which do not provide exact copies of the original data, but which may be the only practical way of retrieving video evidence from the system. This is discussed in more detail in section 3.

3 Production of Working Copies

3.1 Introduction

It is always preferable to create working copies in the native file format to maintain image quality; however where the file format does not permit further processing, or where editing or replay is hindered by proprietary software then it may be necessary to convert the video to a more accessible format.

This section gives guidance on the production of copies in non-native file format. In some circumstances, it may also be necessary to follow this procedure if it has not been possible to create a master copy of the CCTV sequence from the original recorder in its native file format, as discussed in note 11 of section 2.5.

The options available will depend on the form in which the master copy is stored, i.e. whether it is to be replayed directly from a DVR, is in a proprietary video file on CD/DVD for replay on a PC or stored on a secure server. The option selected may also depend on the desired output format for the working copy, particularly whether there is a requirement to view the video on a PC or on a standalone player (such as a DVCPro/DVD/VHS machine).

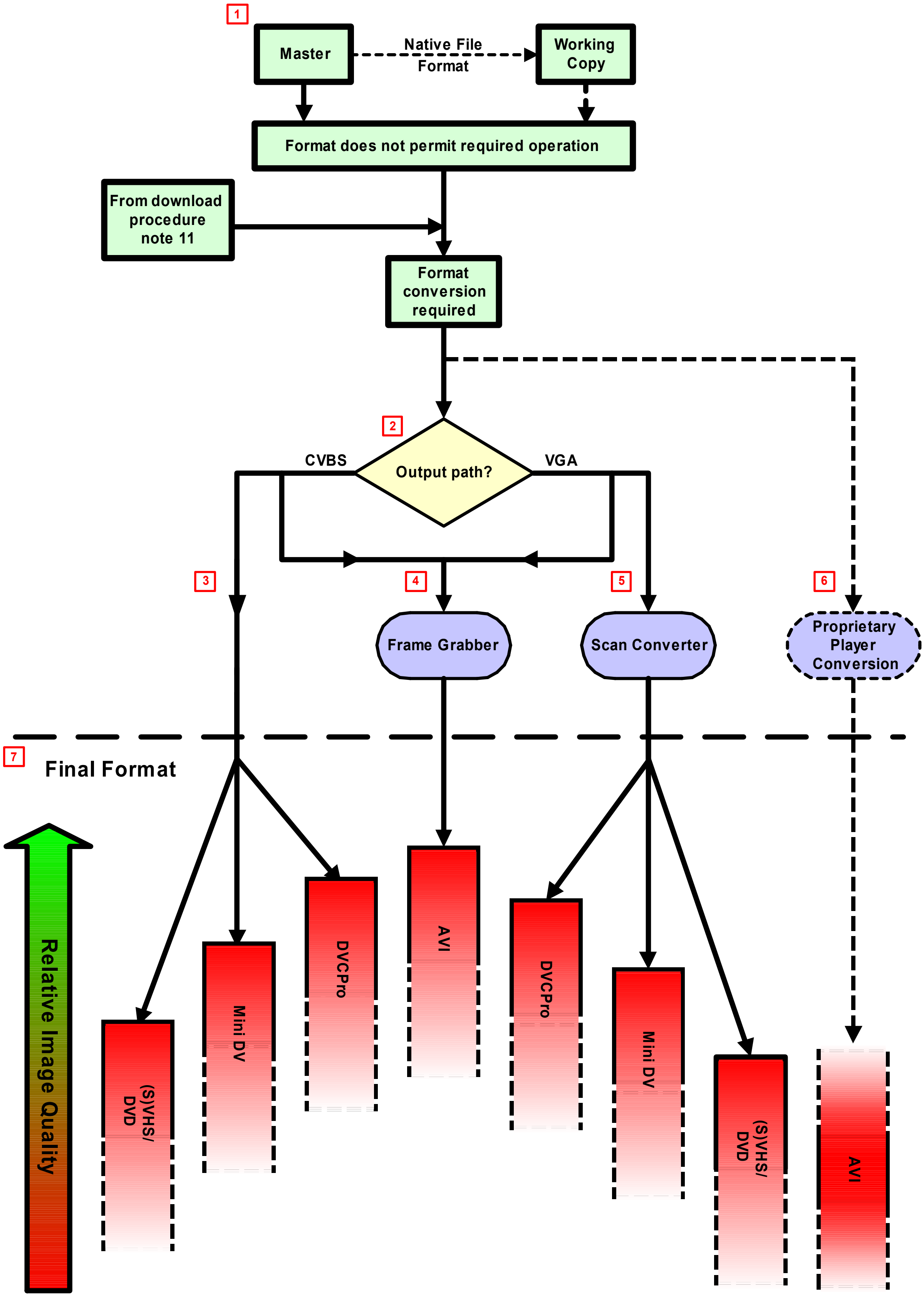
The various routes available for format conversion are presented in the chart opposite, which also shows the different options available for final storage of the working copy. These storage options are ranked on the chart to provide an indication of the relative image quality that can be expected after conversion when viewing the product.

The boxes on the chart have been left open-ended and marked with dotted lines to signify that whilst it is possible to measure the 'best' image quality possible from each technique, the actual image quality may be poorer. Several factors can affect this, the most significant of which is the quality of the equipment used. (In other words, a cheap scan converter recording to a worn VHS machine will be substantially worse than a good scan converter recording to a new VHS machine. However, the same scan converter will usually produce a better result if recording to DVCPro than VHS.)

The AVI box (on the proprietary player conversion route) is open ended at both top and bottom, as the final image quality is highly variable and is dependent on how the AVI is generated. Also on the chart, DVD refers to the video DVD format that can be played directly on a domestic standalone player.

Further details on the conversion routes are provided in the guidance notes. Information is given as to the suitability of each conversion technique and storage medium, so that appropriate choices can be made to best minimise the potential degradation in image quality.

PROCEDURE FOR PRODUCTION OF WORKING COPIES



3.2 Explanatory Notes for Chart

1 Master in native format

Best evidence and image quality is provided by a master in the native file format. To best retain image quality the working copy should also be in the native file format, made either from the master or at the same time as it. Producing a first working copy in the native file format will also reduce the need to access the sealed master.

This format, however, may need proprietary software or hardware for replay and this may not provide the required functionality to enable editing or processing to be undertaken. If this is the case a format conversion will be required.

2 Output path?

There are three possible routes for format conversion. Firstly it might be possible to output via an analogue CVBS connection, such as the PAL monitor output from a DVR. Secondly it may be possible to connect via a VGA cable, either from the DVR or from the replay PC. Thirdly there is direct conversion of the data using functionality that may be available from within the proprietary software.

3 Analogue (CVBS) Output from DVR

If the DVR unit itself has been retained as evidence, or a DVR is being used to replay a hard drive that was retrieved as evidence, it may be possible to create a working copy of the required video sequence by recording directly from the analogue PAL output. The DVR should be set to give a single camera output rather than a multiple camera view to maximise the image quality. Time and date information should also be displayed within the picture if possible.

4 Frame Grabber

Frame grabbers are used to capture a video signal, such as the CVBS output from a DVR, and then output this to a PC either as a bitmap image or a movie file, which can then be edited. Some frame grabbers additionally have the capability to take in a VGA signal. They can thus be used to capture the CCTV displayed within the proprietary software replay window on a PC (including the time and date information if this is shown separately) and save it in a format that is compatible with video processing software.

- High quality frame grabbers such as those associated with professional non-linear editors can produce working copies with little loss in image quality compared with the original. However, this assumes that the images are saved in an uncompressed format. The major drawback to this method is the resulting file size, which can be up to 1GB for a 15 second video sequence from a VGA frame grabber. Compression would significantly reduce this file size, but at the expense of picture quality, particularly as a result of concatenation effects.

- A high specification VGA frame grabber card and PC would be required to provide full-frame capture at a high refresh rate, at a total cost of approximately £7000[2].
- Software based screen capture programmes are a possible alternative to a hardware based VGA capture card, as they can be used to capture a window and save it to AVI. However, they rely solely on the processing power of the PC, which is generally insufficient to reliably acquire all the frames of moving video from the proprietary software replay window.

5 Scan Converter

A scan converter is a hardware device that is used to transform a computer graphics (VGA) signal to a PAL video signal which can then be recorded directly onto videotape or video DVD. It could be used to record the CCTV signal directly from a DVR if the DVR has a VGA monitor output. Alternatively it could be used to capture the video played with proprietary replay software on a PC and then output this to tape or video DVD. Most scan converters allow the user to define a window on the VGA screen to be captured, although only the most expensive provide the flexibility to select a window to precisely match that of the proprietary player.

As well as scan converters, some PC graphics cards are available which have an analogue output and enable a user-defined window on the VGA screen to be converted to PAL format. They can thus be used as a direct replacement for a traditional scan converter to capture the output from a proprietary player.

Many scan converters exist, ranging in price from approximately £300 - £8000[2] Since scan converters operate by digitising a VGA signal, re-sampling and processing before converting to analogue video format, some loss in image quality is inevitable.

- The degree of quality loss is highly dependent on the make of scan converter used, and the image quality correlates with the price of the scan converter.
- The best scan converters produce images that are almost as good as those that would be obtained by taking the analogue feed directly from the DVR.
- Graphics cards with an analogue output can produce an image quality which, while not as good as the most expensive scan converters, is significantly better than those scan converters in the equivalent price bracket (approximately £400[2].

A more detailed description of the operation and performance of scan converters is given in the HOSDB publications 20/02 (Video Processing and Analysis Training Reference Manual) and 24/05 (Scan Converters and Retrieving Digital CCTV Images).

[2] 2008 prices

6 Proprietary Player Conversion

Some CCTV replay software provides the facility to directly convert the video sequence from the manufacturer's proprietary format to a standard AVI file. If it were possible to undertake this process without changing the original image data, then this route would be the most suitable for retaining image quality. However, in practice this process often involves re-compression of the video, which could result in severe image quality degradation. Alternatively, the software may save the file in an uncompressed format, but this leads to the creation of extremely large files. The precise conversion process used varies, and is usually not described in the software user guide provided by the manufacturer. Because of this uncertainty, this technique should usually be avoided.

7 Final Format

Several types of storage media exist onto which the working copy can be recorded, including DVCPro, MiniDV, (S)VHS and video DVD, as well as PC-based (AVI) formats.

- The use of a frame grabber to create a PC-based file in uncompressed AVI format is the route which best maintains image quality.
- Where there is a choice available between CVBS and VGA outputs, it is usually preferable to record to tape from the CVBS output than to record to tape via a scan converter from the VGA output.
- Of the tape-based media, the use of DVCPro usually results in the most faithful reproduction of the image, although for low quality images, there may be little to visually differentiate the performance of the DVCPro, MiniDV, (S)VHS and DVD recorders.
- There is little difference in quality between recording onto SVHS and a high quality VHS recorder, given the typical quality of most CCTV.
- There is minimal difference in image quality between recording onto (S)VHS and video DVD.

Glossary

ACPO

Association of Chief Police Officers

AVI

Audio Video Interleave. A multimedia file format for storing sound and moving pictures developed by Microsoft. An AVI file can use different codecs and formats so there is no set format for an AVI file, unlike VCD video, for example, video which sets a standard for resolution, bitrates, and codecs used. The term AVI is used in this report to denote any general widely-recognised movie file format.

CCTV

Closed Circuit Television. System where video is transmitted for display or capture without being broadcast. Commonly used for surveillance and security applications

CD

Compact Disc. Digital optical recording medium. Available both in write-once (CD-R) and re-writable (CD-RW) form. CD-R versions are preferred in order to ensure evidential integrity.

CVBS

Chroma, Video, Blanking and Syncs. A single channel colour analogue signal also known as composite video

DVCPro

Professional digital video tape format introduced by Panasonic

DVD (DVD+/-R, +/-RW, RAM)

Digital Versatile Disc. Optical recording medium similar to a compact disc, but with closer track and pit spacing allowing for greater storage capacity (up to 4.7GB for a single layer DVD disc).
Like CD, DVD is available in write-once and re-writable forms; however, two competing and incompatible standards exist, denoted by either '+' or '-' labelling. Many modern DVD drives can read both formats. An additional, less common re-writable form exists, known as DVD-RAM, which can be written to in a similar way as a computer hard disk drive.

DV / Mini DV

Digital Video. The DV format is an international digital video recording standard for consumer use. MiniDV uses a smaller form factor cassette tape than standard DV and is commonly found in camcorders in the consumer market.

DVR

Digital Video Recorder. A generic term for a device that is similar to a videocassette recorder but records video data in digital form on a hard drive as opposed to a videocassette tape.

FireWire

FireWire is Apple's brand name for the IEEE1394 High Performance Serial Bus for connecting devices to a computer, developed by Apple Computers. It allows data transfer at speeds of up to either 400 megabits per second or 800 megabits per second, depending on the version. The same protocol is called iLink by Sony.

GB

Gigabyte. A unit of information or storage equivalent to 1 billion bytes or 1 thousand megabytes. Typical computer hard disk drives have a storage capacity measured in tens or hundreds of gigabytes.

HOSDB

Home Office Scientific Development Branch

IEEE 1394

See FireWire

iLink

See FireWire.

IP

Internet Protocol. A standard that allows for the transmission of data across networks. Every machine on the network has a unique identifying number, known as an IP address.

Master

The original copy of the data, that is documented, sealed and stored according to established procedures and can be examined by a court if required, to confirm the authenticity of the evidence. When video is recorded to a hard drive, the data may be transferred to a removable medium, e.g. CD/DVD, creating a permanent copy which would be defined as the master.

MB

Megabyte. A unit of information or storage equivalent to 1 million bytes

Native File Format

The file format of the primary image or original recording on the hard disk drive

PACE

Police and Criminal Evidence Act

PAL

Phase Alternate Line. Video colour coding standard adopted for television in UK and most other European countries using 625 lines and 25 frames per second.

PC

Personal Computer

Secure Server

The term 'secure server' should be taken to mean an environment, including a security management system, which is accredited to a level of at least 'RESTRICTED' under the Government Protective Marking Scheme (GPMS), in accordance with the ACPO Community Security Policy (CSP), as documented in an associated Accreditation Documentation Set (ADS) and as approved by either the local Force Information Security Officer and/or the National Accreditor for Police Information Systems.

SIO

Senior Investigating Officer

SVHS

Super VHS. Higher quality semi-professional version of VHS with improved picture detail

TB

Terabyte. A unit of information or storage equivalent to 1 million megabytes or 1 thousand gigabytes

USB

Universal Serial Bus. A standard interface port between a computer and add-on devices. USB transfers data at speeds of up to 12 megabits per second, while the newer USB2 allows data transfer at up to 480 megabits per second.

VGA

Video Graphics Array. Refers to both a resolution format for digital monitors and the cables which connect to the display

VHS

Video Home System. Domestic analogue videotape format

Working Copy

A copy of the data made either from the master copy, or at the same time as the master copy, and used for investigation, technical investigation, briefings, circulation and preparation of prosecution or defence evidence.

WORM

Write Once Read Many. Used when discussing computer storage media that can be written to only once, but read from multiple times, such as CD-R and DVD+/-R.

This is an official document.

If found please return to the nearest police station and inform them how and when it was found. Its unauthorised possession, use, retention, alteration, destruction or transfer to another person may be an offence under the Official Secrets Act.

Home Office Scientific Development Branch
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051
Fax: +44 (0)1727 816233
E-mail: hosdb@homeoffice.gsi.gov.uk
Website: http://science.homeoffice.gov.uk/hosdb/

ISBN: 978-1-84726-832-7