



GUIDELINES FOR BEST PRACTICE IN THE FORENSIC EXAMINATION OF DIGITAL TECHNOLOGY

Contents

This Document, which can be regarded as a Quality Assurance "core" document, is divided into the following sections:

1. AIMS/GOALS
2. SCOPE
3. QUALITY ASSURANCE
 - 3.1. Introduction
 - 3.2. Personnel
 - 3.3. Competence requirements
 - 3.4. Proficiency Testing
 - 3.5. Documentation
 - 3.6. Equipment
 - 3.7. Validation
 - 3.8. Physical Work Space
 - 3.9. Audit
4. ASSESSING THE CASE EXAMINATION REQUIREMENTS
5. GENERAL PRINCIPLES APPLYING TO THE RECOVERY OF DIGITAL EVIDENCE
 - 5.1. G8 Recommendations
 - 5.2. Documentation
 - 5.3. Responsibility
6. PRACTICES APPLICABLE TO DIGITAL EVIDENCE EXAMINATIONS
7. LOCATION AND RECOVERY OF DIGITAL EVIDENCE AT THE SCENE
 - 7.1. Anti-Contamination Precautions
 - 7.2. Searching the Scene
 - 7.3. Collecting the Evidence
 - 7.4. Packaging, Labelling and Documentation
8. PRIORITISATION
9. EXAMINATIONS
 - 9.1. Analysis Protocols
 - 9.2. Case Records
10. EVALUATION AND INTERPRETATION
11. PRESENTATION OF WRITTEN EVIDENCE

12. CASE FILE REVIEW

12.1. Technical Review

12.2. Management/Administrative Review

13. PRESENTATION OF ORAL EVIDENCE

14. HEALTH AND SAFETY

15. COMPLAINTS PROCEDURE

16. REFERENCES AND BIBLIOGRAPHY

17. APPENDIX

FOREWORD

It is recognised that the diversity in personnel, experience and equipment available in the Forensic IT sections of various forensic science laboratories and other law enforcement agencies throughout the world makes the task of reaching a consensus of opinion about how examinations involving various types of technology should be carried out, an enormous one. The underlying tenor of the document, however, is to try to raise standards, by offering a source of sound advice, put together by the most experienced practitioners in this field. Time and the rapidly changing technology encountered in casework will require periodic revisions to be necessary.

Each member State is encouraged to consider the following document when establishing procedures for the collection, preservation, examination and use of digital evidence, according to its national law and standards bodies, and to be aware of potential differences when collecting evidence at the request of other States.

IOCE 2002 DIGITAL EVIDENCE STANDARDS WORKING GROUP

1 AIMS/GOALS

- To provide a framework of standards, quality principles and approaches for the detection, preservation, recovery, examination and use of digital evidence for forensic purposes in compliance with the requirements of an accrediting body and or an organization widely recognized in the digital forensic community.
- To encourage more consistent methodology and hence the production of more comparable results, so as to facilitate interchange of data.

2 SCOPE

- The scope of this document covers systems, procedures, personnel, equipment and accommodation requirements involved in the entire forensic process of digital evidence, from examinations at the scene of a crime to the presentation of evidence in court.

3 QUALITY ASSURANCE

3.1 **Introduction** (Each agency should provide an introductory paragraph relating to specific quality assurance issues specific to its organization.)

3.2 Personnel

An individual may be responsible for more than one of the defined roles.

- The person who has overall authority and responsibility for the management and quality of the work carried out in their area of the laboratory and or Unit.
- One who is trained to assess and identify digital evidence at the scene for collection, the first responder.
- One who is responsible in a particular case for directing the examination of the items submitted, interpreting the findings, writing the report and providing evidence of fact and, if necessary, opinion for the court.
- One who has achieved levels of technical competency for specific equipment and services. They are able to write reports/statements of factual information in their specific specialist areas and can provide factual testimony in court. This person can have the authority and responsibility for the technical quality of digital evidence casework when the agency designate is not competent in technical aspects of digital evidence.
- An individual carrying out general casework examinations and/or technical work under the supervision of a reporting officer or a technical specialist and who is able to provide information to assist with the interpretation of the tests.

3.3 Competence Requirements

Competence requirements for all roles listed above should address the following:

- Qualifications, Competence and Experience
 - such as a degree or equivalent years of experience in the field.
- Training and Assessment
 - to ensure an individual's competence on processes and or equipment they use during the forensic process.
- Maintenance of Competence.

3.4 Proficiency Testing

Proficiency Testing is an integral part of an effective quality assurance program. It is one of many measures used to monitor performance and to identify areas where improvements may be needed. Proficiency testing measures the capability of its examiners and the reliability of its analytical results.

All personnel involved in the field of forensic digital evidence/technology examinations should be required to demonstrate their competence at regular intervals.

3.5 **Documentation**

There should be a documented Quality Management System (QMS) for controlling all systems, processes and methods used in the examination and reporting of forensic digital technology/evidence casework.

The QMS should include requirements for the following minimum documentation relating to forensic digital technology/evidence casework to be maintained:

- Standard Operating Procedures
- Training
- Validation of tools
- Physical Work Space
- Equipment Maintenance/Calibration
- Health and Safety
- Evidence Handling Tracking System
- Assessment
- Proficiency Testing
- Report of Findings
- Evidence Seized
- Audits
- Corrective Action Policy/Procedures
- Complaints and conflict resolution

3.6 **Equipment**

All equipment used during forensic casework should be suitable for its purpose and maintained in a fully operational condition.

3.7 **Validation**

Only properly evaluated tools, techniques and procedures should be used for the forensic examination of digital technology and the interpretation of their evidential significance in the context of the case.

Validation requires as a minimum that:

- there is a minimum acceptable criteria for the technique or procedure;

- the critical aspects of the examination procedure and tools have been identified and the limitations defined wherever possible;
- the methods, materials and equipment used have been demonstrated to be fit for its purpose;
- there are appropriate quality control and quality assurance procedures in place for monitoring performance;
- the technique or procedure is documented;
- the results obtained are reliable and reproducible.

3.8 **Physical Work Space**

Laboratories and or forensic workspace for the examination of digital technology items should be designed and equipped for efficient, secure, safe and effective use. Particular attention needs to be given to the management of the variety of trailing electrical cables and environmental conditions.

3.9 **Audit**

Audits of the quality system should be conducted in a timely manner.

4 ASSESSING THE CASE EXAMINATION REQUIREMENTS

- 4.1 It is essential to understand the case examination requirements and the associated legal authority. This should be expressed in terms of what the requestor is seeking to establish rather than a menu of tasks to be carried out.

- 4.2 It is also helpful in planning the work in any case to establish the requestor's priorities, time scales by which results/responses are required and whether there are any constraints (e.g. preservation of material for other purposes such as fingerprint examination, custody time limits, cost, etc.) to be taken into account.

5 GENERAL PRINCIPLES APPLYING TO THE RECOVERY OF DIGITAL EVIDENCE

- 5.1 The general principles, that have been adopted as G8 recommendations relating to digital evidence, that should be followed by forensic laboratories are as follows:
- A. *The general rules of evidence should be applied to all digital evidence.*
 - B. *Upon seizing digital evidence, actions taken should not change that evidence.*
 - C. *When it is necessary for a person to access original digital evidence that person should be suitably trained for the purpose.*
 - D. *All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.*
 - E. *An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.*
- 5.2 All activity relating to the seizure, examination process, and presentation of evidence must be documented, preserved and available for review.
- 5.3 Responsibility for maintaining evidential value and provenance is a personal, not corporate issue. If an individual has acknowledged responsibility for an item by signing an access log they are responsible for all actions taken in respect of that item until such time as it is returned to store or formally transferred to another individual.

6 PRACTICES APPLICABLE TO DIGITAL EVIDENCE EXAMINATIONS

- 6.1 Whatever the specific practices employed in digital evidence recovery they should fall within a defined and accepted framework and must comply with the principles stated above.
- 6.2 Policy regarding jurisdictional practices should be documented whenever possible as Standard Operating Procedures (SOP) and included in a training program.
- 6.3 Each agency should establish an SOP that would include seizure, storage, and examination procedures.

7 LOCATION AND RECOVERY OF DIGITAL EVIDENCE AT THE SCENE

Forensic personnel may need to attend the scene or may need to give advice to others attending the scene and recovering the evidence. They should be aware of any relevant jurisdictional guidelines.

7.1 Anti-Contamination Precautions

7.1.1 Appropriate anti-contamination precautions should be taken to minimise any chance of accidental contamination of items, which may subsequently be required for other laboratory examinations, e.g. fingerprints, DNA.

7.1.2 Consideration of what anti-contamination precaution to take should be based not only on the digital evidence media and devices, but also on the other evidence types which may be potentially available. If these include materials, which may be required for DNA analysis, extreme caution should be taken because of the sensitivity of current DNA techniques, including the wearing of barrier clothing such as disposable scene of crime suits, gloves and face masks.

7.1.3 All equipment, sampling materials and storage and transportation containers should be new, preferably disposable, or cleaned thoroughly before and after use.

7.1.4 Additionally, care should be taken, when handling evidence to document any suspicion of the presence of potentially dangerous or sensible substance on the material (narcotics, poison, explosives etc...)

7.2 Searching the Scene

7.2.1 All scenes, indoor, outdoor or those involving vehicles, should be protected at the earliest opportunity to reduce the risk of loss, movement or damage to digital evidence.

7.2.2 Legal, technical and appropriate jurisdictional guidelines need to be followed.

7.2.3 Scenes should be searched systematically and thoroughly for digital evidence and related material, targeting and prioritising areas, which in the context of what has been alleged are most likely to contain material of evidential significance.

7.3 Collecting the Evidence

7.3.1 It is vital that items for forensic examination are preserved securely as soon as possible following appropriate jurisdictional practices.

7.3.2 Where practicable, the items should be examined in the laboratory or forensic work space rather than at the scene.

7.3.3 Where it is impracticable to recover the items for examination, the digital evidence may have to be copied at the scene according to SOPs.

7.4 Packaging, Labelling and Documentation

7.4.1 A record should be made, at the time of seizure of items from the scene, or from the suspect(s) or victim(s), describing the exact locations from where the items were recovered. It is also helpful to mark this location on a sketch/plan of the scene or person.

7.4.2 Evidence should be properly packaged and sealed when seized.

7.4.3 Agency policy on evidence handling and security must be followed.

7.4.4 Each package should be labelled at the time of seizure. While the legal status and use of labels can vary, the minimum details that should be recorded and be directly and unequivocally attributed to each package are:

- a unique identifying mark
- the name of the person and organisation (e.g. police force, technical department, etc.) responsible for collecting and packaging the material
- a brief description of the material (e.g. laptop computer, serial numbers)
- the location from where and from whom the material has been seized
- the date and time the material was seized

8 PRIORITISATION

8.1 Consideration should be given to the following before commencing any examinations for digital evidence:

- the urgency and priority of the customer's need for information and time constraints
- the other types of forensic examination which may have to be carried out on the same items
- which items have the potential to provide the most information in response to the various propositions
- which items offer the best choice of target data, in terms of evidential value,

8.2 After the assessment of case requirements, the examination will be assigned to the appropriate qualified individual.

9 EXAMINATIONS

Any anti-contamination precautions or requirements of the particular case (e.g. presence of narcotics, poisons, explosives, etc.) must be considered before any examination proceeds, and the minimum precautions are identified and implemented.

All items submitted for forensic examination should first be reviewed for the integrity of their packaging. Any deficiency in the packaging should be documented.

All personnel involved in examinations should take adequate precautions to preserve any evidentiary material from external factors such as electrical hazards or static.

9.1 Analysis Protocols

9.1.1 The agency should establish an SOP for analysis of digital evidence.

9.2 Case Records

9.2.1 The exact requirements for recording casework information will depend on the policy and any requirements of the member agency/country. As a minimum, however, the records should be in sufficient detail to allow another examiner, competent in the same area of expertise, to be able to identify what has been done and to assess the findings independently. Case records should include both administrative and examination documentation. Whenever appropriate standardised forms should be used to document examinations.

9.2.2 For example, casework involving digital evidence should include details of case records such as notes, work sheets, photographs, printouts, charts, spectra and other data or records which support findings should be generated during the course of the examination, and kept.

10 EVALUATION AND INTERPRETATION

- 10.1 Evaluation and interpretation of the case findings will require consideration of the background information available about the case and the original expectations formulated during case assessment.

11 PRESENTATION OF FINDINGS

- 11.1 The purpose of the report is to provide the reader with all the relevant information in a clear, concise, structured and unambiguous manner, to make the task of assimilating the information as easy as possible.
- 11.2 Reports should include factual findings and may include interpretation and expert opinion. Expert opinion and interpretation should be clearly identified in the report. Oral evidence may also subsequently be required.
- 11.3 The style and content of written reports must meet the requirements of the criminal justice system for the country of jurisdiction.

12 CASE FILE REVIEW

All work undertaken should be subjected to both technical and administrative review.

12.1 Technical Review

Technical review should be conducted by a qualified agency designee. It should include consideration of the validity of all the critical examination findings and all the raw data used in preparation of the statement/report. It should also consider whether the conclusions drawn are justified by the work done and the information available. The review may include an element of independent testing, if circumstances warrant it.

A written record of the technical review should be made and retained with the case records.

12.2 Administrative Review

Administrative review should be carried out by a qualified agency designee. It should ensure that the requester's needs have been properly addressed, editorial correctness and adherence to policies.

13 TESTIMONY

- 13.1 Witnesses should provide testimony regarding the content of their statement/report, and their area of expertise. Witnesses should advise the court when responding to questions that will take them outside their field of expertise.

14 HEALTH AND SAFETY

- 14.1 All elements of an agency's health and safety program should be clearly documented. The health and safety program should be continually monitored and documented by designated agency representatives.
- 14.2 Health and safety considerations are extremely important in all of the work carried out at all stages of the forensic process. Personnel engaged in the examination of various forms of digital technology should operate in accordance with the regulations of the agency.

15 COMPLAINTS PROCEDURE

- 15.1 Each agency should have a procedure dealing with complaints or anomalies. This procedure should minimally include investigating the complaints or anomalies, taking corrective actions, assuring personnel are aware of their responsibilities and reporting on the findings.

16 REFERENCES AND BIBLIOGRAPHY

Interpol Computer Crime Manual – 1992-2001

ACPO Good Practice Guide for Computer based evidence, Issue 2, 1999

Bibliography - Quality Assurance

Qualitative analysis: A Guide to Best Practice, ISBN 0 85404 462 0, Royal Society of Chemistry, Cambridge, 1998.

The Scenes of Crime Handbook, 2nd edition, The Forensic Science Service, 1994 (currently under review)

Standard Practice for Receiving, Documenting, Storing and Retrieving Evidence in a Forensic Science Laboratory, ASTM E 1459-92

ILAC Guidelines for Forensic Science Laboratories, (Draft 1.3), International Laboratory Accreditation Co-operation, July 1999

General Requirements for the Competence of Testing and Calibration Laboratories, ISO/IEC 17025, International Organisation for Standardisation, 1999

Standard Guide for the Recovery of Trace Evidence, Technical Working Group for Materials, Quantico, VA, 1998

Quality Management and Quality Assurance Standards - Part 1 : Guidelines for selection and use, ISO 9000-1, International Organisation for Standardisation

Accreditation Criteria for Forensic Science Laboratories, Issue 3, National Association of Testing Authorities, 1998

PT-001-A1 June 1998 Guidance on the Conduct of Proficiency Tests and Collaborative Exercises within ENFSI, European Network of Forensic Science Institutes Yearbook, 1998-1999

-ISO 8402:1994 Quality management and quality assurance-Vocabulary.

-ISO/IEC: 1997 guide 4 3-1. Proficiency test by interlaboratory comparison Part 1: development and operation of proficiency testing schemes

-ISO/IEC: 1995 guide 30 Terms and definitions used in connection with reference materials.

17 APPENDIX

DEFINITIONS (TO BE ADDED)