Forensic Science Regulator

Overseeing Quality

Codes of Practice and Conduct

Appendix: Digital Forensic Services

FSR-C-107

Issue 1

Contents

1. INTRODUCTION

1.1.1 The provider of digital forensic science (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/IEC17020:2012 for any crime scene activity and BS EN ISO/IEC17025:2005 for any laboratory function (such as the recovery or imaging of electronic data).

1.1.2 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 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, BS EN ISO/IEC17025:2005 and the International Laboratory Accreditation Cooperation (ILAC) publication *Guidelines for Forensic Laboratories,* ILAC-G19[1], 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 digital forensics work only as it applies to the identification, capture, preservation, investigation, evaluation, reporting and storage of data on digital data storage devices and mobile phone devices.

3. IMPLEMENTATION

3.1.1 This appendix is available for incorporation into a provider's quality management system from the date of publication. The Forensic Science Regulator (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.

[1] Available from: https://www.ilac.org/documents/g19_2002.pdf [Accessed 8/8/14]

4. MODIFICATION

4.1.1 This is the first issue of this document.

5. TECHNICAL RECORDS (ISO/IEC17025:2005, 4.13.2)

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.

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 (ISO/IEC17025:2005, 5.4.2)

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 Risk Assessment of a Method

7.1.1 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.

7.1.2 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.

7.1.3 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 Validation of Measurement-Based Methods (the Codes, 20.8)

7.2.1 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.

7.2.2 Any of the functional and performance requirements listed a–m in paragraph 29 in Section 20.8 of the Codes may be applicable. However, it is expected that the

following requirements taken from the list in Section 20.8.2 of 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 original list);

d. the results are consistent, reliable, accurate, robust and with an uncertainty measurement, e.g. time stamps (item l. in the original list); and

e. the limitations of applicability (item n. in the original list).

7.3 Verification of the Validation of Adopted Methods (the Codes, 20.10)

7.3.1 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.

7.3.2 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.

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

7.4 Verification of Minor Changes in Methods

7.4.1 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.

7.4.2 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.

7.5 Implementation Plan and Any Constraints

7.5.1 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 (see Section 6.4).

8. HANDLING OF TEST ITEMS (ISO/IEC17025:2005, 5.8)

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. REVIEW

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

9.1.2 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

10. 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]

11. GLOSSARY

Method

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

Provider

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 BS EN ISO/IEC 17025:2005 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
https://www.gov.uk/government/organisations/forensic-science-regulator

ISBN: **978-1-78246-492-1**