Forensic Science Regulator

Overseeing Quality

Codes of Practice and Conduct

Appendix: Digital Forensic Services

FSR-C-107

Issue 2

Contents

1. Introduction

1.1.1 Forensic units [1] providing digital forensic science services shall comply with the Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System (the Codes) [1] and where required by the Statement of Standards and Accreditation Requirements within the Codes, be accredited to ISO17020 [2] for any inspection or testing activity at the scene of incident or ISO17025 [3] for any laboratory function (such as the recovery or imaging of electronic data away from the scene of incident or investigation).

1.1.2 Standards such as ISO27037 [4] 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 This appendix provides further explanation of some of the requirements of the Codes specifically pertaining to the provision of digital analysis.

1.1.4 This appendix should be read alongside the Codes with any relevant appendices, the relevant international standards (ISO17020 or ISO17025) and the International Laboratory Accreditation Cooperation (ILAC) publication Modules in a Forensic Science Process, ILAC-G19 [5].

2. Scope

2.1.1 This appendix covers digital forensics work as it applies to identification, capture, preservation, investigation, evaluation, reporting.

3. Implementation

3.1.1 This document became effective on 22 September 2020.

4. Modification

4.1.1 This is the second issue of this document.

[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.

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. [2]

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. Technical Records

5.1.1 The provider shall carry out policies and procedures, appropriate to the device and/or scope of the planned activity, which incorporate:

a. Keeping a record of the state, mode and physical condition of any seized device and any potentially relevant information; and

b. Labelling the components of the device and taking photographs (screen, computer front and back, and the area around the device to be seized) and/or sketching the device's connections and surrounding area where relevant.

[2] 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, 1.1.4, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 7.1, 7.1.1, 7.1.2, 7.2.4, 7.3.2, 9, 9.1, 9.1.1, 9.2, 9.2.1, 11, 12. The following footnote has been amended: 2.

5.1.2 A contemporaneous audit trail shall be retained, to show all changes to the records without obscuring the original record. It shall be possible to associate all changes to data with the person having made those changes, e.g. by the use of timed and dated (physical or electronic) signatures. Reasons for the changes shall be given.

5.1.3 The provider shall ensure that an audit trail is created and preserved for all processes or methods applied to computer-based electronic evidence, to the extent that an independent third party would be able to examine and repeat the processes and achieve the same result.

6. Test Methods

6.1 Selection of Methods

6.1.1 A method is logical sequence of operations or analysis which may include the use of software, hardware and tools.

6.1.2 The provider shall take account of the need for backup and redundancy when working on cases, to ensure that a single technical failure (e.g. a power loss or disk corruption) will not result in the loss of data on working copies.

6.1.3 Software, hardware and tools, where operation of these has an impact in obtaining results will require validation within the method they are deployed, or any existing validation to be verified, as laid out in Section 6 below.

6.1.4 The provider shall ensure that, for the range of the digital forensics methods it uses, the validation requirements take account of staff competency levels, the nature and difficulty of the tasks to be carried out, and the level of acceptability of the method in the wider forensic science and criminal justice community.

7. Validation of Methods

7.1 General

7.1.1 The general requirement is that all technical methods and procedures used by a forensic unit shall be validated. This section details the principles of the requirement for validated methods, the Codes detail the required processes; this appendix builds upon those requirements, it does not replace them.

7.1.2 The Codes require the validation procedure to include consideration of the following:

a. Determining the end-user's requirements;

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.

7.1.3 The end goal of validation is for the user of the method (the forensic unit), and the user of any information derived from it (the end user), to be confident about whether the method is fit for purpose as well as understanding any limitations. The ability to assess if a method is fit for purpose depends on first defining what the forensic unit needs the method to reliably do, as well as identifying who are the end users of the method and subsequent results.

7.1.4 The Regulator has issued general guidance on validation [6] as well as more specific guidance on method validation in digital forensics. [7]

7.2 Risk Assessment of a Method

7.2.1 The risk assessment process detailed in the Codes is intended to used be to determine the impact of the overall method used. It is important to look at how a method or tool is to be used. For instance, when imaging storage media, the risks may include:

a. Writing on the evidential machine storage;
b. Returning incomplete and/or misleading data; or
c. Incorrectly determining the media to be unreadable.

7.2.2 In certain parts of the process, the competent use of a suite of software tools or the use of visual/manual checks could be demonstrated to mitigate the identified risks in the method. Proper consideration of the nature of risks at this stage should feed into the development of a method as well as into the validation strategy.

7.2.3 The development of the forensic science process and the subsequent validation shall set out how the identified risks are being addressed and how the effectiveness of the method will be tested along with the end-user requirements.

7.2.4 A formal risk assessment method should be used. There are various risk assessment methods that may be chosen, one which may be suitable is called failure modes and effects analysis [6] [8]. Failure modes and effects analysis is a step-by-step approach for analysing each stage of a method looking for potential weakness that might result in a failure of some sort, with consideration of if the failure were to occur, would it be detected without causing harm e.g. an erroneous result being picked up by a quality control.

7.2.5 Whichever risk assessment method is used, inclusion of cross referencing between the stage in the procedure and the risk assessment table, and identifying what controls are to be assessed during validation ensures the testing is focussed. It also provides documentation to support the requirements set out in in 7.2.3.

7.3 Validation of Measurement-Based Methods

7.3.1 The Codes describes validation for measurement and interpretive methods. For the purposes of digital forensics, the section referring to measurement-based methods is applicable. This includes methods where direct measurements are not made, such as extraction processes using automated tools or manual methods for the purpose of providing data.

7.3.2 Any of the functional and performance requirements listed in the Codes for validation of measurement-based methods be applicable. However, it is expected that the following requirements taken from the list in the Codes shall normally be given particular consideration for software or digital applications:

a. The competence requirements of the analyst/user;

b. Environmental constraints;
c. The ability of the sampling process to provide a representative sample of the exhibit, e.g. indecent images (item f. in the list in the Codes);
d. The results are consistent, reliable, accurate, robust and with an uncertainty measurement, e.g. time stamps (item l. in the list in the Codes); and
e. The limitations of applicability (item n. in the list in the Codes).

7.4 Verification of the Validation of Adopted Methods

7.4.1 In most cases adopted methods or software tools and scripts should follow a tailored process for the validation of measurement-based methods. However, an adopted method would normally be expected to be already well supported through documentation, available validation studies, testing-house studies or published papers. In this case the Codes require confirmation of the applicability of the validation and a documented demonstration that a method works within acceptable performance parameters.

7.4.2 There is a requirement in the Codes for the production of an available library of documents relevant to the authorisation of a method and the production of a certificate of validation completion.

7.4.3 The final requirement in the Codes is to demonstrate that a method works in the hands of the intended users.

7.5 Verification of Minor Changes in Methods

7.5.1 Methods are validated to a specific configuration; therefore any changes in any of the constituent parts (hardware, firmware, script, operating system, etc.) may affect its overall operation and any dependant systems, which could invalidate the results.

7.5.2 Any proposed change shall be risk assessed at the method level as even a patch in a software tool may adversely affect the operation of a second tool or process using its output, e.g. giving a plausible but incorrect date stamp. Other examples include a tool inadvertently becoming write-enabled through a firmware update.

7.6 Implementation Plan and Any Constraints

7.6.1 The implementation plan is required to include monitoring of controls and communication that in the digital forensic sciences shall include configuration management, dependencies, how identified software/firmware/hardware bugs are to be handled and how patches, etc. are to be controlled.

8. Handling of Test Items

8.1 Exhibit Handling, Protection and Storage

8.1.1 The provider shall consider whether the value of any other type of evidence (e.g. fingerprints) that may be present could be compromised during the capture, preservation and investigation of the digital evidence.

8.1.2 The provider shall ensure that devices containing potential digital evidence are packaged, sealed and transported in such a way as to protect the integrity of the digital evidence.

8.1.3 There are two main issues to consider in the transporting of digital evidence:

a. The security of the device and digital evidence to ensure that access to it is correctly supervised when moving it from the scene to the laboratory or other location; and
b. Protection of the device and digital evidence to ensure that it is not affected by physical shock, electromagnetic interference, extremes of heat and humidity or other environmental hazard.

9. Reporting

9.1 General

9.1.1 Reports to investigators or to courts may be:

a. Factual, produced by technical staff acting as witnesses; or
b. Evaluative, including an interpretation and/or opinion by staff competent to provide expert evidence.

9.2 Declarations of compliance and Non-compliance with Required Standards

9.2.1 The Regulator's Code of Conduct requires compliance with the quality standards set out by the Regulator in the Statement of Standards and Accreditation Requirements. The Codes require that all practitioners shall disclose in statements/reports intended for use as evidence, their compliance, or non-compliance, with the Code of Conduct. The Codes detail specific requirements for reporting, and the Regulator has issued the following guidance.

a. Non-Expert Technical Statement Guidance, FSR-G-225. [8]
b. Expert Report Guidance, FSR-G-200. [9]

10. Review

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

10.1.2 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

11. 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 30 07 2020].

[2] International Organization for Standardization, Conformity assessment — Requirements for the operation of various types of bodies performing inspection, ISO/IEC 17020:2012.

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

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

[5] International Laboratory Accreditation Cooperation, "Modules in a Forensic Science Process, ILAC-G19:08/2014," [Online]. Available: http://ilac.org/news/ilac-g19082014-published/. [Accessed 30 07 2020].

[6] Forensic Science Regulator, Guidance: Validation, FSR-G-201, Forensic Science Regulator.

[7] Forensic Science Regulator, "Method Validation in Digital Forensics," [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 03 08 2020].

[8] Forensic Science Regulator, "Non-Expert Technical Statement Guidance, FSR-G-225," [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 03 08 2020].

[9] Forensic Science Regulator, "Expert Report Guidance, FSR-G-200," [Online]. Available: www.gov.uk/government/collections/fsrlegal-guidance. [Accessed 30 07 2020].

12. Glossary

Method

A logical sequence of operations, described generically for analysis or for comparison of items to establish their origin or authenticity.

Forensic Unit

The term is used to include all providers of forensic science, whether commercial, public sector or internal to the police service (e.g. scenes of crime, fingerprint bureau).

Uncertainty of Measurement

The estimation of the uncertainty of measurement is a Codes and accreditation requirement and is based upon the principle that all measurements are subject to uncertainty and that a value is incomplete without a statement of accuracy.

Sources of uncertainty can include unrepresentative samples, rounding errors, approximations and inadequate knowledge of the effect of external factors.

Validation

The process of providing objective evidence that a method, process or device is fit for the specific purpose intended.

Verification

Confirmation, through the assessment of existing objective evidence or through experiment that a method, process or device is fit (or remains fit) for the specific purpose intended. The provider must demonstrate the reliability of the procedure in-house against any documented performance characteristics of that procedure.

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