Forensic Science Regulator
Overseeing Quality

Codes of Practice and Conduct

Appendix: Digital Forensic Services

FSR-C-107-001

Consultation Draft

This is a consultation draft and therefore should not be regarded or used as a standard. This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. Comments should be sent to FSRConsultation2@homeoffice.gsi.gov.uk using the form available from http://www.homeoffice.gov.uk/agencies-public-bodies/fsr/ and should be submitted by 10 MARCH 2013. This mailbox is not for general correspondence and is not routinely monitored so no acknowledgement will normally be sent.
THIS DRAFT IS NOT CURRENT BEYOND 10 MARCH 2013.

1. INTRODUCTION

1.1.1 The provider of digital forensic science (the provider) shall comply with the Codes of Practice and Conduct (the Codes) and be accredited to BS EN ISO/IEC 17020:2004 for any crime scene activity and BS EN ISO/IEC 17025:2005 for any laboratory function (such as the recovery or imaging of electronic data).

1.1.2 This appendix provides further explanation of some of the requirements of the Codes specifically pertaining to the provision of digital analysis.

1.1.3 This appendix should be read alongside with the Codes, BS EN ISO/IEC 17025:2005 and ILAC-G19 and will generally follow the heading titles used in the Codes with cross references to ISO 17025:2005 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. TECHNICAL RECORDS (ISO 17025:2005, 4.13.2)

3.1.1 The provider shall include in 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 legible photographs (screen, computer front and back, and the area around the device to be seized) and/or sketching of the device's connections and surrounding area where relevant.

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

3.1.3 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.

4. TEST METHODS AND METHOD VALIDATION

4.1 Selection of methods (ISO 17025:2005, 5.4.22)

4.1.1 With consideration of any instructions from the customer the provider shall consider, in the context of each specific case and the type of evidence being sought (e.g. photographs, spreadsheets, documents, databases, financial records), the potential value of obtaining:

a. Additional information regarding the case (e.g. aliases, e-mail accounts, e-mail addresses, ISP used, names, network configuration and users, system logs, passwords, user names);additional digital evidence (e.g. by sending a preservation order to an Internet Service Provider (ISP), identifying remote storage locations, obtaining e-mail); and

b. The relevance of peripheral components to the investigation (for example, in forgery or fraud cases, non-computer equipment such as laminators, credit card blanks, cheque paper, scanners, and printers; in child pornography cases, digital cameras).

4.1.2 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 loss of data on working copies.

4.1.3 Software, hardware and software tools whose operation has an impact in obtaining results will require validation, or any existing validation to be verified, as laid out in section 5, Validation of methods.

4.1.4 The provider shall ensure that, for the range of digital forensics tools 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 acceptance of the tool in the wider forensic science and criminal justice community.

5. VALIDATION OF METHODS

5.1 Risk assessment of the method

5.1.1 The risk assessment process detailed in the Codes is intended to determine the impact of the overall method and the operation of deployed software tools in the digital forensic science process may have. It is important to look at how the how the method or tool is to be used, the configuration and to systematically look at the types of risk that might occur. For instance, when imaging storage media, the risks may include:

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

5.1.2 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 the method as well as the validation strategy.

5.1.3 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 action will be tested along with the end-user requirements.

5.2 Validation of measurement based methods (Codes, 20.8)

5.2.1 Measurement based methods can include extraction processes using automated tools or manual methods for the purpose of providing data.

5.2.2 Any of the functional and performance requirements listed a-m under paragraph 29 in this section of the Codes may be applicable, however it is expected that the following from the list in section 20.8.2 of the Codes shall normally be given greater consideration for software or digital applications:

a. The competence requirements of the analyst/user;
b. Environmental constraints;

...

f. The ability of the sampling process to provide a representative sample of the exhibit;

l. The results are consistent, reliable, accurate, robust and with an uncertainty measurement; and

m. The limitations of applicability.

5.3 Verification of the validation of adopted methods (Codes, 20.10)

5.3.1 In most cases adopted methods or software tools and scripts should follow a tailored process for the validation of measurement based methods. However, as an adopted method would normally be expected to be already well supported through documentation, available validation studies, testing-house studies or published papers much of the required work may only require verifying as detailed in the Codes.

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

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

5.4 Verification of minor changes in methods

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

5.4.2 Any proposed change should 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 at tool inadvertently becoming write-enabled through a firmware update.

5.5 Implementation plan and any constraints

5.5.1 The implementation plan is required to include monitoring of controls and communication which in the digital forensic sciences should include configuration management, dependencies, how identified software/firmware/hardware bugs are to be handled and how patches etc. are to be controlled (see Verification of minor changes in methods).

6. HANDLING OF TEST ITEMS (ISO 17025:2005, 5.8)

6.1 Exhibit handling, protection and storage

6.1.1 The provider shall ensure that the value of any other type of evidence that may be present is not compromised during the capture, preservation and investigation of the digital evidence.

6.1.2 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.

6.1.3 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.