Forensic Science Regulator
Overseeing Quality

Codes of Practice and Conduct

Appendix: Digital Forensics - Video Analysis

FSR-C-119

Issue 2

Contents

1. Introduction

1.1.1 Forensic units [1] providing digital video analysis shall comply with the Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System (the Codes) [1], this appendix FSR-C-135, and when required by the Codes, [2, 3] be accredited to ISO17025 [2] 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 ISO17025 is the appropriate international standard for the digital forensic sciences, including the processing and handling of video, related imagery and audio. Standards such as ISO/IEC27037:2012 [3] 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 Digital Forensics) [4]. However, there are some significant differences that the forensic unit 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 See glossary for full definition; it is used in this document to cover forensic science providers of all sizes including small teams or even sole practitioners carrying out the forensic activity and is therefore not limited to a video unit, imaging unit etc.

2 The Codes section titled ‘Statement of Standards and Accreditation Requirements for all forensic units providing forensic science services’ details the required standards and timetable and the assurance mechanisms required such as accreditation.

3 Where the activity performed is viewing with no further analysis, the Codes contain further detail on the extent of the accreditation element of this requirement for activities such as CCTV replay conducted by competent staff using methods approved by the organisation. Except for provisions in PACE Code D, no exemption should be inferred where opinion is required to be given in evidence.

1.1.4 In many situations the role of forensic units 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 [5]).

1.1.5 This appendix should be read alongside the Codes, the appendix to the Codes Digital Forensics (FSR-C-107), ISO17025 and the International Laboratory Accreditation Cooperation (ILAC) publication Modules in a Forensic Science Process (ILAC-G19), [6] and will generally follow the heading titles used in the Codes.

1.1.6 The word ‘shall’ is used in this document where it is a requirement; the word ‘should’ has been used to indicate a recommendation that is generally accepted practice in the forensic science process.

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 include additonal detail on retrieval from the scene [4] nor include all of the requirements laid out in the Codes on the presentation of evidence. It applies to all forensic units undertaking this work whether they are police facilities, commercial suppliers, individual practitioners or in academia.

2.1.2 The above scope is very broad in terms of the circumstances in which forensic units 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 forensic units 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 7.2 and the Glossary.

[4] The primary consideration when conducting scene retrieval of video data is where possible to acquire the data in its native format.

2.1.4 Digital stills derived from sources other than video devices (such as digital still cameras, mobile phones) remain 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. Not being in the scope of this video appendix should not be taken to automatically provide an exclusion from standards or accreditation requirements, but it is anticipated that most analysis of still images will form part of another activity e.g. fingerprint enhancement.

2.1.5 Analysis of associated audio material is not within the scope of this appendix, but forensic units should have a procedure to ensure that any audio is identified and its presence recorded in the case-notes. See appendix on: Speech and Audio Forensic Services (FSR-C-134). [7]

3. Implementation

3.1.1 This appendix is available for incorporation into a forensic unit's quality management system from the date of publication. The Regulator requires that the Codes and this appendix are included in the forensic unit's schedule of accreditation by October 2017 for the video scope set out in the Statement of Standards and Accreditation Requirements within the Codes.

4. Modification

4.1.1 This is the second issue of this document.

4.1.2 Significant changes to the text have been highlighted in grey.

4.1.3 The modifications made to create Issue 2 of this document were, in part, to ensure compliance with The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018. [5] Text identified as out-of-date during this accessibility review has either been modified or deleted.

---

[5] To facilitate the operation of the Regulations the following significant changes to sections of the document are noted here. The following sections of the document have been amended: Contents table, 1.1.1, 1.1.2, 1.1.6, 2.1.1, 2.1.4, 2.1.5, 3.1.1, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 5.1.2, 6.1.1, 6.1.3, 6.1.4, 6.1.5, 7.1.2, 7.2.2, 7.3.1, 7.4.1, 7.5.1, 8.1.2, 8.1.3, 8.3.2, 8.3.3, 9.1.1, 9.1.2, 9.1.3, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 10.1.1, 10.2.1, 10.3.1, 10.3.2, 10.3.3, 10.4.1,10.5, 10.5.1, 10.5.2, 10.5.3, 11.1.1, 11.1.2, 11.2, 11.2.1, 12.1, 12.1.1, 12.2, 12.2.1, 12.2.2, 12.2.3, 12.4.2, 12.5.1, 12.6, 12.6.1, 12.6.2, 12.6.3, 12.6.4, 12.6.5, 14, 15. The following footnotes have been amended: 1, 2, 3, 4, 5, 7, 9, 11, 13, 14, 15, 16, 17, 18, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30. To facilitate the operation of the Regulations

4.1.4 The Regulator uses an identification system for all documents. In the normal sequence of documents this identifier is of the form 'FSR-#-###' where (a) the '#' indicates a letter to describe the type or document and (b) '###' indicates a numerical, or alphanumerical, code to identify the document. For example, the Codes are FSR-C-100. Combined with the issue number this ensures each document is uniquely identified.

4.1.5 In some cases, it may be necessary to publish a modified version of a document (e.g. a version in a different language). In such cases the modified version will have an additional letter at the end of the unique identifier. The identifier thus becoming FSR-#-####.

4.1.6 In all cases the normal document, bearing the identifier FSR-#-###, is to be taken as the definitive version of the document. In the event of any discrepancy between the normal version and a modified version the text of the normal version shall prevail.

5. Service to The Customer

5.1.1 When clarifying the customer's requirements for work to be performed, the forensic unit 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 forensic unit's existing accreditation;
b. The method required is not validated for the specific purpose;
c. The work required is likely to include aspects outside of the forensic unit staff's competence; [6] [8]
d. The underlying scientific basis or application of the method is questioned; [7]

---

the following significant changes to sections of the document are noted here. The following sections of the document have been amended.

6 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).

7 For example, with comparison of facial images derived from uncooperative/uncontrolled settings (i.e. CCTV), the following methods are questioned in the scientific literature and international guidance for both inculpatory and exculpatory purposes: facial feature classification, photo anthropometry/proportional alignment and superimposition/overlaying [18] [19] [20] [21] [22] [23] [24].

e. Decisions of the Court of Appeal Criminal Division suggest such evidence is only admissible as expert evidence and, for example, the forensic unit's analysts are not experts in the subject matter intended to be compared within the footage; [8] [8] and

f. The method's inherent measurement uncertainly is likely to provide such a wide range that the result is likely to be inconclusive in advance (e.g. a height measurement with a calculated tolerance of ± 5 cm could apply to a wide range of the population and may be of no probative value).

6. Personnel

6.1 Competence

6.1.1 Practitioners 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. They shall be competent in the formulation of process workflow to correctly achieve a desired task without unnecessary transformations. They shall be able to assess the impact of video transformations at all stages of the process and understand the importance of keeping contemporaneous notes.

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 shall be competent at recognising the byte-level indicators of the likely presence of video or audio on such storage media.

6.1.3 Statements related to provision of recognition rather than an identification through comparison should be prepared by individuals competent in the

[8] 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." [8] 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." [25]

application of the Police and Criminal Evidence Act (PACE) Code D, Code of Practice for The Identification Of Persons By Police Officers. [9]

6.1.4 All practitioners shall understand the distinction between expert evidence and evidence of fact.

6.1.5 The person proposing to give opinion evidence shall be an expert in all relevant aspects they intend to give an opinion on. Expertise in CCTV, video, imaging, enhancement etc. does not equate to expertise on the content of the image. Unless they are also an expert in the content of the images, imagery experts should not attempt to give expert opinion evidence on the meaning of a comparison between the objects in question. [8]

6.1.6 Image analysis requires specific subject matter expertise of both the system and the subject to be analysed. [9]

7. Selection of Methods

7.1 Transformations

7.1.1 Video material received by a forensic unit will already have undergone transformations [10] 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 Where a forensic unit undertakes the transformation of video material, the transformations shall be appropriate for the intended use of the transformed material and shall be documented.

---

[9] An expert in video processing or even facial comparison is not necessarily competent to give an opinion on vehicle identification without demonstrating specific competence in that activity using a demonstrably valid method.

[10] 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.

7.2 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 needs to be done so as to minimise any loss of information that may be relevant to the investigation. Equally, any decision not to digitise shall take into account the risks of degradation to the analogue medium and the rationale shall 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 Forensic units 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 preserved.

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 in Footage

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

7.5 Image Comparison and Image Analysis

7.5.1 Forensic units that undertake image comparison shall do the following.

a. Use valid methods. [11]

b. Recognise that image comparison is a form of opinion evidence [10] and is admissible where the judge and jury require the assistance of evidence which depends on the application of specialist skill or knowledge in the field that is under comparison (i.e. are experts). [8]

c. Demonstrate the appropriate competence in relation to the image-based processes [12, 13] that have been undertaken in addition to demonstrating competence in comparison of the type of material being compared in an image.

d. To reduce the risk of confirmation bias, [14] incident footage containing unknown persons or objects of interest shall be analysed to identify distinguishing features before known footage of the suspect objects of

---

11 Validations should include an objective literature review so that the design of the validation study takes into account shortcomings previously identified in the scientific literature in that and all related methods. Methods that been challenged in the scientific literature should not be used unless the validation is shown to overcome previous shortcomings, and the court must be made aware of the previous criticism even if they have been overcome. Previous acceptance in this jurisdiction does not provide evidence of validation.

12 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.

13 Experts shall ensure that they act only within their area of expertise; an expert in facial comparison is not necessarily competent to give an opinion on vehicle identification without demonstrating specific competence in that activity using a demonstrably valid method.

14 Such bias is a subconscious 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.

interest is viewed or information revealed to the analyst expected to form an opinion as to the activity, identity or perform any comparison. [15, 16]

e. Ensure that all relevant information in relation to image processing undertaken by a third party is communicated to the person undertaking the comparison.[17]

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

g. 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. [18]

8. Validation of Methods

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 operation has an impact [19] in obtaining results are to be validated as part of that validation of the method.

8.1.2 Validation studies shall be conducted as set out in the Codes, and shall include where relevant, but not limited to:

a. Determining the end-user's requirements;

---

15 The forensic unit commissioned to do the work may be able to insulate the analyst conducting the examination by having a different individual involved in the contract review and case conference. This should ensure that the analyst receives only the information appropriate for each stage of the examination, while still ensuring that proper case assessment can be made and that the most appropriate techniques are used.

16 Experts in sole practice should consider how to advise prospective customers as to whether phased disclosure of the details of the case to them is appropriate, and how this will be managed.

17 Information on image processing is required to understand processing artefacts. Procedures should ensure the analyst receives information appropriate for each stage of the examination, including identifying when information on image processing is required.

18 For example, with comparison of facial images derived from uncooperative/uncontrolled settings (i.e. CCTV), facial feature classification, photo anthropometry/proportional alignment and superimposition/overlaying are all questioned in the scientific literature for both inculpatory and exculpatory purposes. The validation would need to take into account the issues raised, and even if the method is demonstrated to not exhibit the issues raised in the literature, the issue that the generic of method has been challenged in the scientific literature must be disclosed.

19 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.

b. Determining the specification;
c. Risk assessment of the method;
d. A review of the end-user's requirements and specification;
e. Setting the acceptance criteria;
f. The validation plan;
g. The outcomes of the validation exercise;
h. Assessment of acceptance criteria compliance;
i. Validation report;
j. Statement of validation completion; and
k. Implementation plan.

8.1.3 The Regulator has issued guidance on performing method validation. [11] [12]

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 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 9.1.1 Photo/Videogrammetry).

8.3.2 Forensic units shall review the scientific literature to identify the following.

a. The scientific basis for the method.
b. Studies critical of the method.
c. Examples of testing methodologies.
d. End-user requirements to be included in the validation, including avoiding any biasing effect of the observer (including juror).

e. Reproducibility of finding (including any verbal confidence scale).
f. False inclusion/exclusion rates.

8.3.3 Image comparison methods which are cited in the scientific literature as unreliable or biased should not be used unless comparable research and validation indicates the issues identified are now controlled. Irrespective of the findings of any such study, the fact that the method was criticised remains disclosable and should be addressed in the statement/report, with the remedial actions that address the issues.

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; and
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

9.1.1 The Codes require that a forensic unit performing testing is required to evaluate measurement uncertainty, even where the test method precludes rigorous evaluation of measurement such as a test that is qualitative in nature.

9.1.2 The impact uncertainty may have on the finding shall be included in both factual and evaluative reports to the Criminal Justice System where it is relevant.

9.1.3 Only two example methods are included here, all analytical methods are in scope for this requirement (see also 11.2 Analytics and Tools).

Photo/Videogrammetry [20, 21]

9.1.4 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.

Derivation of Date/Time/Framing Rate

9.1.5 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 as well as other factors such as measuring the frame rate shall be employed. This method will take account of the whole recording process (image capture, image encoding, metadata assignment, data storage).

9.1.6 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.
e. The image capture rate may not be fixed so a calculated average framing rate cannot always be applied to a single specific frame interval.
f. The frame rate 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.

---

20 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.

21 Empirical research current at the time of this issue indicates photo anthropometry/proportional alignment should not be used in facial comparison involving images from an uncooperative/uncontrolled setting (i.e. CCTV) until methods advance and further research indicates the issues identified are now controlled.

h. What is displayed might not correspond to what is stored. For example, a CCTV system may display an on-screen clock with second precision whereas the data stored on the unit may actually be stamped with millisecond precision.

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

9.1.7 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 a holistic view of the accuracy of the derived times/rates. Test recordings cannot confirm the accuracy of the recording at the time of an incident, but can be used to provide an estimate of uncertainties provided the assumption is stated that the recording device was operating in the same manner as at the time of recording.

9.1.8 If the method includes analysis of output from variable rate cameras, the validation and estimate of measurement uncertainty shall include this use.

10. Control of Data

10.1 Recovery of Data

10.1.1 The overarching requirement of the control of data procedure is to able to show that the recovered footage is true to the original video recording, and remains so from the point of recovery; in practice a bit-for-bit copy of the original with a method to show it has not been tampered with. [13] Video footage should be extracted in its native format [22] in order to maintain image quality and be stored as a master copy. [23]

[22] Some systems may provide an option to write the sequence to standard playable format such as .VOB or .AVI, which may seem to be an advantage in that the video will be replayable using standard software; however the generation of the playable formats often requires the video to be recompressed, resulting in a loss of quality, and so this method should be avoided at the initial recovery stage.

[23] Although due for revision, guidance contained in the Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0 remains relevant. [26]

10.2 Inadvertent Overwriting by Digital Video Recorders

10.2.1 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, particularly if new disk or clone is then subsequently connected, rendering the video inaccessible by that machine; this should only be performed by a competent individual as part of a validated method.
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, and connection of clones may result in the original HDD being 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.

10.3 Creation of a Master and Working Copies

10.3.1 A master exhibit of the source/original data shall be preserved, the forensic unit should define in the procedure what constitutes a master. [24]

10.3.2 Working copies of the video footage may be produced and these will typically be either:

a. A bit for bit copy of the master in its native format, suitable for further analysis by specialists instructed by either the prosecution or the defence;

[24] Write-once discs, with sufficient protections against tampering and information on continuity, are typically used as master discs. However, if the intention is to use a USB stick or CD/DVD only as a transport medium and to store the master evidence on a secure server then the methodology would require validated steps to demonstrate that the copy remains as recovered (e.g. the validated method may include generation of a hash value at the point of creation on the server).

b. A bit for bit copy of the master in its native format, supplied with a player suitable for investigating officers to view the footage; or

c. A "playable" format suitable for investigating officers to view the footage and potentially for supplying to the CPS marking this as "Converted Format" and therefore no longer a true copy of the original.

10.3.3 Any media produced whereby original data has been converted to a different format should be clearly marked as "Converted Format", or identifiable as such in some other way defined in the procedure.

10.4 Conversion to Broadcast Video

10.4.1 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. Therefore, any media produced whereby original data has been converted to a different format should be conspicuously marked or identifiable as such in some other way defined in the procedure (see section 10.3 Creation of a Master and Working Copies).

10.5 Wifi Enabled Courts

10.5.1 Court Wifi systems intended for displaying material such as static images and documents may be considered adequate for the majority of cases. However, caution should be exercised when using wireless presentation systems for displaying video material, particularly in cases where there is lots of movement or high-resolution footage. In such cases, there is a risk of lost frames, jitter, or loss of resolution. If replay through wireless systems is identified as inadequate, provision of appropriate playback equipment in court should be sought; if these arrangements are not already in place the forensic unit should discuss this with the instructing authority. [25]

[25] For forensic units instructed by the prosecution, the CPS Complex Casework Unit may need to be engaged and/or CPS caseworkers may outline requirements via EPPE.Enquiries@cps.gov.uk, a minimum of two weeks' notice is advisable.

10.5.2 The forensic unit should ensure that any material produced that would not be suitable for display via a wireless presentation system is conspicuously marked as such.

11. Computers and Automated Equipment

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; export should be in native format where possible and this native format is what should be used to create the master copy. [26]

11.1.2 Many CCTV players will distort the original recorded material by light, colour, shape and size. They may also not display all frames, or playback recorded audio. They may also detail a timecode and frame rate that is calculated during playback and may not be frame accurate. Any use of a player, either in review, or to achieve a task should be considered and tested. 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 (see glossary entry for Replay Software).

11.2 Analytics and 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 forensic unit shall be aware of the impact of video quality on performance. Video analysis tools shall be validated as part of the method they are deployed in, the risk analysis of the actual PD and FAR on the required task shall be undertaken as part of that validation and communicated to the customer.

---

[26] USB sticks are typically considered to be a transport media only, however see section 10.3 Creation of a Master and Working Copies for exceptions.

12. Test Reports, Statements and the Presentation of Evidence

12.1 General

12.1.1 The Codes give general instruction on reporting requirements. [14] [15] One requirement is that compliance or non-compliance [27,] with the Code of Conduct [28] shall be disclosed in statements/reports from all practitioners that are intended for use as evidence. [29, 30] The Code of Conduct requires compliance with the quality standards set out by the Regulator in the Statement of Standards and Accreditation Requirements.

12.2 Statements and Reports

12.2.1 Practitioners shall understand the distinction between expert evidence and evidence of fact and be aware of the relevant legal requirements in preparing statements or reports.

12.2.2 The Regulator has issued a Regulatory Notice by setting out specific principles based on case law which apply when presenting opinion in relation to image enhancement and/or comparison. [8]

12.2.3 Guidance setting out the legal requirements for non-expert technical statements [14] and expert reports [15] has been issued by the Regulator.

---

27 Non-compliance is considered to be information that could significantly detract from the credibility of a witness and may have a bearing on reliability. In England and Wales, disclosure of such matters is not restricted to experts as made clear by the Criminal Procedure and Investigations Act 1996, R v Ward [27] and Kumar v General Medical Council [28]). Disclosure of this sort of issue is not to restricted to experts instructed by the prosecution (see Criminal Practice Direction V 19B (1) 13 and Criminal Procedure Rules 19.3 (3)(c)). Similar requirements are in place in other UK jurisdictions e.g. Criminal Justice and Licensing (Scotland) Act 2010.

28 The Codes of Practice and Conduct are made up of three distinct sections, the Code of Conduct, Statement of Standards and Accreditation Requirements and the Code of Practice.

29 This does not apply to a Streamlined Forensic Report 1 (SFR1) as is not intended to be used as evidence.

30 In England and Wales.

12.3 Displaying Images

12.3.1 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.

12.3.2 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.

12.4 Interpretation

12.4.1 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).

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

12.4.2 In the case of bulk viewing, there should be consideration of PACE Code D and the competence of the person who prepares the material for viewing shall be assessed to ensure that the risk of errors are minimised.

12.5 Multiple Evidential Approaches

12.5.1 Where the expert has undertaken several forms of analysis (e.g. height analysis and the comparison of physical features) the report shall 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.

12.6 Defence Examinations

12.6.1 Forensic units instructed by the defence shall ensure that any tests or examinations they conduct are carried out in accordance with the requirements set out in the Codes and this appendix. These forensic units shall they also comply with any conditions attached by the prosecutor to the release of the exhibits, or parts of exhibits, or evidential material recovered from them.

12.6.2 The forensic unit appointed by the prosecution shall have defined policies and procedures to facilitate access by defence examiners to carry out a review of the work already completed by the forensic unit in the relevant case.

12.6.3 The forensic unit appointed by the prosecution shall make available to the defence's forensic unit only what has been deemed by the prosecutor or court to be relevant. Where footage is released, if possible it should be in its native format, usually as a copy of the master version, unless masking of additional individuals is ordered.

12.6.4 The defence forensic unit shall use material supplied by the prosecution forensic unit only for the specific purpose and case(s) for which the material was provided. The defence's forensic unit shall retain the notes and records it has created in line with these Codes, material supplied by the prosecution forensic unit supplied by the prosecution may be required to be returned or copies destroyed.

12.6.5 Any policies and procedures for access shall be based on appropriate guidance in the jurisdiction of the case. [16]

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.gov.uk.

14. References

[1] Forensic Science Regulator , "Codes of practice and conduct for forensic science providers and practitioners in the Criminal Justice System," [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 22 07 2020].

[2] International Organization for Standardization, General requirements for the competence of testing and calibration laboratories, BS EN ISO/IEC 17025:2017.

[3] International Organization for Standardization, Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence, BS ISO/IEC 27037:2012.

[4] Forensic Science Regulator, “Codes of Practice and Conduct, Appendix: Digital Forensic Services,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 22 07 2020].

[5] Forensic Science Regulator, “Cognitive bias effects relevant to forensic science examinations,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 22 07 2020].

[6] International Laboratory Accreditation Cooperation, “Modules in a Forensic Science Process, ILAC G19:08/2014,” [Online]. Available: http://ilac.org/latest_ilac_news/ilac-g19082014-published/. [Accessed 22 07 2020].

[7] Forensic Science Regulator, “Codes of Practice and conduct, Appendix: Speech and Audio Forensic Services,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 22 07 2020].

[8] Forensic Science Regulator , “FSR Regulatory Notice 01/2019, Image Enhancement and Image Comparison: Provision of Opinion,” [Online]. Available: www.gov.uk/government/publications/image-enhancement-and-image-comparison-provision-of-opinion. [Accessed 03 08 2020].

[9] Home Office, “Police and Criminal Evidence Act 1984 (PACE) codes of practice,” 23 02 2017. [Online]. Available: www.gov.uk/government/publications/pace-code-d-2017. [Accessed 22 07 2020].

[10] R. v. Cooper [1998] EWCA Crim. 2258.

[11] Forensic Science Regulator, “Method validation in digital forensics,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 04 08 2020].

[12] Forensic Science Regulator, “Validation” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 04 08 2020].

[13] Crown Prosecution Service, “Legal guidance, exhibits: Video recordings,” [Online]. Available: www.cps.gov.uk/legal-guidance/exhibits. [Accessed 22 07 2020].

[14] Forensic Science Regulator, “Forensic Science Regulator legal guidance: Non-expert technical statements,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 22 07 2020].

[15] Forensic Science Regulator, “Forensic Science Regulator legal guidance: Expert report content,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 22 07 2020].

[16] Crown Prosecution Service, “CPS Guidance for Experts on Disclosure, Unused Material and Case Management,” [Online]. Available: www.cps.gov.uk/legal-guidance/cps-guidance-experts-disclosure-unused-material-and-case-management. [Accessed 22 07 2020].

[17] Forensic Science Regulator, “FSR Regulatory Notice 01/2019, Image enhancement and image comparison: provision of opinion,” 17 07 2019. [Online]. Available: www.gov.uk/government/publications/image-enhancement-and-image-comparison-provision-of-opinion. [Accessed 22 07 2020].

[18] Facial Identification Scientific Working Group, “Facial Comparison Overview and Methodology Guidelines,” [Online]. Available: https://fiswg.org/documents.html. [Accessed 22 07 2020].

[19] A. Towler, D. D. White and R. Kemp, “Evaluating training methods for facial image comparison: The face shape strategy does not work,” Perception, vol. 43, no. 2-3, pp. 214-218, 2014.

[20] S. Ritz-Timme, P. Gabriel, Z. Obertovà, M. Boguslawski, F. Mayer, A. Drabik, P. Poppa, D. De Angelis, R. Ciaffi, B. Zanotti, D. Daniele Gibelli and C. Cattaneo, “A new atlas for the evaluation of facial features: Advantages, limits, and applicability,” International Journal of Legal Medicine, vol. 125, no. 2, pp. 301-306, 2011.

[21] R. Moreton and J. J. Morley, “Investigation into the use of photoanthropometry in facial image comparison,” Forensic Sci.ence International, vol. 212, no. 1-3, pp. 231-237, 2011.

[22] K. F. Kleinberg and P. P. Vanezis, “Variation in proportion indices and angles between selected facial landmarks with rotation in the Frankfort plane,” Medicine, Science and the Law, vol. 47, no. 2, p. 107–116, 2007.

[23] A. Strathie, A. Mcneill and D. White, “In the Dock: Chimeric Image Composites Reduce Identification Accuracy,” Applied Cognitive Psychology, vol. 26, no. 1, pp. 140-148, 2012.

[24] A. Strathie and A. McNeill, “Facial Wipes don’t Wash: Facial Image Comparison by Video Superimposition Reduces the Accuracy of Face Matching Decisions,” Applied Cognitive Psychology, vol. 30, no. 4, pp. 504-513, 2016.

[25] R. v. Atkins & Atkins [2009] EWCA Crim. 1876.

[26] Home. Office, “Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0,” [Online]. Available: www.gov.uk/government/publications/cctv-guidance. [Accessed 22 07 2020].

[27] R v. Ward [1993] 1 W.L.R. 619; [1993] 2 All E.R. 577; (1993) 96 Cr. App. R. 1.

[28] Kumar v. General Medical Council [2012] EWHC 2688 (Admin).

15. Glossary, Abbreviations and Acronyms

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. 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 [31] 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

Closed-Circuit Television (CCTV) 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.

---

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

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 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.

Forensic Unit

A term used in ILAC-G19 to mean “a legal entity or a defined part of a legal entity that performs any part of the forensic science process”. It is interchangeable with provider. However, it is used in this document as these are small teams or sole practitioners that for accreditation purposes may be

considered separate legal entities in larger organisations, forensic science providers and police forces.

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

a. 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. Type/s of electromagnetic radiation employed in the formation of the image i.e. visible light, near-infrared

e. Shadows and halation effects;

f. Viewing on different equipment; and

g. 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. [8] An expert in facial comparison is not necessarily competent to give an opinion on vehicle identification without demonstrating specific competence in that activity using a demonstrably valid method. It is a core principle that any expert shall confine themselves to their own sphere of expertise. Therefore, in some instances, it may be that two

experts are required. An expert in imagery may be required to analyse and interpret the imagery, taking account of all of the technical considerations and artefacts and ensuring the court is aware of any limitations that the imagery presents for subsequent comparison. Unless that expert also has demonstrable expertise in the subject matter requiring comparison, then there would be no legal basis on which they could give expert evidence of comparison. For example, an imagery expert is unlikely to be able to comment on how rare or common an observation of a particular type of clothing may be, or could potentially miss the significance of a very subtle difference between two trainers, which an expert from Adidas would be able to differentiate between two models. Likewise, if the expert from Adidas were to perform a comparison without being aware of technical issues in the imagery, they could misinterpret an apparent difference between two trainers that was actually caused by a video artefact. It may be, in some instances, that a single expert has both sets of expertise, but in all instances, experts shall be careful to confine themselves to presenting opinion in only their own area of expertise.

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 with relevant specific subject matter expertise involving ‘expert-based interpretation’:

a. Image processing/enhancement;

b. Image comparison (of objects or individuals);

c. Chronology of events;

d. Authentication;

e. Photogrammetry, particularly 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. The methodology used should be clear and normally should include the Analyse,

Compare, Evaluate, Verify, Report (ACE-VR) methodology that is used for other types of comparisons to control cognitive bias. If multiple experts from different backgrounds and using different equipment find the same feature, then confidence may be improved that the feature exists.

b. 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 system will usually also include proprietary replay software that has been developed and distributed by the system's manufacturer. 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, if conducting further analysis other than viewing, the examiners shall 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) that may affect such analysis.

It should be noted that there may not be obvious signs when replay software is performing incorrectly, so where the footage is to be used for further analysis rather than simply viewing it is good practice is to follow the dual approach, and to document any reason why this has not been possible or relevant in the case.

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; and

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 sometimes made 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 should be considered. Examiners should satisfy themselves that the footage can be relied upon and/or shall ensure that any caveats are clearly made.

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