Forensic Science Regulator

Overseeing Quality

Codes of Practice and Conduct

Appendix: Digital Forensics - Video Analysis

FSR-C-119

Issue 1

CONTENTS

1. INTRODUCTION

1.1.1 The provider of digital video analysis (the provider) shall comply with the *Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System* (the Codes) and be accredited to BS EN ISO/IEC17025:2005 for any laboratory activity (such as the recovery, preservation, production and analysis of video material).

1.1.2 The Forensic Science Regulator (the Regulator) has determined that BS EN ISO/IEC17025:2005 is the appropriate international standard for the digital forensic sciences, including video analysis, related image analysis and audio analysis. Standards such as ISO/IEC27037:2012 may be used as guidance if required, however, they are not equivalent and cannot be used as a substitute for the accreditation standard.

1.1.3 Digital video analysis is a subset of the broader field of digital forensics, and reference should therefore be made to the appendix to the Codes on Digital Forensics (FSR-C-107-001 Digital Forensics)[1]. However, there are some significant differences that the provider needs to be aware of, such as:

a. the use of unusual storage media formats;

b. proprietary video formats; and

c. the fact that video and associated audio material more commonly comes from 'witness' rather than 'suspect' sources, often without access to the original.

1.1.4 In many situations the role of providers is to facilitate viewing by others rather than to undertake analysis as such, and this also raises various issues relating to human factors (e.g. contextual bias, although this is outside the scope of this document).

1.1.5 This appendix endeavours to explain the above differences, principally through the use of an extensive glossary, with the main body of the text being used to

[1] Available from: https://www.gov.uk/government/publications?departments%5B%5D=forensic-science-regulator [Accessed 8/8/14]

identify the specific measures that the Regulator believes an auditor would expect to see demonstrated.

1.1.6 This appendix should be read alongside the Codes, the appendix to the Codes Digital Forensics (FSR-C-107[2]), BS EN ISO/IEC17025:2005 and the International Laboratory Accreditation Cooperation (ILAC) publication *Guidelines for Forensic Laboratories,* ILAC-G19,[3] and will generally follow the heading titles used in the Codes with cross references to ISO/IEC17025:2005 given in parentheses.

2. SCOPE

2.1.1 This appendix covers forensic digital video analysis laboratory activity from receipt of video material through to preparation for court. It does not yet include retrieval from the scene (this is expected to be added in due course) nor expand on the requirements laid out in the Codes on the presentation of expert evidence. It applies to all providers undertaking this work whether they are police facilities, commercial suppliers or academia.

2.1.2 The above scope is very broad in terms of the circumstances in which providers are asked to operate ranging, e.g. from the simple viewing of CCTV in volume crime cases through to detailed analysis of material for more serious crimes. A 'one size fits all' approach is unlikely to be efficient, and providers are encouraged to identify and justify responses to the Codes that are suitably proportional to the circumstances that apply.

2.1.3 Forensic analogue video analysis is not the focus of this appendix, in view of its declining prevalence. However, the digitisation of analogue video is covered and some general advice provided in section 6.2 and the Glossary.

2.1.4 Digital stills derived from sources other than video devices (such as digital still cameras, mobile phones) are currently (as at June 2014) outside of the scope of this appendix, though the post-capture analysis of such images will generally follow the same processes and principles contained here.

---

[2]Available from: https://www.gov.uk/government/publications?departments%5B%5D=forensic-science-regulator [Accessed 8/8/14]

[3] Available at: http://www.ilac.org/documents/g19_2002.pdf [Accessed 8/8/14]

2.1.5 Analysis of associated audio material is not within the scope of this appendix, but providers should have a procedure to ensure that any audio is identified and its presence recorded in the case-notes.

3. IMPLEMENTATION

3.1.1 This appendix is available for incorporation into a provider's quality management system from the date of publication. The Regulator requires that the Codes and this appendix are included in the provider's schedule of accreditation by October 2017 as detailed in the Codes.

4. MODIFICATION

4.1.1 This is the first issue of this document.

5. SERVICE TO THE CUSTOMER (ISO/IEC17025:2005, 4.7)

5.1.1 When clarifying the customer's requirements for work to be performed, the provider shall ensure that the customer is made aware of any limitations or caveats that are already known to apply to this type of analysis.

5.1.2 Examples of limitations or caveats known in advance may include that:

a. the method required is outside of the provider's existing accreditation;

b. the method required is not validated for the specific purpose presented;

c. the work required is likely to include aspects outside of the provider's professional competence.[4]

d. the underlying scientific basis is questioned;

e. decisions of the Court of Appeal Criminal Division suggest such evidence may not be received as expert evidence;[5]

---

[4] For example, the scientist may be competent in processing video material and images but not in image comparison or in assessing material in the images (e.g. vehicle type).

[5] In *R. v. Cooper* [1998] EWCA Crim. 2258: *"An expert's opinion is admissible to furnish the court with scientific information which is likely to be outside the experience and the knowledge of a judge or jury. If, on the other hand, on the proven facts or on the nature of the evidence, a judge or jury can form their own conclusions without help, then the opinion of an expert is unnecessary."* However, see also *R. v. Atkins & Atkins* [2009] EWCA Crim. 1876: *"… leaving the jury to make up its own mind about the similarities and dissimilarities, with no assistance at all about their significance, would be to give the jury raw material with no means of evaluating it."*

f. the method's inherent measurement uncertainly is likely to provide such a wide range that the result is likely to be inconclusive *a priori* (e.g. a height measurement with ± 5 cm could apply to a wide range of the population and if given with a 95% confidence limit, may not exclude either).

6. PERSONNEL (ISO/IEC17025:2005, 5.2)

6.1 Competence

6.1.1 Staff shall have a clear understanding of the overall video forensic process (refer to Glossary) and be mindful of the objectives of all operations they perform. Those responsible for formulating the work flow through the process shall be able to assess the impact of video transformations at all stages of the process.

6.1.2 Storage media from digital video recorders (DVRs) will often present unknown, proprietary file-systems. These are not recognised or interpreted by common digital forensic hard disk drive interrogation tools. Thus to avoid misinterpreting a storage medium as containing no CCTV, a digital forensic examiner must be competent at recognising the byte-level indicators of the likely presence of video or audio on such storage media.

7. SELECTION OF METHODS (ISO/IEC17025:2005, 5.4.2)

7.1 Transformations

7.1.1 Video material received by a provider will already have undergone transformations[6] such as spatial and temporal sampling, digitisation, transcoding and compression. The effect of those transformations shall be taken into account in all subsequent processing and interpretation.

7.1.2 The person responsible for transforming video material should be competent to assess the likely impact of the transformations on its intended use.

[6] Any process that alters the format or information content of video, e.g. digitisation, transcoding (i.e. digital-to-digital conversion of one encoding to another to an alternative file). See Glossary, Video transformation.

7.1.3 Where a provider undertakes the transformation of video material, the transformations shall be documented and shall be appropriate for the intended use of the transformed material.

7.2 Analogue Video

7.2.1 Where analogue video is to be digitised, the conversion should take place as soon as possible in the process once it has been identified that the footage may be of interest (typically after initial viewing).

7.2.2 As with all transformations, where digitisation is performed it must be done so as to minimise any loss of information that may be relevant to the investigation. Equally, any decision not to digitise must take into account the risks of degradation to the analogue medium and must be documented.

7.2.3 Appropriate hardware is required to extract the maximum amount of information in terms of image quality, audio tracks and associated metadata. Any departures from this shall be justified and documented.

7.3 Enhancement

7.3.1 Providers shall be clear on the purpose of any image enhancement that is to be carried out and anticipate any data losses that may occur as a side effect. They shall be able to demonstrate the appropriateness of any enhancements. An audit trail is to be maintained and the original (pre-enhanced) image retained.

7.3.2 Images enhanced for one purpose shall not be used for another purpose without fully reconsidering the appropriateness and the risks.

7.3.3 In forensic applications, enhancements should not generally be applied to selective portions of an image unless these regions and the enhancements within them are clearly identified. However, it is permissible to enhance the whole of a cropped image.

7.3.4 It is important that recipients of enhanced images (e.g. investigators, experts or jury members) are not misled in any way. To this end, care shall be taken to ensure that enhanced images are identified as such and that sufficient information on the performed enhancement is available in the case-notes.

7.4 Tracking

7.4.1 The basis for tracking objects or people (either manually or automatically) shall be documented with risks identified and mitigated.

7.5 Image Comparison and Image Analysis

7.5.1 Providers who undertake image comparison must do the following.

a. Demonstrate the appropriate competence in relation to the image-based processes[7] that have been undertaken in addition to demonstrating competence in comparison.

b. To reduce the risk of confirmation bias, incident footage containing unknown persons or objects of interest shall be analysed to identify distinguishing features before known footage of the suspect objects of interest is viewed or information revealed to the analyst.[8]

c. Ensure that all relevant information in relation to image processing undertaken by a third party is communicated to the person undertaking the comparison.

d. Demonstrate the decision process and basis for critical findings.

e. Demonstrate that the methods used for comparison are appropriate, through validation, for the image characteristics of the case material. For example, methods developed for high quality recordings may not be valid for low quality CCTV images.

8. VALIDATION OF METHODS (ISO/IEC17025:2005, 5.4.5)

8.1 Validation Introduction

8.1.1 The method shall be validated, or any existing validation to be verified, as laid out in the Codes. The functions used in hardware and software tools where

[7] The methodology used should be clear. The method may include the Analyse, Compare, Evaluate, Verify, Report (ACE-VR) methodology that is used for other types of comparisons. However, the overall method still requires validation as detailed in the Codes and Section 8 of this document.

[8] When commissioning experts, officers should consider whether phased disclosure to the provider is appropriate as the bias is an unconscious act and prior knowledge by the examiner of certain information (e.g. the target number plate, injury, congenital disorders, damage features) may be seen as a source of such bias.

operation has an impact[9] in obtaining results are to be validated as part of that validation of the method.

8.2 Data Recovery

8.2.1 When video data are not readily accessible by standard/manufacturers' methods (e.g. because a file-system or a file has become corrupted) it may be necessary to recover these video data in the laboratory by a process akin to reverse engineering. When undertaking this casework the method shall be subject to validation in line with ISO/IEC17025:2005 and the Codes noting especially the following.

a. Not all video material will necessarily be recovered.

b. Data might be incorrectly interpreted (e.g. time and date stamps).

8.3 Image Comparison

8.3.1 All methods designed for image comparison require validation, where the comparison uses proportional relationships and/or metrics the validation shall include an appropriate, robust and repeatable method for quantifying the associated uncertainties (see **9.1 Photo/Videogrammetry**).

8.4 Reliability of Manufacturers' Players

8.4.1 In many instances examiners will have no option but to utilise proprietary replay software but will not have the practical means of comprehensively validating it. Consideration shall be given to the associated risks and how these may be mitigated in a proportionate manner as required in the Codes. For example, the risk mitigation approach may take into account:

a. the context, including what the tool is required to do and how the data will be used;

b. the competence of the practitioner;

[9] The Codes require software to be assessed for the impact on results and is documented in sufficient detail based on that assessment. The validation requirement is for the overall method, rather than individual software packages and all the functions they contain.

c. how well-established the body of knowledge for the replay tool is within the forensic practitioner community.

8.4.2 The version of software used shall always be included as part of the record. In the absence of this information being available, preservation of one or more screenshot images may provide a basis for identification of the version used.

9. ESTIMATION OF UNCERTAINTY OF MEASUREMENT (ISO/IEC17025:2005, 5.4.6)

9.1 Photo/Videogrammetry[10]

9.1.1 When extracting dimensional information from imagery, it is essential that there is an appropriate, robust and repeatable method for quantifying the uncertainties associated with any quoted value. In addition, in cases where timing information from a video recording is crucial (e.g. speed estimations of vehicles from CCTV), a suitable method for quantifying the uncertainty in such a measurement must be employed.[11] This method will take account of the whole recording process (image capture, image encoding, metadata assignment, data storage).

9.2 Derivation of Date/Time/Framing Rate

9.2.1 The date/time information provided by the multitude of CCTV systems in use is of highly variable quality. The following shall be taken into account where the date/time information may be important.

a. The displayed time may not represent the actual capture time.

b. It is necessary to consider both the precision and the accuracy of any displayed time as apparent precision may not be an indicator of accuracy.

c. The internal/displayed clock may not be accurate or sufficiently precise.

d. There may be more than one displayed clock.

---

[10] This is taken to be a technique that attempts to compare the proportional relationships of one photo usually using metrics. Related terms include photoanthropometry and to a lesser extent proportional alignment.

[11] For instance as described in HOSDB (2007) *Single Image Photogrammetry*.: http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/VP_A_Manual_-_Analysis_-_Si12835.pdf?view=Binary [Accessed 10/03/14]

e. The image capture rate may not be regular so a calculated average framing rate cannot always be applied to a single specific frame interval.

f. The frame lapse setting information contained within the system menu will not always be a true reflection of the actual recorded rate.

g. All computer-based systems are prone to hesitation under load, which can introduce unpredictable interruptions in record sequences.

h. What is displayed may not correspond to what is stored.

i. Time stamps might be a network time stamp of when information is received, not when it is digitised.

9.2.2 Techniques such as extended section analysis, analysis of camera sequence order, interrogation of the system menu and independent timing of the system performance may be considered to provide an holistic view of the accuracy of the derived times/rates.

10. CONTROL OF DATA (ISO/IEC17025:2005, 5.4.7)

10.1 Inadvertent Overwriting by Digital Video Recorders

10.1.1 Due to the proprietary nature and often limited functionality of some digital video recorder (DVR) equipment it is necessary to consider and prevent mechanisms that could result in lost or inaccessible data. Consideration shall be given to the following when processing a DVR device.

a. Disconnecting the hard disk drive (HDD) from the main board of the DVR may cause the HDD to be permanently disassociated from this machine, rendering the video inaccessible by that machine.

b. Connecting a HDD write blocker in line with the HDD may result in the HDD being unrecognisable by the DVR.

c. Clone copy HDDs may be unrecognisable by the DVR.

d. DVR units may go into auto-record mode when switched on – even if no video source is connected.

e. Some DVR units are equipped with timed expiry (refer to Glossary). This can result in data being marked as 'deleted' even if the machine is switched off.

10.2 Suspect Versus Witness

10.2.1 A distinction may be made between video material that has been received from a suspect source and that from a witness source, and the examination procedure and forensic strategy may reflect this.[12] This is because in most cases it is reasonable to assume that a witness machine has not been tampered with and does not contain deliberately hidden data. For example, for a suspect machine it may be essential to recover the system log for an extended period of time, whereas for a witness machine this may only be required for a short period of time, if at all.

10.2.2 Given this assumption, and noting that it is not always possible or practical to image or write-protect the entire device, a proportionate approach may be taken in the forensic strategy.

10.2.3 If digital CCTV systems are to be examined without write protection or a forensic copy produced prior to any live examination, justification needs to be included in the laboratory procedures and documented in the case-notes.

10.2.4 The HOSDB 58/07 Digital Imaging Procedure[13] shall be taken into account when formulating the strategy.

10.3 Conversion to Broadcast Video

10.3.1 Video material from CCTV sources often does not conform to the constraints of broadcast video. Transforming video from CCTV sources into broadcast video often requires spatial and temporal re-sampling, which leads to a loss of information that may be important in subsequent processing and interpretation.

---

[12] Good practice would suggest that all material should be treated the same, and the risk of tampering considered, irrespective of the source. Also the possibility that a witness becomes an additional suspect later on should be borne in mind. Examiners must satisfy themselves that the footage can be relied upon.

[13] Available from: http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)47aa.html?view=Standard&pubID=555512 [Accessed 8/8/14]

10.3.2 Validated procedures shall therefore be in place to ensure that the conversion of video material to a broadcast video format is appropriate for its intended use.

11. COMPUTERS AND AUTOMATED EQUIPMENT (ISO/IEC17025:2005, 5.5)

11.1 Export of Video and Stills from CCTV Players

11.1.1 Many CCTV players perform a conversion to a broadcast video format either implicitly during playback or explicitly during video export. They also commonly re-sample and transcode images when exporting still images. The nature of the transformations introduced by tools used for exporting video and stills from CCTV shall be assessed so that their impact on the subsequent use of the transformed material can be determined.

11.2 Automated Tools

11.2.1 The declared performance, in terms of probability detection (PD) and false alarm rates (FAR), of video content analysis tools is dependent on the quality of the video to be analysed. When using video analytic tools for post-event analysis, the provider shall be aware of the impact of video quality on performance. A risk analysis of the actual PD and FAR on the required task shall be undertaken and communicated to the customer.

12. TEST REPORTS, STATEMENTS AND THE PRESENTATION OF EVIDENCE (ISO/IEC17025:2005, 5.10.2)

12.1 Displaying Images

12.1.1 In cases where the detail of an image or the colour of an item is important, (e.g. in court), the optimised set up of viewing screens, prints and other presentation media shall be considered in conjunction with the use of high quality originals.

12.1.2 Care shall be taken to ensure that recipients of enhanced images (e.g. investigators, experts or jury members) are given sufficient information so as not to be misled.

12.2 Interpretation

12.2.1 All imagery viewing requires a degree of interpretation. This may be considered as ‘expert-based interpretation’ or ‘bulk viewing interpretation’ (refer to ‘Image Interpretation and Comparison’ in the Glossary, which also gives examples of the types of problems that can arise).

12.2.2 In the case of expert interpretation, all reasoning and justification shall be explicitly noted in reports.

12.2.3 In the case of bulk viewing, the competence of the person who prepares the material for viewing shall ensure that the risk of errors are minimised.

12.3 Multiple Evidential Approaches

12.3.1 Where the expert has undertaken several forms of analysis (e.g. height analysis and the comparison of physical features) the report must make clear the opinions and conclusions reached by the expert in relation to each of these individually. The expert may then provide an overall opinion and conclusion.

13. REVIEW

13.1.1 This document is subject to review in accordance with the Codes and other appendices.

13.1.2 If you have any comments please send them to the address as set out on the internet site at www.gov.uk/government/organisations/forensic-science-regulator or email: FSREnquiries@homeoffice.gsi.gov.uk.

14. BIBLIOGRAPHY

BS EN ISO/IEC 17020:2012, *General criteria for the operation of various types of bodies performing inspection*.

BS EN ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories.*

BS ISO/IEC 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence*

ILAC-G19:2002, *Guidelines for Forensic Science Laboratories.* Available from: https://www.ilac.org/documents/g19_2002.pdf [Accessed 8/8/14]

Home Office Scientific Development Branch (2007) *Digital Imaging Procedure*, v2.1, 58/07 Available from: http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)47aa.html?view=Standard&pubID=555512 [Accessed 8/8/14]

Home Office Scientific Development Branch (2007) Single Image Photogrammetry.: http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/VP_A_Manual_-_Analysis_-_Si12835.pdf?view=Binary [Accessed 10/03/14]

National Policing Improvement Agency (2007) *Practice advice on police use of digital images.* Available from: http://www.acpo.police.uk/documents/crime/2011/20111014%20CBA%20practice_advice_police_use_digital_images_18x01x071.pdf [Accessed 8/8/14]

15. GLOSSARY

Analogue Video

Video that is in non-digital form. It is generally stored on magnetic tape and as such shall be regarded as being fragile since repeated use may result in damage (See Neil D. C., Mather P. and Brown E. C. (1998) *Guidelines for the Handling of Videotapes*, Police Science Development Branch Publication 21/98). Therefore it is advised that a working copy of a master recording be made to an appropriate medium wherever practical.

Broadcast Video

Video material with a format that is consistent with that commonly used in broadcast, film and on the internet. There is a wide range of standards for such video ranging from older ones derived from PAL and NTSC[14] analogue formats through to more recent ones based on high-definition television (HDTV). Tools for broadcast video typically assume a fixed frame rate and a limited set of image sizes and pixel aspect ratios.

CCTV Video

Video obtained from CCTV sources. Video material from CCTV sources often does not conform to the constraints of broadcast video. Images may be recorded at a rate that is neither fixed nor consistent with the assumptions of tools designed for non-CCTV sources. Additionally, the width and height of the images in pixels, and the pixel image aspect may not conform to broadcast conventions. Transforming video from CCTV sources into broadcast video often requires spatial and temporal re-sampling, which leads to a loss of information that may be important in subsequent processing and interpretation. As with all transformations, care shall be taken to ensure that the conversion of video material to a broadcast video format is appropriate for its intended use.

Contextual Bias

To be unconsciously influenced by knowledge about the background to the case or by other case information.

Derivation of Date/Time/Framing Rate

The derivation of real time, date or time data from CCTV recordings and determination of the framing rate (elapsed time between images) for a particular recording.

Displaying Images

The process of making images available in viewable form. Various problems can be introduced if images are displayed inappropriately, as indicated below. However, an issue to consider first is whether the information is reliable with respect to the purpose for which it is being used. For example, if colour is evidentially important it becomes pointless and potentially misleading to concentrate on ensuring that a

[14] Denoting Phase Alternating Line and the National Television System Committee standards.

display monitor is properly calibrated if the colour integrity has been undermined by a previous transformation.

That said, the following shall be noted.

a. Images can be subjected to degradation or changes to colour and brightness if viewed on an un-calibrated monitor or on a screen set to a low resolution. The effect on the image being viewed compared with the image as recorded should be understood. In cases where viewing is done simply to verify the presence or absence of a person or item in the scene these differences may be of little significance.
b. In cases where the detail of an image or the colour of an item is important (e.g. in court) the optimised set up of viewing screens should be considered. It should further be remembered that the wiring used to connect monitors, if incorrectly used, can cause significant degradation of the image in relation to its original state.

DVR

Digital video recorder – hardware that records video data (and may also record audio data) to a digital medium (usually a hard disk drive).

Enhancement

A transformation that seeks to accentuate the information of interest that potentially diminishes other information. Enhancement reduces the information content of imagery but can aid its interpretation. Examples include brightness and contrast adjustment, cropping, sharpness filters and noise reduction filters. Reference should be made to the Association of Chief Police Officers (ACPO) National Policing Improvement Agency's (NPIA's) *Practice Advice on Police Use of Digital Images 2007*[15] – Section 3.3.

HDD

Hard disk drive

Image Interpretation and Comparison

Every (normally sighted) person inherently believes that they are competent to interpret images. However, particularly when dealing with images of poor quality,

[15] Available from: http://www.acpo.police.uk/documents/crime/2011/20111014%20CBA%20practice_advice_police_use_digital_images_18x01x071.pdf [Accessed 8/8/14]

this false sense of capability may lead to erroneous conclusions. Every viewing action involves some form of interpretation.

Expert-Based Interpretation

'Expert-based interpretation' is the allocation of significance (a blend of subjective opinion and factual information) to elements of an image by specifying ranges for the variables. This incorporates a knowledge and due consideration of factors such as:

a. resolution;
b. compression;
c. aspect ratio;
d. shadows and halation effects;
e. viewing on different equipment;
f. confirmation bias.

As such, a large part of any examination and interpretation exercise is the consideration of other potential causes for the formation of the 'feature'. Expert-based interpretation requires specific subject matter expertise of both the system and the subject to be analysed. The role of the forensic imagery analyst is to assist the court in understanding what may reasonably be learnt from the imagery. The following are examples of tasks that may be undertaken by a forensic imagery analyst involving 'expert-based interpretation':

a. image processing/enhancement;
b. image comparison (of objects or individuals);
c. chronology of events;
d. authentication;
e. photogrammetry, including height assessment;
f. vehicle registration number (VRN)/determination of vehicle make and model.

During these tasks, different approaches may be adopted by different practitioners, which may result in different conclusions. As a result, it is essential that all reasoning and justifications are explicitly noted in reports. If multiple experts from different backgrounds and using different equipment find the same feature, then confidence must be improved that the feature exists.

Bulk Viewing/Basis Interpretation

The competence of the person who prepares the material for viewing should ensure that the risk of errors during 'bulk viewing' are minimised. However, levels of competence/training/guidance for those undertaking bulk viewing need to be addressed to avoid errors in the early stages of determining the 'usefulness' of any imagery. Competence may be tested at pre-trial case management or ultimately in court.

Imagery

A general term that denotes still and/or video images.

Laboratory Activity

The current scope of this appendix (see Section 2) covers laboratory practices from receipt of video material through to preparation for court. In this context a laboratory practice (i.e. activity or function) is any measure taken when handling, developing, analysing or interpreting forensic evidence with a view to providing an expert opinion or exchanging forensic evidence.

Replay Software

Digital CCTV systems often have an export function so that video footage can be backed up to removal media (e.g. CCTV, Universal Serial Bus hard disk). In addition to the digital video footage the systems will also include proprietary replay software that has been developed and distributed by the systems manufacturers. This software can be classed as commercial off-the-shelf software and initially treated as a trustworthy piece of software, as laboratories do not have access to the coding in order to verify its implementation. For this reason the examiners must assure themselves that the software is working correctly on this workstation and investigate further using other replay software if there are any signs of replay issues (e.g. dropping frames, rescaling issues, wrong proportions).

It should be noted that there may not be obvious signs when replay software is performing incorrectly, so best practice is to follow the dual approach as standard, and to document any reason why this has not been possible.

It is also worth noting that the video files exported from the digital systems may contain additional information, e.g. audio, Global Positioning System (GPS), which is not presented by the replay software. If this type of information is of relevance to

the case the examiner should investigate further. It is expected that the examiners will have been trained to identify issues with replay software in Section 6.1.

Reverse Engineering

Reverse engineering is the process of deconstructing and interpreting an electronic device or data format without prior access to the creator's specification or design.

Timed Expiry

A feature of DVRs that allows the equipment to adhere to data retention policies that may be mandated in certain parts of the world and that result in video data becoming inaccessible after a certain date. This may happen even when the DVR is switched off.

Tracking

Moving objects or people are often tracked through a scene by applying arrows or highlights on a digital editing suite in order to draw attention to the object or person of interest. Whilst being a helpful technique to aid the understanding of a video sequence, caution should be exercised.

a. Automated tracking software can easily be misled by other unrelated objects in a scene and should be used with caution.
b. Manual tracking of objects by a human operator is more reliable but still prone to error, particularly within confusing scenes or where the object of interest is of low resolution. In such cases it is advisable to verify the accuracy of the path of the object being tracked by using more than one camera viewpoint. If there is only a single viewpoint available any uncertainty should be documented.

Transcoding

The process of converting a file from one encoding to another, usually in an alternative destination i.e. not written over.

Transformation

See Video Transformation.

Video Forensic Process

The overall process whereby video evidence is made available to investigators and to court comprising:

a. field retrieval;
b. laboratory retrieval;

c. lossless extraction of data from proprietary formats;
d. processing;
e. interpretation;
f. reporting.

Video Material

A sequence of images together with associated metadata.

Video Transformation

Any process that alters the format or information content of video. Commonly occurring transformations include:

a. digitisation;
b. transcoding;
c. spatial and temporal sampling/re-sampling;
d. enhancement;
e. rendering to computer displays; and
f. printing of images.

Video is subject to a series of transformations from its initial creation through to rendering on a display surface for human interpretation. Many of these transformations add and remove information from the video material. During these tasks, different methods may be adopted by different practitioners, which may result in different opinions.

Witness Versus Suspect

A distinction is made in this document between evidence that comes from a witness source (i.e. a person not under suspicion) and evidence that comes from a suspect source (i.e. a person who may be suspected of having committed an offence). However, this should be identified in the forensic strategy as the risk of tampering should be considered, and as additional circumstances may later come to light, for example a witness becomes an additional suspect. In the latter situation the possibility of falsified or hidden video images must be considered. Examiners must satisfy themselves that the footage can be relied upon.

Published by:
The Forensic Science Regulator
5 St Philip's Place
Colmore Row
Birmingham
B3 2PW
https://www.gov.uk/government/organisations/forensic-science-regulator

ISBN: **978-1-78246-493-8**