



Working group Forensic IT www.enfsi.org

<u>GUIDELINES FOR BEST PRACTICE IN THE FORENSIC EXAMINATION OF DIGITAL TECHNOLOGY</u>			
DOCUMENT TYPE :	REF. CODE:	ISSUE NO:	ISSUE DATE:
GUIDLINES	FIT-2005-001	006	20/04/09

Contents

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

- 1. AIMS**
- 2. SCOPE**
- 3. QUALITY ASSURANCE**
- 4. ESTABLISHING THE CUSTOMER REQUIREMENT**
- 5. CASE ASSESSMENT**
- 6. PRIORITISATION AND SEQUENCE OF EXAMINATIONS**
- 7. GENERAL PRINCIPLES APPLYING TO THE RECOVERY OF DIGITAL EVIDENCE**
- 8. PRACTICES APPLICABLE TO DIGITAL EVIDENCE EXAMINATIONS**
- 9. LOCATION AND RECOVERY OF DIGITAL EVIDENCE AT THE SCENE**
- 10. LABORATORY EXAMINATIONS**
- 11. EVALUATION AND INTERPRETATION**
- 12. PRESENTATION OF WRITTEN EVIDENCE**
- 13. CASE FILE REVIEW**
- 14. PPRESENTATION OF ORAL EVIDENCE**
- 15. HEALTH AND SAFETY**
- 16. COMPLAINTS PROCEDURE**
- 17. REFERENCES AND BIBLIOGRAPHY**

REVISION HISTORY

The main content of this document was agreed in 2003 by the ENFSI Forensic IT Working Group. Version 4 was edited by Eric Freyssinet (ICGRN) and dr. Les Russell (Forensic Science Service – UK). The working group is grateful for all the hard work they put into generating the first version of these documents.

The latest version of this document was discussed at the ENFSI FIT working group meeting held by the Guardia Civil on 1st-3rd October 2008 in Madrid. The final editing by dr. David Compton (Forensic Science Service – UK).

1 AIMS

- 1.1 To provide a framework of standards, quality principles and approaches for the detection, recovery, examination and use of digital evidence for forensic purposes in compliance with the requirements of ISO/IEC 17025 and ILAC G19:2002, as interpreted for forensic science laboratories.
- 1.2 To provide a systematic approach for ENFSI member laboratories and other Law Enforcement forensic units to establish and maintain working practices in the field of digital evidence that will deliver reliable results, maximise the quality of information obtained and produce robust evidence.
- 1.3 To encourage more consistent methodology and hence the production of more comparable results, so as to facilitate interchange of data between laboratories.

2 SCOPE

- 2.1 This document is mainly focused on the requirements for the recovery of data from the following digital devices :
 - Computer Related Media - hard disks, USB drives, smart media, flash memory, floppy discs and other storage media such as Zip, Jaz or Optical disks, Tapes and CD-ROMs.
 - Mobile Phones
 - Telecommunication data (e.g. Cell Site Analysis)
 - Card Skimming devices
 - digital devices associated to cars (e.g. GPS devices and car electronics)
- 2.2 However, the document stills related to requirements for other digital evidence casework and examination requests such as :
 - Live Forensics – recovery of data from RAM memory in computers or recovery of data across a network.
 - Gather evidence from computer peripheral devices (such as tape streamers, removable hard disks etc.) and other devices with digital storage capability (e.g. cameras, various consumer goods)
 - Establish the functionality of a piece of software or a machine e.g. could a system be used for phone cloning?

- Sequencing the events that have occurred within a computer to say if a particular act occurred before another.
 - Recovery of information from personal organisers (PDAs), and other portable (embedded systems) or office technology.
 - Reading and deciphering magnetic stripes on plastic cards.
 - Analysis of Smart cards
 - Capture and analysis of system involving media media.
- 2.3 The scope of this document covers procedures, personnel, equipment and accommodation requirements involved in the entire forensic process, from examinations at the scene of a crime to the presentation of evidence in court

3 QUALITY ASSURANCE

3.1 *Introduction*

The ENFSI Board wishes to promote consistent and reliable evidence through the whole forensic process, from scene of crime to court. As one part of this aim, it is the policy of the Board that all member laboratories should have achieved, or should be taking steps towards, ISO/IEC 17025 for their laboratory testing activities. The ILAC G19:2002 can be used as a guidance to implement this standard in Forensic Sciences Laboratories. For activities other than the testing part of the forensic process e.g. work at the scene of crime, ISO/IEC 17020 can be implemented as the standards used to achieve accreditation. The scope of accreditation should aim to include the frequently performed examination at the individual member laboratories

3.2 *Definitions*

- 3.2.1 For digital forensic terminology please refer to “SWGDE and SWGIT Digital & Multimedia Evidence Glossary” (<http://www.swgde.org/documents.html>). SWGDE has agreed for ENFSI FIT WG to refer to these definitions to provide consistency between organisations.
- 3.2.2 The following definitions used within the forensic community have been used throughout this document:
- *Audit* - a systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether

these arrangements are implemented effectively and are suitable to achieve objectives. [ISO 8402: 1994 - 4.9]

- *Competence* - a person's qualification for and ability to do, the job by virtue of their education, training and/or experience and demonstrated knowledge, skills and abilities.
- *Competence Test* - a formal assessed check of an individual's performance against a pre-determined expected outcome for specific examinations, measurements or procedures using material of known provenance.
- *Management/Administrative Review* - review of a case file and report to ensure that the customer's needs have been properly addressed, compliance with laboratory policy and, for the report, editorial correctness.
- *Proficiency Test* - the use of inter-laboratory comparisons to determine the performance of individual laboratories for specific tests or measurements and to monitor laboratories' continuing performance. [ISO/IEC guide 43-1 Proficiency test by inter-laboratory comparison - Part 1: Development and operation of proficiency testing schemes : 1997]
- *Quality Assurance* - All the planned and systematic activities implemented within the quality system, and demonstrated as needed, to provide adequate confidence that an entity will fulfil the requirements for quality [ISO8402 : 1994 - 3.5].
- *Quality Control* - Operational techniques and activities that are used to fulfil the requirements for quality [ISO8402 : 1994 - 3.4].
- *Raw Data* - the record of results of analysis and examinations in the form in which those results were interpreted by the original analyst.
- *Scientific/Technical Review* - review of a case file and report for the reliability and interpretation of the scientific findings.
- *Systematic Error* - any discrepancy due to improper instrument function or setting.
- *Contact Trace Material* - referring to the forensic discipline involving any of the following materials: fibres, hairs, glass, paint, soil.
- *Validation* - Confirmation by examination and provision of objective evidence that the particular requirement for a specific intended use are fulfilled [ISO 8402 : 1994 - 2.18].

3.3 *Personnel*

- 3.3.1 Due to variations in the size of different laboratories and variability within different laboratory systems, absolute standardization cannot be achieved. As a result an individual may be responsible for more than one of the defined roles.

The key roles recognised for digital evidence units in laboratories are :

Section Head/Operations Manager - the person who has overall authority and responsibility for the management and quality of the work carried out in their area of the laboratory. This person's responsibilities may include providing a non-technical review of individual cases.

Reporting Scientist - the forensic scientist/officer 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 opinion for the court.

Technical Specialist - a forensic scientist/officer who has achieved levels of technical competency for specific equipment and services. They are able to write reports and 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 Section Head/Operations manager is not competent in technical aspects of digital evidence.

Analyst/Assistant - an individual carrying out general casework examinations/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

- 3.3.2 In the event that no personnel in the laboratory are competent to be the forensic digital evidence technical specialist on specific cases or specific technical aspects, arrangements should be made for a qualified and competent consultant to be retained from outside the laboratory to perform these duties, until this situation can be remedied. The external consultant should have similar roles within their organisations and be able to demonstrate their technical competency to the same standards required within the laboratory.

3.4 *Competence requirements*

3.4.1 Qualifications, Competence and Experience

The qualifications, competences and experience that individuals require to carry out the various aspects of forensic examinations involving digital technology will depend on the demands of the various aspects of the work.

The following qualifications and areas of competence would be expected as the minimum standard for the key roles in forensic digital evidence examinations :

Section Head/Operations Manager - a minimum of a degree (or equivalent) in a science or engineering discipline, with skills to manage the resources to process casework efficiently and effectively and develop staff.

Reporting Scientist - a minimum of a degree (or equivalent) in a science or engineering discipline, or acceptance as an expert in the field through peer review and publication, knowledge of and ability to demonstrate the theories, technology and procedures applicable to the examination of digital technology (hardware and software); competence in the evaluation of digital evidence from casework; and knowledge and experience of the requirements and procedures of the criminal justice system for the presentation of evidence, both written and oral as an expert witness.

Technical Scientist - a minimum of a Degree (or equivalent) in a natural or applied science, or peer acceptance as an expert in the field of digital evidence/technology through experience and publication; a high level of knowledge of the relevant technology and procedures applicable to the examination of digital technology (hardware and software); extensive experience in the field and proven competence in the evaluation of results and conclusions in cases involving digital evidence

Analyst/Assistant - qualifications in a natural or applied science; knowledge of the theories, technology and procedures applicable to the examination of digital technology (hardware and software), the practical skills to operate specialist equipment and to carry out examinations safely and reliably in compliance with laboratory protocols; and an understanding of the requirements of the criminal justice system.

3.4.2 Training and Assessment

3.4.2.1 Laboratories should have written standards of competence for each role, a documented training programme and processes for assessing that the trainee has achieved the level of competence required.

3.4.2.2 The training should be carried out within a specified time frame and the outcome of the assessments should be documented on the individual's training record.

3.4.2.3 The assessment of competence can be accomplished through a combination of appropriate means, including:

- practical tests which can include field work
- written and oral examinations

- ‘moot/mock’ court exercises
- casework conducted under close supervision
- a portfolio of previous casework

N.B Please refer to the ENFSI document QCC-CAP-003 “Performance Based Standards for Forensic Practitioners” for more details (<http://www.enfsi.eu/page.php?uid=46>)

3.4.2.4 Each trainee should be recognised as competent following successful completion of an assessment exercise as specified before being allowed to undertake independent case work.

3.4.2.5 All personnel involved in the field of forensic digital evidence/technology examinations should maintain their competency and evidence in support of this should be available for periodic review which will include that date on which competence was reconfirmed.

3.4.2.6 All personnel should have adequate approved training in the use of electronic equipment

3.4.3 Maintenance of Competence

3.4.3.1 *Reporting Scientist, Analysts and Assistants*, should:

- participate actively and routinely in casework examinations involving digital technology
- provide a portfolio of evidence demonstrating a participation in cases involving digital technology/digital evidence
- read journals, books and other literature containing pertinent information relating to forensic digital evidence examinations.
- Take part in appropriate workshops, seminars, meetings, training courses and Research and Development projects.
- Is up to date with any technical procedures or international standards.

3.4.3.2 *Section Heads/Operations Managers* should:

- keep abreast of current developments within the digital technology/evidence field that could improve operational efficiency or the evidential value of casework, nationally and internationally.

3.4.3.3 *Technical Scientists* should actively participate in forensic casework involving digital technology/evidence and keep abreast of any published work containing pertinent information relating to digital technology and digital evidence. They should also participate annually in at least one of the following :

- Research & development
- Publication of a technical paper related to digital technology/evidence in a recognised forensic journal
- Presentation of a paper at a professional meeting/seminar
- Technical training events as a presenter/instructor
- The work of an organisation dealing with the technical advancement of digital technology examinations in a forensic environment

They should also routinely communicate the relevance of selected forensic topics within the digital technology/evidence team of the laboratory.

3.5 Proficiency Testing

- 3.5.1 Proficiency testing relates to the systems within the laboratory, but may also provide some information on the competence of individual participating in the tests.
- 3.5.2 The forensic digital technology/evidence team of the laboratory should participate in at least one proficiency test each year. Participants in the test should follow the laboratory's/unit's standard procedures for casework. They should not give the test any special treatment that would not be given in the same circumstances to casework.

N.B – At the time of writing the number of independent proficiency tests in the field of digital forensic is small. In addition, relevant test take significant effort to set up. Therefore, it is recognised that it may not be practical to carry out test for every digital forensic area in a year. Laboratories are encourage to work together in generating sharing tests.

- 3.5.3 [ENFSI Laboratories only] The design and implementation of the proficiency tests should be carried out in accordance with the recommendations of the ENFSI Guidelines on the Conduct of Proficiency Tests and Collaborative Exercises.
- 3.5.4 The Team Leader/Ops Manager should ensure that the test is completed in a timely manner, and that the following test data and information is collected and returned to the proficiency test co-ordinator, or other designated individual, for evaluation:
- the proficiency test unique identifier
 - the identity of the participant
 - the dates of examination and completion
 - copies of all data sheets and notes
 - copies of all charts, graphs and printouts
 - the results and conclusions
- 3.5.5 The proficiency test co-ordinator, or other designated individual, should review all the test documentation and compare the results from the test with the expected

result based on information from the supplier of the test in a timely manner. The co-ordinator should provide a written summary report for each proficiency test to the participants and/or other appropriate individuals as determined by laboratory policy.

- 3.5.6 [ENFSI Laboratories only] Any incorrect results should be notified by the organiser of the proficiency test to the laboratory QA Manager and Team Leader as soon as possible. After discussion of the problem appropriate corrective action should then be implemented either in conjunction with the ENFSI FIT Working Group or within the laboratory in question. The QA Manager should consider the points laid down in sub-section 4 of the ENFSI Guidelines on the Conduct of Proficiency Tests (QC-PT-001). It is the responsibility of the labraority to ensure that the corrective actions are completed.
- 3.5.7 Any deficiency in a proficiency test result shown to be the consequence of an examination/interpretative error should result in a critical review of that laboratory/unit's systems involved and this may require the individual(s) who produced the discrepant result undergoing re-training as appropriate. The QA Manager, or other designated individual, should also determine the identified shortcoming is sufficiently serious as to warrant the need for review of relevant case work carried out by the individual according to established laboratory practice.
- 3.5.8 The results of all proficiency tests should be maintained at the laboratory according to established laboratory policy.

3.6 *Documentation*

- 3.6.1 The laboratory/unit should have 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.
- 3.6.2 The QMS should include requirements for the following minimum documentation relating to forensic digital technology/evidence casework to be maintained:

Casework

- records of all movements of casework material, for chain of evidence purposes
- records of all communications within the laboratory and with external personnel
- details and results of all examinations/tests carried out
- draft and final statements/reports
- records of case file review
- financial and costing data (if applicable)

Equipment

- inventories of equipment held, records of maintenance operations and names of those persons responsible for them

Protocols and Standard Operating Procedures

- for the examination methods and other processes used
- for quality control
- for recording and presenting results

Knowledge Databases

- Useful background information on technology
- Useful tools to progress casework
- Limitations on examination techniques / tools
- Reference to validation documentations and tests.
- Legal requirements

Training

- competence standards, training programmes and assessment protocols
- training packages
- training/competence records for individuals

3.7 *Equipment*

- 3.7.1 An equipment inventory should be maintained for all significant items held in the forensic digital technology/evidence unit, recording the manufacturer, model, serial number, date of acquisition, date placed in service and location for each piece of equipment.
- 3.7.2 All equipment used during forensic casework must be suitable for its' purpose and maintained in a fully operational condition. For software this relates to different version releases of the same tool. Regular testing of electrical items (safety checks and calibrations) should be carried out and documented.
- 3.7.3 Only appropriate and properly operating equipment (hardware and software version) should be employed in casework, and then only within the limits of its performance check.
- 3.7.4 '*Off the Shelf* ' Hardware Solutions
There are a number of forensic hardware tools offered by commercial companies and these usually come packaged with software. The contract for the purchase of such equipment should ideally include some form of maintenance agreement and it should be established that the company will agree to supply suitably qualified personnel to explain the configuration and purpose of the hardware (via a certificate, or statement) should this prove necessary during the production of

evidential material using their equipment. This agreement may be difficult to obtain where equipment is purchased outside of the country.

3.7.5 *'In House ' Solutions*

For in-house developed solutions version control needs to be implemented with detail records of any changes.

3.8 *Validation*

3.8.1 The laboratory should only use properly evaluated techniques and procedures for the forensic examination of digital technology and the interpretation of their evidential significance in the context of the case. For more details on ENFSI validation requirement refer to QCC-CAG-001 “VALIDATION AND IMPLEMENTATION OF (NEW) METHODS”

3.8.2 Validation requires as a minimum that:

- there is an agreed requirement for the technique or procedure;
- the critical aspects of the examination procedure have been identified and the limitations defined;
- the methods, materials and equipment used have been demonstrated to be fit for purpose in meeting the requirement;
- there are appropriate quality control and quality assurance procedures in place for monitoring performance;
- the technique or procedure is fully documented;
- the results obtained are reliable and reproducible.
- the technique or procedure has been subjected to independent assessment and, where novel, peer review;
- the individuals using the technique or procedure have demonstrated that they are competent to do so.

3.8.3 Where the techniques or procedures have been validated elsewhere, the laboratory should demonstrate that it can achieve the same quality of results in its own hands. With key software tools such as imaging packages, independent assessment could be sought or, failing that, an assurance from the provider that they will support their product in court if necessary.

3.8.4 Software testing procedures should involve identifying its key functions and formulating a test procedure to ensure that it fully meets these requirements. Testing should be documented and re-testing should take place on upgrades when these become available. A software library should be maintained within the laboratory/unit and strict control kept over usage during casework thereby eliminating the use of untested or unauthorised packages

3.9 *Digital Software / Hardware*

- 3.9.1 There are many specialist software tools available for use in the forensic field. Reporting Scientists should ensure that they have a current valid licence to use commercial software.
- 3.9.2 Software used in forensic computing can be broadly divided into three categories: Preservation tools, Data Recovery Tools and Investigation Tools.

3.9.3 *Preservation Tools*

3.9.3.1 Imaging Tools

Disk imaging is now a fairly straightforward process, the key to obtaining an accurate image being the presence of a reliable verification tool. In theory a commercial disk imaging tool, which has the capability to verify the image copy, should be suitable for the purpose of obtaining a forensically sound image. It should also have an inbuilt audit function and produce a process log file. Testing of these disk imaging tools should cover the following areas:

- 1) Checking that the software makes no changes to the evidence/suspect drive
- 2) Checking that the verification process is reliable
- 3) Checking the audit/log function for accuracy and detail
- 4) Where possible, comparing the results with those of another disk imaging product.

3.9.3.2 Data Accessing Tools

Digital devices have a range of interfaces and storage capacities. It therefore may not be possible to image a device directly or it is impractical to generate an image of all the memory (e.g. A complete Network). In these situations solutions are available which allow direct access to the digital data in a write protected mode. For such tools it needs to be demonstrated that their interaction with the device does not change any data. All tests carried out on imaging tools should also be carried out to understand any limitations of the tool.

3.9.4 *Data Recovery Tools*

For main embedded systems devices the only practical solutions for recovering data from the devices is to interact directly with the memory or by installing 3rd party software on the device. In these instances care must be taken to fully understand the implications of accessing the memory direct without any write protection. It is therefore important that the tools are tested to demonstrate that the data important to the investigation is unaffected by the data recovery tools. As the recovery process is controlled by the electronic devices operating system it may not always be possible to get all data back. Therefore the testing of such tools should also make the operator aware of any limitations.

3.9.5 *Investigation Tools*

Investigation tools may consist of commercially available software and any utilities that may either be written to deal with specific problems or else obtained in an unvalidated form (e.g. from the Internet or from other Law Enforcement colleagues).

Because of the dynamic nature of many of the commercial software tools and the fact that some of them can be customised by the user, it would probably be impractical and prohibitively expensive to expect each to be externally accredited. Inter-agency co-operation however, may present an opportunity in identifying tools thought to be suitable and reliable and to share the results of any trials, testing and any deficiencies discovered with the products.

For all other types of software tools, their use should be defined and a regime of testing established for each purpose to ascertain both its suitability and reliability. All testing programmes should be fully documented .

For tools that can be used in a variety of configurations it is particularly important when they are used to document all steps taken in order to produce a process that could be repeated, if necessary, by someone else and give the same result as the original.

- 3.9.6 In the area of digital forensics it is important to ensure that the testing environment is suitable for the examination before any tools are used. In cases where direct access to the chips is required ESD protection is required. For examination of devices which have wireless/mobile connectivity they will need to be examined in a faraday cage or switched to a state which will prevent the data being contamination from outside source (e.g. Network). With current technology a device can be remotely re-set losing data if allow to connect to the network.

3.10 Accommodation

Laboratories for the examination of digital technology items should be designed for efficient and effective working and furnished with furniture and equipment suitable and sufficient for its intended use. Particular attention needs to be given to the management of the variety of trailing electrical cables. Restricted access to the rooms and vision of monitors must be considered if distressing material is being reviewed to minimise exposure to individuals not involved in the case.

3.11 Audit

- 3.11.1 Audits covering all aspects of forensic digital technology/evidence work (casework, research and development, training, etc.) should be conducted at least once a year by an appropriate individual in conjunction with the QA Manager.
- 3.11.2 Where case files are reviewed in audits, they should be chosen randomly taking into account any sensitive issues related to the case.
- 3.11.3 Records of each audit should be kept. They should include the date of the audit, the name of the person conducting the audit, the findings and any corrective actions necessary.
- 3.11.4 All corrective actions should be designated to a nominated appropriate individual for completion by an agreed specified date, and the QA Manager should ensure that the action is completed as agreed.

4 ESTABLISHING THE CUSTOMER REQUIREMENT

- 4.1 It is essential before starting any examination at the scene or in the laboratory to agree with the customer (e.g. the investigating officer) the purpose of the examination. This should be expressed in terms of what the customer is seeking to establish rather than prescribing tasks to be carried out.
- 4.2 It is also helpful in planning the work in any case to establish the customer'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, DNA, custody time limits, cost, etc.) to be taken into account.

5 CASE ASSESSMENT

5.1 *Introduction*

- 5.1.1 Before starting work on any case the Reporting Scientist should carry out an assessment of the information available and the items provided for examination in light of the agreed customer requirement. The Reporting Scientist should, if necessary, clarify requirements with the customer.
- 5.1.2 The Reporting Scientist should also make an assessment of the risk of contamination to both electronic and contact trace evidence before any items provided for examination are submitted to the laboratory, or before examination commences.
- 5.1.3 Where interpretation is required the Reporting Scientist should consider to what extent the proposition put forward by the customer can be tested and should assess whether recovered data could be present due to other circumstances.
- 5.1.4 The Reporting Scientist should consider what they would be expected to find if each proposition were correct and he should make an assessment of the likely evidential value of the anticipated findings. For computer based evidence for example, this would require consideration of the types of data or files involved, the potential for innocent possession, the likelihood of accidental transfer in the proposed circumstances, and the extent to which the significance may be established.

5.2 *Information requirements*

- 5.2.1 In order to gain access to the data stored on a digital device it may be possible to obtain the following information to progress the examination in a speedier manner :
 - PIN/Password
 - Make/Model of device that generate any electronic data
 - Network/equipment configuration
 - Telecommunication data configuration (e.g. Locations of masts, changes to network, Call Data Records)
- 5.2.2 In order to be able to assess the likelihood, for example, of accidental or innocent possession, comprehensive details are required about:
 - what is the suspected or known use of the computer system before, during and after the incident/arrest
 - the persons involved
 - any known sequence or timings of events

- the persons responsible for and the sequence and timing of events in the recovery of items submitted for examination
- 5.2.3 All these issues are considered further in Section 11: Evaluation and Interpretation.

5.3 ***The Chance of Recovery of Digital Evidence***

The opportunity for recovery of digital evidence will depend on many factors, including, the age and condition of the item submitted and the level of any security features applied by the user.

5.4 ***The Potential Significance of Digital Evidence***

It is usually possible to recover data but it may not be possible to state that specific recovered data originated from a particular data source to the exclusion of all others.

For example, the matching of documents may be of very limited evidential value because of the variety of facilities available within word processing, graphics, desktop publishing and other drawing software packages that may generally exist in modern computer systems. However the potential of linking documents with particular printers should not be overlooked.

6 PRIORITISATION AND SEQUENCE OF EXAMINATIONS

6.1 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
- 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

6.2 It is usually preferable to start by searching for the best choice of target data on the items where the finding of target data may have the most evidential significance.

6.3 To minimise the possibilities of contamination it is preferable to examine all items relating to one individual before commencing with items relating to others.

7 GENERAL PRINCIPLES APPLYING TO THE RECOVERY OF DIGITAL EVIDENCE

7.1 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.*

Any agency with powers of search and seizure will have a code of practice or general principles defined in order to protect the best interests of all parties. For example, the UK Police Code B deals with the searching of premises and seizure of property and covers such topics as search records, handling of property, relevance and retention of material. Such codes must always be adhered to when dealing with digital evidence and in addition, current relevant legislation must be taken into account.

B. *Upon seizing digital evidence, actions taken should not change that evidence.*

Wherever possible no actions taken during the seizing of any evidential material should cause that material to be changed and this is of particular importance when dealing with digital evidence which could be seen as prone to accidental ‘tampering’. Where actions have been taken that change the data, this should be fully documented

C. *When it is necessary for a person to access original digital evidence that person should be suitably trained for the purpose.*

Although generally accepted best practice is to take an image copy of digital evidence there may be occasions or examination techniques when a course of action has to be taken that may involve directly accessing the evidence (e.g. traditional phone examination or live forensics). Such action should only be taken by someone suitably trained. ‘Suitable’ training is defined elsewhere.

D. *All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.*

Contemporaneous notes should be kept at all stages of handling digital evidence. Full access records should be maintained and signatures obtained on transfer of material. Procedural notes should be sufficiently comprehensive that the actions they document can easily be reproduced if necessary.

E. *An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.*

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.

8 PRACTICES APPLICABLE TO DIGITAL EVIDENCE EXAMINATIONS

- 8.1 Whatever the specific practices employed in any forensic laboratory they should fall within a defined and accepted framework and must comply with the principles stated in section 7.
- 8.2 Policy regarding local practices should be documented whenever possible as Standard Operating Procedures (SOP) and included in a training programme. It should be regularly reviewed and updated if necessary and should be in an easily accessible and comprehensive format which can be used to support a statement of action taken.
- 8.3 The following is a suggested framework for any SOP document. Guidance on the production of best practise manuals within ENFSI can be found in document QCC-BPM-001 (<http://www.enfsi.eu/page.php?uid=46>)

8.3.1 Recovery Details

The recovery of digital evidence should be fully documented at all stages. A set of stock forms could be compiled to complement the use of contemporaneous notes and ensure that all the required information is recorded consistently. This would typically include serial numbers of equipment being processed, BIOS settings, date, time and place of seizure, hardware and software (including version numbers) used in the processing and details of production media.

8.3.2 Storage

Whilst items are in the custody of the laboratory all care should be taken to ensure that they are suitably stored. Attention should be paid to the environment – temperature, humidity etc. The items should be identified with a non-detachable label or permanent markers indicating their source. They should be kept in a secure environment, preferably with some type of pin-lock and in certain cases, guarding against any potential cross contamination of any physical or electronic evidence. Precautions should be taken to ensure that batteries of electronic devices are kept properly charged. Items should be returned to the custody of the exhibits officer or the person/agency requesting the work as soon as processing is completed.

Other factors to consider regarding the storage of devices which require power to ensure data is not lost (e.g. fax machines losing stored pages after power outage) are non interrupted power suppliers and faraday cages to prevent network communication.

8.3.3 *Examination*

An examination strategy should be agreed upon and documented. This could be reinforced by the use of stock forms to serve as a check list. Suggested steps to be included:

- Assess that an appropriate authority has been obtained to allow a legal examination to be carried out. This may vary for different countries as well as for different data types on a single device (e.g. voice mail).
- Obtain agreement with relevant investigator if a digital device needs to be dismantled or the examination will cause the destruction of the device (e.g. desoldering memory chips from printed circuit board)
- Assess the electrical safety of a device prior to any examination of mains equipment. This would also consider any potential electrical discharges.
- Internal examination of all equipment is essential to check for hidden items, disconnected drives etc.
- Carry out specified pre-processing checks e.g. system date/time, port settings, BIOS geometry etc and complete required documentation.
- Complete processing using tools selected from a library of tested and approved software.
- Maintain contemporaneous notes and complete statements as necessary. Secure items produced from the processes and identify with labelling. Complete required paperwork.

9 LOCATION AND RECOVERY OF DIGITAL EVIDENCE AT THE SCENE

9.1 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 local guidelines followed by their police forces. For example , in the UK, the procedures followed in cases involving computers are defined in the ACPO Good Practice Guide for Computer Based Evidence (Version 5). As a minimum the following should be carried out.

9.2 *Anti-Contamination Precautions*

- 9.2.1 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.
- 9.2.2 Consideration of what anti-contamination precaution to take should be based not only on the digital evidence, 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. Where necessary, precautions should also be taken to ensure that the location in which electronic examination takes place, is free from contamination (for example drugs).

- 9.2.3 Consideration of electronic contamination should be taken into account. For example “always on” wireless networks or telecommunication devices.
- 9.2.4 All equipment, sampling materials and storage and transportation containers should be free from contamination. The use of plastic or paper sacks for storage and/or transportation should be considered. See section 9.5 for packaging information.
- 9.2.5 Additionally, care should be taken, when conditioning evidence to document any suspicion of the presence of potentially dangerous or sensible substance on the material (narcotics, poison, explosives etc...)

9.3 Searching the Scene

- 9.3.1 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.
- 9.3.2 Local police guidelines relating to the search and seizure of evidence needs to be followed. (For example, in the UK the practices and procedures documented in the ACPO Good Practice Guide for Computer Based Evidence are followed when conducting scene examinations for computer systems).
- 9.3.3 Scenes should be searched systematically and thoroughly for evidence, targeting and prioritising areas which in the context of what has been alleged are most likely to contain material of evidential significance.
- 9.3.3 During the search and seizure procedures the suspect and witnesses should be kept away from the electronic material.

9.4 Collecting the Evidence

- 9.4.1 It is vital that items for forensic examination are preserved securely as soon as possible following local police practices. It should be noted that some items of equipment must be switched off at the time of seizure and transportation in order to preserve the data (e.g. navigation equipment). In the UK details are supplied in the ACPO Good Practice Guide for Computer Based Evidence covering the preservation of computer evidence.
- 9.4.2 Where practicable, the items should be examined in the laboratory rather than at the scene.

9.4.3 Where it is impracticable or appropriate (i.e. prevent business continuing to operate) to recover the items for laboratory examination, the ‘system’ may have to be copied at the scene according to local procedures.

9.5 Packaging, Labelling and Documentation

9.5.1 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. Photographs can also be taken, and are especially useful as a reminder of the setup details of computer systems (cables, plugs in or not etc)

9.5.2 All items should be packaged and sealed as soon as they are taken. Plastic bags or containers of an appropriate size should be used so as to avoid the packaging being damaged or the seal broken. Adhesive tape rather than staples should be used for sealing and all corners and gaps in the packaging should be covered.

9.5.3 Once sealed, packages should not be re-opened outside the laboratory. If they are needed for interview purposes, then packages with transparent panels should be used.

9.5.4 Labels should be attached to each package at the time of seizure. Whilst 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 specifying make, model and serial number)
- the location from where and from whom the material has been seized
- the date and time the material was seized

9.5.5 Specific care should be taken with the transportation of digital evidence material, to avoid physical damage, vibrations, and the effects of magnetic fields, electrical static and large variations of temperature or humidity.

10 LABORATORY EXAMINATIONS

- 10.1 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 necessary are identified and implemented.
- 10.2 All items submitted for forensic examination should first be examined for the integrity of their packaging. Any deficiency in the packaging which may compromise the value of a laboratory examination should be grounds for refusal to carry out the laboratory examination.
- 10.3 All personnel involved in examinations of computer systems should take adequate precautions to minimise any risks from electrical hazards or static. Also some items need to be protected from Electro Static Discharge (ESD)
- 10.4 Teams engaged upon the recovery of digital evidence should maintain a set of written procedures particular to their requirements but within the broad framework of an accepted national or international standard. (In the UK, Law Enforcement agencies can follow the principles documented in the ACPO Good Practice Guide for Computer based Evidence and procedures should be available describing how these principles are followed). The relevant local procedures manual should be specific, comprehensive and understood by all members of staff in that unit.

10.5 Analysis Protocols

- 10.5.1 The actual work that is carried out in individual cases should be determined by the requirements of the case and will depend on the value of any other evidence which may be available. A systematic approach should always be adopted, to ensure consistency of delivered services, that they are fit for purpose.
- 10.5.2 Whatever work is done, the examiner/analyst should always use the combination of tools and techniques available that offers the greatest potential for locating and identifying relevant information.
- 10.5.3 The choice of the most suitable casework strategy can only be made at the time of the examination by the forensic scientist (Reporting Scientist or Technical Scientist) involved. Given the same case circumstances, all laboratories would ideally adopt the same analysis protocol, but in practice the extent to which such harmonisation can be achieved may be limited by personal experience, availability of tools or equipment and other factors. The differences in legal systems might also affect the analysis protocol. Therefore this protocol can act only as a guide.

10.5.4 If a new or unknown procedure is to be carried out or a procedure on a unstable media it is good practice to used a reference device first to get familiar with the procedures, especially if data could potentially be lost or damaged.

10.6 Case Records

10.6.1 The exact requirements for recording casework information will depend on the legal system operating in the member country/agency. As a minimum, however, the records should be in sufficient detail to allow another forensic scientist (reporting Officer or Technical Specialist), competent in the same area of expertise, to be able to identify what has been done and to assess the findings independently.

10.6.2 For example, in casework involving the examination of computers or computer media, the records should include details of:

- the items that were submitted to the laboratory, the information accompanying the items on submission and the nature of the work requested
- the method of submission (e.g. by hand, by post, etc.), by whom and on what date(s)
- all movement of casework material within the laboratory system, the person(s) responsible for the movement and the date(s) the movements took place
- the method of return of items (e.g. by hand, by post, etc.), by whom and on what date(s)
- any items or material removed for retention by the laboratory
- all communications within the laboratory and between the laboratory and the police about the case
- all communications between the laboratory and external providers of technical advice
- any suspected or known contamination issues, and any special precautions taken to avoid contamination
- for each item examined, the labelling, method of packaging and integrity of packaging on receipt
- what examinations and analysis have been carried out, when, in what order, where and by whom
- the version of any software tools used in the examination
- all observations made, photographs taken and data located
- all draft final reports or statements generated administrative and technical review, when and by whom

10.6.3 Wherever possible, written records should be made on standardised forms.

11. EVALUATION AND INTERPRETATION

- 11.1 There are a number of ways of reporting the findings of a digital examination and this will depend on the police request and information provided. The following levels of opinion are described by the Association of Forensic Science Providers in the UK in the document “Standards for the Formulation of Evaluative Forensic Science Expert Opinion”
- 11.2 Technical (Factual) Reporting - This is the ‘factual’ reporting of a test outcome based solely on the technical competence of the individual. No inferences / explanations (opinion) are drawn from the test results (observations).
- 11.3 Investigative Opinion - This arises in casework in which explanations are generated to account for observations (the outcome of analytical tests or visual examinations). In some circumstances these explanations may be ranked using estimates of probabilities based upon the knowledge and experience of the expert and taking into account all uncertainties relating to the observations and the framework of circumstances. The provision of an explanation for an observation is termed an investigative opinion.
- 11.4 Evaluative Opinion - An opinion of evidential weight (evaluation of a likelihood ratio), based upon case specific propositions and clear conditioning information (framework of circumstances) that is provided for use as evidence in court. An evaluative opinion is an opinion based upon the estimation of a likelihood ratio.

12 PRESENTATION OF WRITTEN EVIDENCE

- 12.1 The findings and any expert opinion are normally provided in the first instance in written form, as a statement of evidence or a report, for use by the investigator and/or the prosecutor/court. Oral evidence may also subsequently be required.

12.2 The Statement or Report

- 12.2.1 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.
- 12.2.2 The style and content of written evidence must meet the requirements of the criminal justice system for the country of jurisdiction. However, in general, the following should normally be included:
 - the unique case identifier
 - the name and address of the laboratory(s) where the Reporting Officer is employed

- the identity and status/qualifications of the Reporting Officer
- the signature of the Reporting Officer
- the date on which the statement/report was signed
- the date of receipt of the material for examination
- the name and status of the submitter
- a list of the items submitted, identified by source
- a comment relating to the condition of submitted material and its packaging when received, particularly where there is evidence of alteration, either by tampering, damage, contamination or any other means
- details of all relevant information received with, or in addition to the items
- the purpose of the examination, as agreed with the police/customer
- details of the examinations carried out
- the results of the examination
- an assessment of the significance of the results in the context of the information provided
- the Reporting Scientist's opinion, and any findings which may influence it
- comment covering any items not examined, and the reasons for this
- details of any submitted items, or parts of such items, not being returned to the submitter, and the reason for this

12.2.3 For cases involving digital evidence, the statement or report should also specifically include:

- the objectives of the examination for data
- details of the target data sought
- the presence or absence of data found on the various items.
- The effects of the examination on the working order of the device. (e.g. During the examination the item was (partially) dismantled. The laboratory does not have the resources to restore the items to its original state)

13 CASE FILE REVIEW

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

13.2 *Technical Review*

13.2.1 Technical review may be conducted by anyone deemed competent to carry out the task and authorised by the Section Head/Operations Manager. 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.

13.2.2 A written record of the technical review should be made, bearing the signatures of both the reviewer and the reporting officer. This should be retained with the case records.

13.2.3 A standard check sheet for the technical review covering the following points can be helpful in ensuring that all the relevant issues have been addressed:

- is there adequate documentation relating to all the materials (items) examined?
- have all the appropriate examinations been carried out?
- have the relevant procedures been followed?
- are there complete notes on all the target items ?
- is the statement/report accurate and does it refer to all items submitted?
- are the conclusions reached justified and appropriate?

13.3 ***Management/Administrative review***

This will normally be carried out by anyone deemed competent by the Section Head/Operations Manager. It should ensure that the customer's needs have been properly addressed, editorial correctness and adherence to laboratory policies.

14 PRESENTATION OF ORAL EVIDENCE

14.1 It is essential that expert witnesses should restrict their evidence to what they have written in their statement/report, and to matters arising from this or raised in the court which fall within their area of expertise. Expert witness's should resist responding to questions that will take them outside their field of expertise.

15 HEALTH AND SAFETY

15.1 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 pertinent government, environmental, safety authorities and laboratory policy.

15.2 General laboratory safety manuals should be available to all laboratory personnel. These should contain details of how to conduct a risk assessment and how to develop safe systems of work, both at the scene of incident and in the laboratory.

15.3 The risks identified, including working with large quantities of offensive material and the associated safe systems of work should be communicated to all personnel likely to be exposed to the risks. This is especially important when this group includes non-scientists or members of the public (e.g. in court).

- 15.4 The relevant safe systems of work should be documented as an integral part of all standard operating procedures.
- 15.5 Laboratory personnel should be responsible for maintaining their assigned work areas in a safe, clean and orderly manner.
- 15.6 Appropriate safety equipment as outlined in the various procedures, should be made available near the work sites by the laboratory management. It is the responsibility of the laboratory personnel to use them where required.
- 15.7 All staff should be instructed on how to proceed in the event of fire, bomb threats, spillage of hazardous chemical or electrical accidents, etc. and be required to practise these procedures once a year. This practice should be documented.
- 15.8 A designated person should be trained and competent to render “qualified first aid” to those doing casework involving digital technology.

16 COMPLAINTS PROCEDURE

- 16.1 Complaints, possible miscarriages of justice and other anomalies need to be reviewed to identify major issues and trends to be brought to the attention of senior management for action.
- 16.2 The parent laboratory/organisation should investigate all complaints made by any providers of casework or others (e.g. courts) as well as any anomalies relating to the services provided which are brought to its attention. Where appropriate the audit process will be used to assess the extent of any underlying problems.
- 16.3 All customer complaints should be dealt with as quickly, efficiently and effectively as possible. The process should aim to resolve misunderstandings and correct errors, where possible. All complaints should be recorded and investigated either by local or senior management, as appropriate. Where necessary, corrective actions are taken to prevent recurrence of the problem.
- 16.4 Any anomaly which could affect the validity of any results or materials supplied to customers will be dealt with promptly through an Improvement and Corrective Action procedure.
- 16.5 All members of staff are responsible for taking prompt action on any such anomaly which comes to their notice and ensuring that possible implications are reported. The appropriate level of management should ensure that corrective action includes advising customers, recalling reports or items and retesting or re-issuing reports as appropriate.

- 16.6 If such an anomaly is recognised specifically as a result of a proficiency test or Quality Assurance Trial, local procedures described in QMS should be followed with, wherever possible, a time limit applied for resolving the matter.
- 16.7 Any possible miscarriage of justice brought to the attention of a laboratory either by an external body or by a member of staff, must be immediately dealt with in accordance with local QMS procedures covering the Possible or Alleged Miscarriages of Justice.

17 REFERENCES AND BIBLIOGRAPHY

Interpol Computer Crime Manual – 1992-2001

ACPO Good Practice Guide for Computer based electronic evidence, Issue 5, 2008

G8 Proposed Principles For The Procedures Relating To Digital Evidence – produced by International Organization on Computer Evidence (IOCE) <http://www.ioce.org/core.php?ID=5>,

Best Practice for Computer Forensics – Produced by Scientific Working Group on Digital Evidence (SWGDE) http://www.swgde.org/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf

Computer Forensics Procedures and Methods, produced by National Centre for Forensic Science <http://ncfs.org/craiger.forensics.methods.procedures.final.pdf>

Good Practice Guide for Mobile Phone Seizure & Examination, Interpol European Working Party on IT Crime – Mobile Phone Forensic Tools Sub-Group, 2006. <http://www.holmes.nl/MPF/Principles.doc>

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

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

ILAC G19:2002 Guidelines for Forensic Science Laboratories, International Laboratory Accreditation Co-operation, 2002

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

Version 6

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

Validation and Implementation of (New) Methods, European Network of Forensic Science document QCC-VAL-001, 2007.

Performance Based Standards for Forensic Science Practitioners European Network of Forensic Science document QCC-CAP-003, 2004.

Guidance on the Conduct of Proficiency Tests and Collaborative Exercises within ENFIS European Network of Forensic Science document QCC-PT-001, 2005.

-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.

Evett I & Buckleton J, *Some aspects of the Bayesian approach for evidence evaluation*, Journal of Forensic Science Society, 1989, 29, 317-324.

Other Useful Links to Digital Forensic References can be found at:

<http://www.swgde.org/documents.html>

<http://www.swgde.org/otherdocs.html>

<http://www.cftt.nist.gov/index.html>

http://www.forensicswiki.org/wiki/Main_Page

http://www.holmes.nl/MPF/Additional_Information.htm