Best Practice Manual for the Forensic Examination of Digital Technology

ENFSI-BPM-FIT-01

Version 01 - November 2015

With the financial support of the Prevention of and Fight against Crime Programme
European Commission - Directorate -General Home Affairs

Background

This Best Practice Manual (BPM) belongs to a series of 10 BPMs issued by the European Network of Forensic Science Institutes (ENFSI) in November 2015. The series covers the following forensic disciplines:

1. Forensic Examination of Digital Technology
2. Forensic Examination of Handwriting
3. Chemographic Methods in Gunshot Residue Analysis
4. Road Accident Reconstruction
5. Microscopic Examination and Comparison of Human and Animal Hair
6. Fingerprint Examination
7. DNA Pattern Recognition and Comparison
8. Application of Molecular Methods for the Forensic Examination of Non-Human Biological Traces
9. Forensic Recovery, Identification and Analysis of Explosives Traces
10. Forensic Investigation of Fire Scenes which have resulted in Fatalities*
11. Forensic Investigation of Fire Scenes which involve the Clandestine Manufacture of Improvised or Homemade Explosive Devices*
12. Forensic Investigation of Fire Scenes which Involve the Clandestine Manufacture of Illicit Synthetic Drugs*

* *The three specific areas on Forensic Investigation of Fire Scenes (numbers 10 -12) were combined into one BPM 'Investigation of Fire Scenes'.*

In the years 2014 and 2015, so-called Activity Teams have - in parallel - developed the 10 BPMs. The activities were performed within the project 'Towards European Forensic Standardisation through Best Practice Manuals (TEFSBPM)' and co-ordinated by the ENFSI Quality and Competence Committee. The realisation of the BPMs was supported by the Prevention of and Fight against Crime Programme of the European Commission – Directorate General Home Affairs (code: PROJECT HOME/2012/ISEC/MO/4000004278). The core project concept was that the BPMs will enhance the quality of the forensic services available to law enforcement and justice across Europe and thereby encourage forensic standardisation and cross-border cooperation between countries.

ENFSI expects that the issuing of this series will stimulate the improvement of already existing BPMs as well as the creation of new BPMs on disciplines that are not covered yet.

Acknowledgements
Gregory Webb (MPS - UK) with the help and guidance of the following personnel and their respective laboratories: Dr. Andrew Barnes (CAST - UK), Dr. Patrick De Smet (NICC/INCC - Belgium), Dr. Zeno Geradts (NFI – The Netherlands), Ralf Kricsanowits (BKA - Germany), Felix Müller (BKA - Germany), Alex Ribot (UCIF - Spain) and Mikael Lindström / Konstantinos Petrou (Europol) are all thanked for their contributions to the realisation of this BPM.

Official language
The text may be translated into other languages as required. The English language version remains the definitive version.

Further information
For further information about this publication, contact the ENFSI Secretariat. Please check the website of ENFSI (www.enfsi.eu) for update information.

Best Practice Manual for the Forensic Examination of Digital Technology

CONTENTS

1 AIMS

1.1 General

This Best Practice Manual (BPM) aims to provide a framework for procedures, quality principles, training processes and approaches to the forensic examination. This BPM can be used by Member laboratories of ENFSI, and other forensic science laboratories to establish and maintain working practices in the field of forensic IT examination that will deliver reliable results, maximize the quality of the information obtained and produce robust evidence. The use of consistent methodology and the production of more comparable results will facilitate interchange of data between laboratories.

The term BPM is used to reflect the scientifically accepted practices at the time of creating. The term BPM does not imply that the practices laid out in this manual are the only good practices used in the forensic field. In this series of ENFSI Practice Manuals the term BPM has been maintained for reasons of continuity and recognition.

This document has been written as a knowledge base document. It provides technical guidance to aid the design of local standard operating procedures (SOPs) in compliance with local regulatory requirements, and international standards.

The intended aim of this guidance is to provide a helpful bridge between the requirements of international and local regulatory standards, and the actual implementation within each member's laboratory environment.

One of the more important inclusions within this document is the decision to formally recommend that the Forensic IT Working Group only consider validating processes, rather than tools. This is due to the additional complications that may exist when assessing human-based interaction of each unique member of staff.

A detailed description of how this can be applied within the laboratory environment is given in section 6.

In order to ensure the maximum compatibility with the requirements of all member laboratories, the document does not describe in a step-by-step fashion how specific forensic processes should be completed, instead it details the abstract processes, the associated possible risks, and the potential size of errors that may exist.

All forensic analysts should be comfortable in accepting that any real world forensic method / process will contain, to some degree, an unavoidable error element.

The primary goals of this document are to discuss the use of resilient atomic and abstract methods, using accepted forensic (scientific) practices, which help to:

- Promote the use of consistent methodologies;
- Encourage the development of new and novel methods;
- Facilitate information interchange;
- Acknowledge the existence of errors in all forensic methods; and
- Promote methods for use in risk analysis and risk mitigation.

2 SCOPE

2.1 General

This BPM is aimed at experts in the field and assumes prior knowledge in the discipline. It is

not a standard operating procedure and addresses the requirements of the judicial systems in general terms only.

This document primarily focuses on Best Practice in the general field of Information Technology in the form of Computer and Phone based forensics.

The areas addressed are the acquisition and analysis of digital systems, including all aspects of the forensic process from before seizure to final report production and archiving.

Whilst general recommendations are contained within the document they are kept abstract in form, this allows ENFSI laboratories the flexibility to design and implement their own processes based on their individual national requirements concerning laboratory procedures, personnel, equipment and accommodation.

2.2 Document Structure

This best practice guide has been developed under the MP2012 European Monopoly project funding and the layout has been implemented in-line with ENFSI/QCC requirements to ensure a standard format compatible with all the separate forensic disciplines taking part.

To aid in the abstract description of common processes this document makes the broad assumption that the reader is already familiar with standard digital technology, and so will consistently refrain from listing specific types when describing methods and processes.

3 DEFINITIONS AND TERMS

For the purposes of the Best Practice Manual (BPM), the relevant terms and definitions given in ENFSI documents, the ILAC G19 (1) "Modules in a Forensic Science Process", as in standards like ISO 9000, ISO 17000 and 17020 apply.

For general information about Validation, Verification and quality control please refer to the ENFSI document QCC-VAL-002 (2) "Guidelines for the single laboratory Validation of instrumental and Human Based Methods in Forensic Science" which must be consulted in conjunction with this document.

The following definitions and terms used within the forensic community have been used throughout this document:

- *Abstract*[1] – The process of considering something independent of its association or attributes.
  For example: Electronics and programming design methods will utilise black-box and white-box abstractions with mathematical algorithms commonly being expressed in their abstract form such as F(x)=y, A+B=C, Ax=b, etc.
- *Art*[1] – A skill at doing something, typically one acquired through practice.
- *Atomic*[1] – Of or forming a single irreducible unit or component in a larger system.
- *Axiom*[1] – A statement or proposition which is regarded as being established, accepted, or self-evidently true.
  Note: If an axiom is not based on a rigorous proof then there is the potential for the axiom [and everything based upon it] to be untrue.

[1] A number of definitions have been taken from the website http://www.oxforddictionaries.com to ensure definition consistency.

- *Encapsulation*[1] – The process of packing of [bundling] data and functions into a single component (object) [with input and/or output interfaces] which is functionally independent of its surroundings.
  i.e. The functional operation is not affected by its external environment under standard specified operating conditions, including connections to its interfaces
- *Error*[1] – A measure of the estimated difference between the observed or calculated value of a quantity and its true value.
  Note: This error element can itself be atomised into the following two distinct abstract parts:

  1) The Known error (reducible through calibration / compensation); and

  2) The Unknown error (bounded variance / uncertainty).
- *Filter*[1] – Process or assess (items) in order to reject those that are unwanted.
  A filter's characteristic can range inclusively between the bounds of accepting everything and rejecting everything.
- *Function* – Within the context of this document a function describes any action which is carried out by either an automated system and/or an analyst.
  Within this document the following also apply
  Each function must be verified in order to form part of a process which may be validated.
  Functions include:

  a) All human-based (analyst) activity from before seizure to reporting; (including user mapping and filter activities)

  b) All data capture solutions;

  c) All instrument-based (automated) mapping and filter activities; and

  d) All Reporting and Peer Review.

  In the case of forensic tools, the term "function" additionally relates to encapsulated program functions or components (objects) within the tool (e.g. Acquisition, File Mapping, Hashing, Search Filters, Sorting, data transfer, etc.).
- *Mapping*[1] – Associate each element of a set with an element of another set.
  Mappings may be of the form one-to-one, one-to-many or many-to-one.
- *Process*[1] – A series of actions or steps [functions] taken in order to achieve a particular end.

Within this document the following also apply

A process can be composed of one-or-more functions and/or sub-processes.

A process must correlate with the agreed Statement of Requirements in order to be validated.

A process should contain human-based functions in order to check and verify compliance, especially when using instrument-based functions which are not traceable to an external standard.

- *Provenance*[1] – The place of origin or earliest known history of something.
  Note: Provenance relates to how, when and why something came into existence and not just identifying where it currently resides.
- *Raw Data* – Data that has been extracted or acquired in a form that is unmodified by the analytical process.

- *Subjective*[1] – Based on or influenced by personal feelings, tastes, or opinions. *Generally this will be limited to human-based methods, but it may encompass some forms of machine learning algorithms (e.g. results based on the training of neural networks and some adaptive filters).*

For additional digital forensic guidance please refer to the North American SWGDE document "SWGDE and SWGIT Digital & Multimedia Evidence Glossary**"** v2.8 (http://www.swgde.org/documents/).

SWGDE has previously agreed for ENFSI Forensic IT WG to refer to these definitions to provide consistency between organisations.

4 RESOURCES

4.1 Personnel

Due to variations in the size of different ENSFI FITWG laboratories, and the variability of their different laboratory systems, this document refrains from defining an absolute standard for personnel in order to allow local flexibility.

All forensic laboratories shall comply with the ENFSI code of conduct.

Generally a digital forensic unit may consist of 1 or 2 distinct groups of personnel:

- Technical (with administrative responsibilities);
- Administrative only.

This document makes the assumption that all administrative responsibilities will be covered by the laboratories standard ISO/IEC 9001 (or equivalent) requirements, and so makes no attempt to cover this area.

A typical laboratory will generally consist of the following technical personnel:

- Section Heads/Operations Managers;
- Technical Experts;
- Analysts; and
- Assistants

These 4 roles may either be uniquely defined for specific personnel, or be a combination of 2 – 3 roles depending on the construction of each local laboratory.

The qualification requirements for all personnel shall be governed by each laboratory and their national and legal requirement.

It is highly recommended that laboratories give consideration to routine proficiency testing of all technical staff to ensure they retain the technical capability in accordance with their assigned roles. The period between routine proficiency testing is at the discretion of each laboratory, but it should be acknowledged that each proficiency test will typically only cover a small sampled proportion of the actual work undertaken by each staff member (see section 7 Proficiency Testing).

All forensic technical personnel have a direct responsibility to ensure they:

- Comply with national regulatory requirements;
- Are up to date with current technical developments and procedures;

- Understand the requirements of the criminal justice system;
- Maintain 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;
- Provide formal feedback to colleagues on problems encountered during analysis and the method that was employed to overcome it;
- Aid in the development of local procedures and standards and improve the technical advancement of examinations.

They should also take part in appropriate workshops, seminars, conferences, meetings and research and development projects. It is strongly encouraged that all technical staff remain up to date using a combination of training programs that are delivered internally and externally.

Analysts should actively and routinely participate in casework examinations involving digital technology.

Technical Experts should actively participate in casework examinations, and also participate annually in at least one of the following:

- Publication of a technical paper in a recognised peer reviewed forensic journal related to digital technology/evidence;
- Presentation of a paper or specific casework experience at a professional meeting/ seminar;
- Technical training events as a presenter/instructor;
- Routinely communicate the relevance of selected forensic topics within the digital technology/evidence forensic community and the laboratory.

They should also aid the quality management through development and critical peer review of proposed changes to local procedures and standards to improve the technical advancement of examinations within the forensic environment.

4.2 Equipment

An equipment inventory register shall be maintained for all forensic tools (and any associated test equipment) held in the forensic laboratory, recording as a minimum:

a) Manufacturer, model, unique serial number;

b) Date of purchase and date placed in service;

c) Location for each item of equipment; and

d) Maintenance and verification (calibration) status.

Note: The validation standard being accredited to should provide details of any additional minimum inventory elements that must be added to the above list.

Ideally, equipment contained within the inventory register should be separated into 3 distinct types:

a) Electrical/Electronic Test Equipment.

b) Self-contained Computer systems with embedded Firmware.

c) All remaining Hardware and Software.

Note: No distinction is made in (b) & (c) between equipment developed in-house and 3rd party tools since the level of testing will typically be the same.

All equipment (both hardware and software) used for forensic purposes will require formal documentation as to its current association with defined laboratory validated processes. The accompanying documentation should also include the results of the associated risk analysis, and all the results of routine re-verification (or calibration) of all the functions deployed within any validated processes.

To aid review and equipment pre-upgrade analysis, this should include some form of function-to-process matrix which matches specific equipment functions to processes, and each process's validated status.

Where practical, each laboratory may find it useful to maintain a set of reference equipment which can be used to routinely test the correct operation of specific elements of their forensic analysis equipment, and for pre-testing firmware updates before general rollout.

In addition to standard function testing, all electrical items will require regular safety appliance testing to ensure they are electrically sound.

Note: Care should be taken to ensure sensitive equipment is not damaged by the safety testing process.

All equipment used within a forensic laboratory will have a limited effective lifespan, which may be measured in weeks, months or years. The lifespan may be determined in terms of:

- Reliability;
- Ability to source upgrade components;
- Ease of use (including training requirements);
- Connectivity; and
- Performance.

Ultimately the decision on the effective lifespan is determined by each laboratory, but 1 to 5 years is the typical period within which changes in computer performance and system OS's generally becomes noticeable and may be justified by an increase in productivity and efficiency.

Forensic analysis machines should be server or workstation grade, which are designed for operation 24hrs a day 7 days a week, the minimum requirement of which should be:

- Memory with error correction, and optionally redundancy, to minimise the effects of internal storage and communication errors;
- High quality PSUs with high stability and low regulation errors, which maintain accuracy under varying loads;
- High quality onboard power converters and regulation components;
- Sufficient effective cooling for constant operation; and
- Protected by an Uninterruptable Power Supply (UPS).

Digital storage solutions should be capable of handling common requirements such as reliability and fast access times. It is also highly recommended that enterprise grade storage is always considered when designing RAID network storage solutions.

Note: It is impossible to guarantee that any storage solution will operate with 100% accuracy. Enterprise grade equipment incurs a greater cost overhead but is typically rated more reliable than the cheaper consumer devices.

Media acquisition devices must be capable of driving all connected media devices within their quoted manufacturer's voltage and current specifications. Particular care should be taken to ensure the:

- PSU used is capable of supplying a sufficient load with good stability and low regulation errors; and
- Dedicated data cables are used to reduce signal reflection issues.

Note: It is recommended that laboratories formally separate media acquisition devices whose components require additional driver circuitry (e.g. Protocol Converters) from those that only alter existing pin arrangements (e.g. Media Adaptors).

Correctly configured security tools (such as antivirus, firewall) should always be considered, especially when connected to a network to protect analysis machines from rogue software whilst allowing forensic software to function. Routine updates of such tools should also be planned to ensure they remain up-to-date.

It is highly recommended that forensic workstations and network devices be isolated from external networks (e.g. corporate networks, internet), especially when handling evidential material, to help maintain the integrity of investigations.

If custom solutions (see Appendix B) are to be deployed within the laboratory then the initial design and whole-life support should also be factored into any cost calculations.

In the interests of data access and community testing, open standards should always be considered in preference to bespoke in-house or commercial intellectual property (IP) protected standards. This is particularly true for common forensic storage formats where it may be desirable to access the processed data from multiple applications.

Note: Where the use of bespoke solutions is unavoidable then careful consideration should be given to the requirement of converting the final output to an open standard which can then be utilised, and verified, by standard forensic tools and methods. If this is not available then additional specialist function verification will be required if it is to be deployed within a validated process.

There will always be occasions when a locally approved forensic tool is not capable of providing a specific function which is required to complete a forensic analysis. Laboratory procedures should be flexible enough to allow the use of alternative tools but must have in place sufficient policies to ensure that the use of the tool is formally approved and recorded, and that formal analysis of the characteristics of the function(s) used have been tested by a competent member of staff before it is employed.

As an additional precaution it may be prudent to create an additional verified forensic working copy to ensure the tool cannot corrupt the original forensic image.

In situations where data or media needs to be destroyed laboratories should consider the risk and the security requirements when determining the methods for destruction.

4.3 Reference Materials

Within digital forensics, reference equipment and materials will typically fall into 2 families:

- Those which can be sent for regular recalibration to an accredited national (or international) standard.
- Everything else.

In computer based forensics the vast majority (if not all) of forensic reference material will fall under the latter classification. In these cases it is the responsibility of each laboratory to maintain known sanitised reference materials (test sets) which are capable of effectively determining whether, or not, relied upon technical functions used within processes remain within their predefined acceptable error bounds.

The design of strong test sets is a specialist skill which is usually the preserve of specialist test laboratories with staff specifically trained over time to fulfill this function.

It is recognised that within forensic IT laboratories staff tasked with designing and reviewing test sets are unlikely to have received formal training of the required type. Therefore, for all test sets used the ownership of risk and responsibility remains the laboratory's.

It is important that all schedules used to create test sets deployed within the laboratory are documented and retained permanently.

In addition, where schedules have been used to create working test sets that are used to verify the operation of a tool, or tools, used within the laboratory, then the physical test set must also be retained; even if it becomes non-operational.

The underlying goal for the development of any test set should be that it is meaningful, appropriate and proportionate to the requirements being tested.

Therefore, wherever possible test sets should be constructed such that they can be used to test similar functions from a variety of available tools and processes rather than limiting them to specific implementations.

In the interests of proportionality it is strongly advised that rather than concentrating on attempting to verify the operation of an entire tool, testing should be limited to encapsulated atomic functions within the tool which are specifically used within local laboratory processes.

The detection of issues in processes and their internal functions will on the whole be primarily encountered during the analysis of standard casework, so proportionate verification on a case-by-case basis should be considered as an element of all laboratory processes. However, no laboratory should seek to directly utilise casework as a primary source of reference test set in order to validate a process as the ground truth will not be known.

It should be understood in digital forensics that even an extremely well constructed test set can only test a very limited (sample) number of possible permutations, it is therefore important that laboratories understand that an error and its associated uncertainty will always exist within the results obtained from any test set they employ.

To help reduce uncertainty, test sets should be designed to actively stress the limits of a process and its functions, this should include tests to determine what happens when known corrupted data is used and for detecting all previously identified issues.

A test set which fails to stress a process or its internal functions being measured is of limited worth, as is a test which is merely a large duplication of the same test.

The construction of test sets should always be considered an evolutionary process which tends towards an ideal as more and more information about the characteristics of processes and their internal functions become known.

Laboratories should always consider sharing aspects of their tests with other member laboratories. This will not only aid in the review and strengthening of bespoke local test sets, but could also lead to the development of traceable test sets which are available and can be used by all member laboratories.

When developing and maintaining bespoke local test sets laboratories should be mindful that any errors that may exist within them may go undetected indefinitely, and that some of the errors may be severe.

In some circumstances, the authors of ENFSI proficiency tests may allow the use of all or part of the test data to be used once the proficiency test has been completed and the results published. Authority shall always be sought in advance from the publishing ENFSI laboratory to ensure it does not infringe on intellectual property.

Third party test sets may also be used, subject to owner authorisation, but care should be taken to ensure that the construction of the test is understood, either by obtaining a copy of the characteristics being tested from the author, or by conducting detailed local analysis, or preferably both.

4.4 Accommodation and Environmental Conditions

When relying on digital systems to aid in forensic analysis it is important to ensure that the operating environments are fully compatible with both the environmental conditions detailed within the equipment manufacturer specification datasheet, and also that of the analysts if accommodation areas are shared.

Typical environmental conditions that need to be considered include temperature, humidity, air quality, hazardous materials, lighting and sound levels (e.g. certain proposed cooling solutions may raise sound levels to inappropriate levels).

Laboratories shall ensure that they are compliant with their national regulations.

Particular attention shall be given to the rating, regulation and reliability of the power supply units (PSUs) being used.

Poor power management may result in corruption of processed data and/or sporadic computer system crashes which may corrupt casework or damage exhibits.

Note: Most manufacturers only guarantee the operation of their electronic equipment within certain voltage and current levels. Therefore methods that may result in equipment operating outside of its limits may require the laboratory to apply for accreditation to additional test and measurement standards, typically at significant additional expense and complexity.

Care should also be taken to ensure all power supplies and electronic equipment is suitably isolated from electrical noise sources which may corrupt power and data lines. This also includes correct management of electrical cables to minimise the effects of interference on data and power lines

For example, unscreened electronic systems and PSUs should not be placed close to sources (e.g. fluorescent lighting) that may induce additional noise into their circuitry.

If any of the environmental conditions result in equipment exceeding the manufacturer's specified limits then either additional environmental controls must be put in-place to compensate, or more robust equipment should be considered as part of the risk mitigation process.

If distressing material is being reviewed then controls should be considered to minimize exposure to individuals not associated with the casework. This can include the restriction of room and visual access towards individuals not involved in the case.

When handling exposed electronic components and circuit boards it is important to ensure that all appropriate Electrostatic Discharge (ESD) and Interference (ESI) requirements are in place. This is especially relevant if there is a need to handle individual circuit board components, or desoldering/soldering operations are to be undertaken.

If the laboratory does not have existing ESD and ESI standard operating procedures in place, then they should consider referencing EN-61000-4-2 before proceeding.

4.5 Materials and Reagents

Not Applicable

4.6 Archive

An integral part of any archive policy is the data protection and security associated with each case type. It is also extremely important that the case management system used (digital or analogue) is capable of continually and accurately tracking user access and movement of all archived material.

Note: Archiving of material must be compliant with local and national regulations.

When a laboratory is choosing an archive solution, care must be taken to ensure that the format chosen is both compatible with the locally defined archive maintenance policies and procedures, and the manufacturer specification.

Archiving policies should ensure that all archive media is stored in accordance with the published manufacturer's environmental specifications (e.g. heat, humidity, etc.) to avoid for instance:

- Degradation due to unwanted oxidization; and
- Mechanical seizure.

If the recommended conditions cannot be met then the additional associated increased risk of potential data loss shall need to be factored into the risk analysis.

The risk analysis and assessment of a laboratory archiving policy and procedure, must address the likelihood that at least some of the archived material will sustain some damage, even if stored under ideal conditions. For this reason the following two issues should be addressed:

- The cost, and ease, of disaster recovery from archive media; and/or
- How to address issues that affect the alteration of imaged hash values for different file types.

It is also important to take into account the potential issues concerning obsolescence and how to read / recover material from obsolescent (historic) archive technology. Two effective ways of protecting against archive access issue are:

1) Maintain a library of equipment that enables the exact recovery and presentation of the archived original; and/or

2) Utilise new equipment that preserves the essence of the old information by transforming it into a new altered form.

When maintaining a library of equipment, both hardware and software, the following should always be considered within the risk analysis.

- Retention of all the original equipment, drivers and software;
- The purchasing of new equipment with a manufacturers formal guarantee of complete[2] backward compatibility;
- The cost of retaining full backward compatibility.

If required to review old casework it is recommended that in addition to the original analysis it is also reviewed using the latest laboratory processes to compensate for advances in analysis methods.

5 METHODS

5.1 Peer Review

A peer review is recommended as a verification measure to ensure the strength and provenance of the details being assessed. It must be conducted by someone who has not participated in the analysis, and shall always be completed by someone who is demonstrably competent to do so.

The review should take into account not only the critical review of methods, accuracy and provenance of technical information that has been used to support the information contained within a report, but should also take into account the intended audience for the report.

Care should be taken to ensure potential areas of misunderstanding and / or misinterpretation are clearly presented, whilst ensuring any simplification does not alter the context of the original results.

Due to the subjective nature of the analysis generally conducted within the forensic laboratory, it is impractical to fully review all work undertaken.

Instead, the level of final review should be based on the findings of the review of the case specific risk assessment, as defined within the laboratory's documented standard operating procedures.

[2] Procedures must be in place to ensure new equipment which is assumed to be completely backward compatible actually is. For example different subversions of software may interpret the data differently.

A more in-depth review shall be considered prudent when:

- The case specific risk assessment requests a detailed review;
- The examination is outside of the analyst's standard recorded competency framework;
- It is an infrequent case type that the analyst has not conducted for a given period of time; or
- There is an unresolved disagreement as a result of the peer review.

Laboratories may also find it effective to provide an initial pre-analysis review, to ensure that the proposed analysis steps are proportionate to the customer's requirements.

It is recommended that laboratories also formally employ additional dip sampling methods to randomly select cases for enhanced review of both pre-analysis and post-analysis stages to verify that the laboratory output remains consistent with its stated requirements.

The purpose of the additional dip sampling is to verify that the existing standard review processes are functioning within acceptable bounds. If as a result of the enhanced review issues are identified then the risk assigned to affected processes should be modified accordingly.

A formal record of the review should be documented and bear the signatures, either handwritten or digital, of both the reviewer and the analyst, and should be retained with the case records.

5.2 Examination Protocols

It is not the intention of this guidance to document or detail the exact examination protocols that should be used within laboratory based investigations.

Instead, the intention of this document is to provide the reader with a core framework, which can then be used to help develop laboratory protocols which are fine tuned to member's own specific requirements, whilst sharing core commonality with other ENFSI FITWG members.

It therefore remains each laboratories responsibility to ensure that all the protocols they employ are both suitable to their requirements, and those required by their regulatory bodies in order to obtain accreditation.

Whilst no two cases are ever likely to be exactly the same, there will typically always be a large proportion of the functions which, at an abstract level, can be considered common. For example at the highest process abstraction it may be:

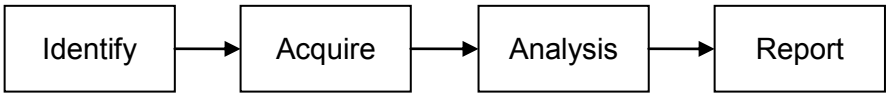


Figure 5.1 Example of a high level abstract analysis method.

In the majority of cases the analysis at any stage of the examination will consist of a sequence of two primary mathematical (functional) element types, which are:

1) Mappings (see Appendix C); and
2) Filters (see Appendix D).

Under standard conditions the quality of the examination results returned by mapping and filter elements will be directly dependent on the quality of the prior elements selected.

Multiple stages can operate either in series, in parallel, or a hybrid combination depending on the analysis requirements being undertaken.

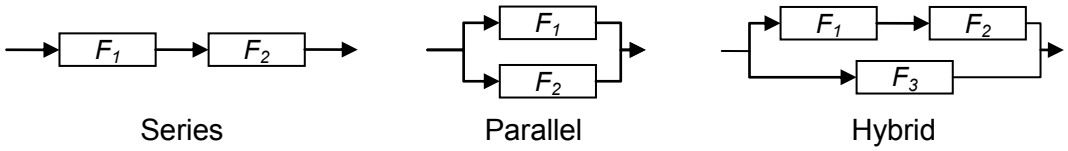


Figure 5.2 Types of abstract Mapping/Filter stages.

Each stage will consist of either or both of the two elements stated above. It is also possible to include a feedback loop to fine tune and calibrate for known errors.

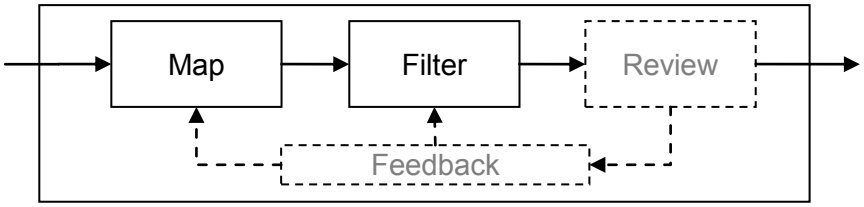


Figure 5.3 Mapping and Filter element with feedback to compensate for known errors.

By using this approach, seemingly complex and supposedly monolithic examination processes can be subdivided into smaller more manageable independent components that can be systematically reviewed.

These simplified components can then be analysed and risk assessed in isolation to form the basis of all the relevant process validation methods. This approach works equally well for automated and manual systems and their hybrid variants.

When subjective inputs are utilised within an examination they must be controlled through the use of case specific risk analysis and assessment which formally details the processes and sequences selected, along with their perceived affect on the accuracy of the analysis.

All subjective analysis, human or instrument based, should be considered in accordance with the human-based methods detailed within QCC-VAL-002 [(2)].

5.3 Research

Research plays a fundamental role in both the development of new and novel techniques, and ensuring that existing techniques remain fit-for-purpose.

Whilst it is true that in the area of forensic IT the technology and applications are constantly evolving and expanding, the foundations on which the discipline and its derivatives are based – computer science, physics (electronics) – are relatively fixed, and ultimately supported by mathematical theory.

Note: Whilst specific forensic models may not yet exist, a large proportion of the core computer theory is over 25yrs old (Information Theory (3) *is over 50 years old), and the concepts of proof (i.e. the kinds of questions that should be asked – see Appendix F) stretch back over 2000 years.*

Therefore, before going to the expense of developing and attempting to prove a new technique, time should be employed to research if the technique (or near equivalent) has already been suggested and perhaps even deployed by another laboratory.

It is also important to critically cross-reference any source before attempting to use a reference as an axiom on which the laboratory bases its validated processes.

All best practice (this document included), guidance, research papers, and SOPs on which forensic techniques are based, must be constantly scrutinised to ensure the axioms on which accepted methods are deployed remain true for the specific purposes for which they were intended.

The reader should always be wary when considering the following:

- There is always the possibility that errors will go undetected within a final published document, for example typographical and translation errors;
- Doing something, just because that is the way it has always been done and is now the assumed standard, or because that is how everyone does it, may very well be flawed in some way;
- Methods proclaiming to be “paradigm shifts” in forensic techniques may only be so due to a lack of research or understanding of existing available methods.

Best practice should always be to seek methods supported by axioms which have been rigorously tested[3], or even better rigorously proved.

6 VALIDATION AND ESTIMATION OF UNCERTAINTY OF MEASUREMENT

6.1 Validation

All ENFSI laboratories must be familiar with the requirements detailed within the ENFSI document QCC-VAL-002 “*Guidelines for the single laboratory Validation of Instrumental and Human Based Methods in Forensic Science*” (2).

The remainder of this section assumes the reader is familiar with the above document, and so only describes specific sub-elements within the Forensic IT Working Group (FITWG).

Validation relates to the ability of a process to meet the formal requirements agreed with the customer. Verification of functions within tools cannot, by themselves, be validated as the environment and ability of the user must be acknowledged as part of a process. A description of function verification is detailed within section 6.6.

[3] A test result is only as good as the test applied. If a test set is weak then the resultant axiom and everything based upon it will also be equally weak.

International Standards and National Regulatory Codes of Practice promote flexible effective methods based on scientific proofs. They deliberately utilise abstract terminology in order that laboratories shall be able to create fit-for-purpose methods.

If a laboratory identifies a local validated process which restricts the use of essential equipment then it has a duty to correct the process in question, and re-validate the improved method.

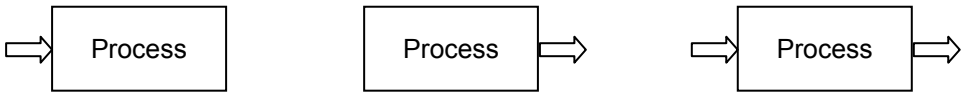
Good practice requires an understanding of both the processes selected to perform a forensic[4] examination of digital technology, and an understanding of the expected knowledge of the intended recipient of any report generated.

Due to the multiplicity of unused functionality that can exist within Forensic IT (FIT) instruments, and the complex ways in which FIT instruments may be combined to produce a result, validation shall be restricted to specific process (task or method) being undertaken.
Referencing appendix E.1, a validated process is described as:

> "*A validated process is one which demonstrably conforms to its statement of requirements. A technical process may be considered to be validated for a particular purpose if, when tested, it meets the stated requirements for that purpose.*"

The overarching guidance around the development of validation techniques and procedures within this document is to sub-divide seemingly large (monolithic) complex systems into smaller, and hopefully simpler, (atomic) components through the use of black-box abstraction methodology.

A process must consist of an input interface (i/p), an output interface (o/p), or both (i/o).



a) i/p interface b) o/p interface c) i/o interface

Figure 6.1 Abstract representations of Process input/output characteristics.

At its simplest a process will consist of one-or-more human-based functions and no instrument-based functions.

Note: As a simplified example, receiving a sealed exhibit and then placing it directly into secure storage would be a process containing two human-based functions.

Processes that require interaction with instrument-based functions, either hardware or software based, will be more complicated but essentially still follow the same pattern. It is also common for instrument-based forensic functions to rely on human-based functions to verify the interpreted result.

To reduce the potential complexity it is generally good laboratory practice to isolate the instrument-based functions commonly used and encapsulate them into groups which can be wrapped into their own processes.

[4] A forensic process requires that analysts understand and report the known limitations of their processes and specific tools selected using proven scientific methods and practice. In other words, they should not use; or incorrectly assert, assumptions if they do not understand the operation and/or limitations of the system used.

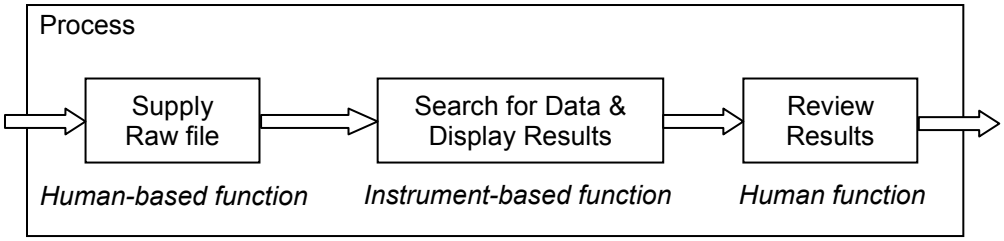


Figure 6.2 Example of encapsulation of a function within a dedicated sub-process

Note: Verification of functions should be limited to those specific to the process, rather than attempting to verify all the functions available within a tool.

Validated processes can be constructed using a combination of smaller sub-processes and functions.

In order to create trustworthy processes, verification (see section 6.5) will be required to validate the developed process, and also demonstrate that the user and instrument functions used do actually operate within the bounds of known risks and their errors.

This is especially true for forensic IT processes where instruments generally do not comply with a proven nationally accepted standard.

For the interpretation of evidential significance in the context of the case, a laboratory should always consider the use of techniques and equipment whose risks have been formally assessed; as part of the required functional verification, in preference to those which have not.

This does not mean that a method or process that has not been formally evaluated cannot be used to aid the analysis; rather it means that if there is a wish to use such a solution, a formal justification as to why it has been chosen in preference to one that is part of a validated process must be made.

When designing a validation process, five key elements of a successful validation policy are:

1) An understanding of known errors and uncertainty;
2) The Statement of Requirements;
3) Risk Analysis and Assessments;
4) Effective validation test sets; and
5) Routine verification.

These elements are expanded upon in the remainder of the section.

6.2 Estimation of Uncertainty of Measurement

All physical systems, even calibrated equipment that is traceable to an international standard, will exhibit a measure of uncertainty which needs to be taken into account within any associated processes.

Uncertainty is the unknown (random) difference (delta) between the measurement taken and its true value. It can never be completely defined, or eliminated, and is represented as a bounded region in which the true value exists within its given confidence level.

Uncertainty within a system is additive in nature, and generally increases with the number of functions deployed within a process. The decision as to whether the uncertainty should be calculated at the function level or abstracted to the process level is at the discretion of each laboratory.

For help in understanding uncertainty the reader is advised to read the uncertainty based documents [4], [5] listed within the References / Bibliography (section 15).

Software solutions will also contain additional uncertainty on top of the uncertainty associated with the physical systems, including the operating system, they are running on. This is especially true for software which relies on functions with no formal specification and/or calibrated standard

As a result, software uncertainty properties will also need to be acknowledged and accounted for.

Uncertainty can be expressed using either historic data to formally evaluate its value using (statistical) analysis or, in cases where this is not currently appropriate, by the inclusion of formal documentation describing the limitations and possible errors (both Instrumental-based and human-based) of the system processes being used.

Any process that is declared as having no uncertainty should raise serious concerns as it is either due to a lack of knowledge on behalf of the person stating this as fact, or worse may be considered an active attempt to obfuscate the true information.

Uncertainties that will typically be present within a forensic process examining digital technology include:

- All forensic functions (Instrumental and human based);
- Media Identification and protected or encrypted areas;
- Disk Acquisition (handling of detectable and undetectable errors);
- Report writing and reader Interpretation (human-based); and
- Archiving (reliability of archive and retrieval – section 4.6).

Even when the effects of uncertainties contained within acquisition and analysis stages are fully appreciated, it is still important to take into account the possibility that reports written in a clear and concise manner may still be misinterpreted.

Note: It is generally not possible to know in advance how reports may be misinterpreted by a reader, instead it should be analysed and fed back into the laboratory system as part of ongoing post case reviews.

6.3 Statement of Requirements

A detailed description of the general Statement of Requirements is presented within Appendix E, and in essence can be described as

> "*The statement of requirements defines the problem to be solved by a technical process. It should provide explanatory text to set the scene for a lay reader, summarising the problem, noting the scope and acceptable risks or limits of any solution and acknowledging the relevant stakeholders. It should be created independently of and without regard to any particular implementation or solution.*"

The remainder of this subsection assumes the reader has reviewed and is completely familiar with all the descriptions given within the appendix.

Customer requirements relate to both the judicial system and the investigating officer, however, the requirements of the local judiciary shall ultimately take precedence.

The statement of requirements provides the interface (or formal bridge) between what the customer[5] believes is achievable (customer requirements), and so desires, and what the laboratory can realistically achieve (laboratory capability) with the available staff, tools and the incurred time costs.

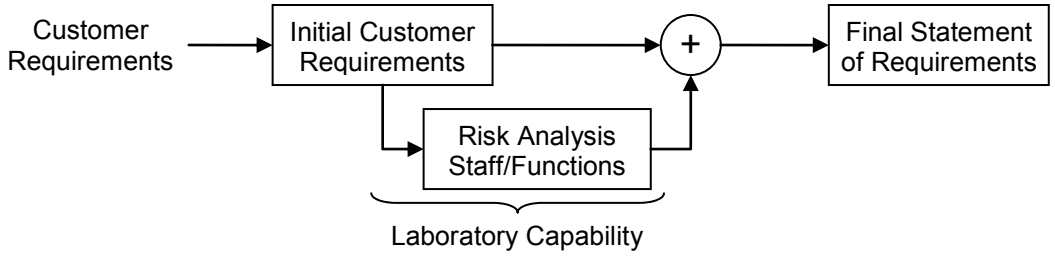


Figure 6.3 Components required in developing an agreed Statement of Requirements.

Note: If the risks are considered too great then either the statement of requirements will need to be amended, or alternate solutions sought, to reduce the risks to acceptable levels.

Common customer requirements that are likely to be required to be met include, but are not limited to:

- The data analysed is a valid copy of the original data;
- Results should be made available within an agreed timeframe;
- The use of un-validated methods should be declared;
- All known errors in the process used should be declared;
- The uncertainty of the methods used should be declared; and
- The general risks associated with a case should be available for review.

The information described within the final 'Statement of Requirements' will form the basis on which the process being validated will ultimately be judged as either a pass or fail. Therefore, it is very important that the defined requirements are both accurate and realistic with respect to standard scientific principles and current available methodologies.

Note: The Instrumental-based validation methods formally described within QCC-VAL-002 (version 1 section 3.1) are designed for forensic solutions in which the tools are within specification and calibrated to a recognised standard.

Once the final "Statement of Requirements" has been defined the list of validation stages described in QCC-VAL-002 can be completed.

6.4 Risk Analysis

The forensic examination of digital technology contains a number of additional risks which are normally not present in most other forensic disciplines.

The largest of which is the general non-compliance with the requirement described within QCC-VAL-002 (section 3.1), namely the actual specifications of most tools won't be known and cannot be calibrated to a recognised national standard.

[5] Within the context of the "Statement of Requirements" the customer is the judicial system.

> "*It is implicit in the method validation process that the studies to determine method performance parameters are carried out using equipment that is within specification, working correctly, and adequately calibrated.*"

The inability to be able to rely on instruments with a set specification and traceability, via a calibrated standard, means that the risk analysis and verification stages are paramount in creating a reliable validation method.

The remainder of this subsection gives a very general guide to risk analysis and the recording of the risk via the formal risk assessment process.

An example of a Risk Assessment is given in Appendix H.

Risk analysis is the process by which both potential errors and uncertainty can be highlighted and then mitigated to help assure that any system or process used operates within acceptable predefined bounds.

At its most simplistic it should be used to determine the reliability of the method(s) used, highlighting issues that may arise during both normal operation and anticipated unforeseen circumstances, and categorising the danger each identified risk poses on the overall process.

Examples of Instrumental-based questions related to risk analysis include, but are not limited to:

- Are new and updated subversions tested before introduction?
- Does it operate correctly for its intended purpose?
- Does it operate correctly in its working environment(s)?
- Are exceptions to its correct operation accounted for?
- Is its operation affected by local resources (section 4)?
- Are test results verified by an independent 3rd party, or a recognised test laboratory (preferred)?
- Are the results during normal operation monitored for consistency?
- Is routine re-verification conducted?

If the answer to any of the above points is "No" then the risk will obviously increase, if the answer is "No" (or "Don't Know") to more than one question then the risk will become more severe, perhaps even critical, as there may be no way to demonstrate that the function operates within specification.

If the risks cannot be reduced to an acceptable level then the "Statement of Requirements" (section 6.3) will have to be amended accordingly.

Risk analysis can not only be used to explain why a verified function has been used within a validated process, but also why in certain circumstances a formally unverified function has been chosen in preference.

Note: When using a formally unverified function, especially one not designed for forensic use, then additional consideration should be given to the risk that it may corrupt the data it is processing.

6.5 Process Verification

Process verification is confirmation that a process does, or does not, conform to its formally accepted performance parameters under current local operating conditions[6].

As with all forms of verification, and calibration, process verification only provides a 'snap-shot' measurement, at the time of verification, of how well a process performs relative to the tests applied and tolerances (uncertainties) allowed for the results measured.

A validated process, even an accredited one, may move out of scope even if subject to seemingly small variations over the period of its existence within the laboratory environment. Examples of variations include, but are not limited to:

- Changes in staff (technical and administrative);
- Changes in tools (see function verification); and
- Changes in resources (see section 4).

It is therefore important to consider the risks that may be involved if a process is not routinely re-verified[7] to ensure it continues to conform to the current statement of requirements.

Unless specified by a laboratory's national requirement, the period between re-verifications should be based on the perceived risk as defined by each laboratory.

To help reduce the cost, and effort, of verifying large processes it is recommended that processes are subdivided (atomised) into smaller encapsulated sub-processes.

6.6 Function Verification – Tool / Instrument based

Many processes utilise technical functions contained within an instrument which must be evaluated and verified to ensure they are technically fit-for-purpose.

Function verification of forensic tools, is concerned not with the verification of the functionality of the entire tool, but instead the verification of only those functions within forensic tools which are used within validated processes.

The design and use of automated verification systems[8] are encouraged, wherever possible, to limit the impact on casework and to provide shorter intervals between verifications.

Where instruments used are not formally traceable to a recognised accepted standard, a more rigorous set of functional verification must be undertaken.

Forensic instruments will include:

a) Functions whose results have to be implicitly trusted; (e.g. Data Acquisition, Hash calculation, etc)

b) Functions whose results can be manually verified; (e.g. Search Filters, etc)

c) Functions whose results are primarily user subjective. (e.g. Manual review of a hex dump, etc.)

---

[6] Please refer to QCC-VAL-002 information on defining a validation plan and its testing. (The validation plan is constructed from the final agreed "Statement of Requirements").

[7] Please refer to QCC-VAL-002 section 2.2 paragraph 2 and associated references.

[8] Automated verification systems will themselves also need to be verified.

The highest priority for formal or out-of-process verification should be assigned to functions where there is an implicit reliance on the generated results (bullet a).

If laboratory processes utilise staff that are not sufficiently trained to manually verify function results (bullet b), then risk analysis should also determine this is equivalent to implicit trust (bullet a) and therefore should be categorised as such.

It is considered best practice to formally verify the accuracy of all technical functions which are implicitly trusted within a process to increase confidence[9] in the results.

Verification must be conducted in-situ to ensure the results are relevant to the environment in which they are used. This requirement is just as important for software solutions as it is for hardware only equipment (see section 4.2).

It is important for the laboratory to locally confirm that the documented functionality of an instrument-based tool is a true reflection of its actual functionality.

Examples of basic verification checks include, but are not limited to:

- Can it accurately map a file's data stream? and to what level?
- Can it accurately search a mapped files data stream?
- Can it accurately visually represent displayed data?
- Can it accurately save / reload the current work? and
- Is the operation of a function affected by external sources?

Appendix F contains examples of the types of questions that should be asked when assessing the ability of a tool and its functionality.

It is the responsibility of all forensic analysts to formally report any functional errors they detect either during a verification sequence or during normal forensic work.

Likewise, it is the responsibility of the laboratory to effectively track the reporting and resolution of these errors, and report faulty functions back to the manufacturer.

It is the responsibility of each laboratory to verify their specific methods and systems based on their formal local implementation.

6.7 Function Verification – User / Human-based

Human-based functions are the pivotal elements within technical forensic processes, all forensic processes are likely to require user interaction, therefore an evaluation of user capability must be made as part of validated process within the laboratory.

Even if an instrument-based function returns a valid result, it may still be reliant on the correct interpretation by the user associating the result. A good example of understanding the implications of this in practice is reported in Zdziarski, 2014 (6).

Verification of human-based (user) functions are covered within proficiency testing (Section 7) and also detailed within section 4 of QCC-VAL-002 (2).

[9] Confidence is subject to the quality of the test sets employed (see section 4.3). A function that is verified using a poor test set can create a false confidence in inaccurate results.

7 PROFICIENCY TESTING

7.1 General

Proficiency tests should be used to test and assure the quality of Forensic IT *s*pecific processes. A list of currently available PT/CE schemes as put together by the QCC is available at the ENFSI Secretariat. “Guidelines on the conduct of proficiency tests and collaborative exercises within ENFSI” (7) provides information for the ENFSI Expert Working Groups (EWGs) on how to organise effective proficiency tests (PTs) and collaborative exercises (CEs) for their members.

Proficiency testing provides a mechanism by which staff development requirements can be formally measured (assessed) as part of a laboratory competency review.

They should be used as a method by which staff development needs can be identified and measured against the requirements within the processes formally used within the laboratory.

Laboratory testing shall be conducted at regular (determined by the laboratory[10]) intervals, and should follow a formal structure that ensures that over time the entire primary scope of the laboratory is assessed.

It is recognised that the scale and nature of forensic IT means it is very unlikely that a laboratory will be able to conduct detailed proficiency testing in all forensic areas within its overall scope. This limitation means that the laboratory must recognise and manage the additional risks and errors this entails.

Proficiency testing for laboratories can be sub-divided into two distinct groups

1) External proficiency testing[11]; and
2) Proficiency testing within the laboratory[12].

Due to common limitations in standard test construction; and the associated design time constraints, the majority of proficiency testing will occur within a known test environment. Under certain conditions it may be desirable to construct tests which attempt to monitor performance under normal investigative conditions through the use of a ‘blind’ proficiency test introduced as a regular case.

Laboratories should consider using the variation in results obtained during proficiency tests of staff to help monitor the risk and errors associated within their processes.

Internal proficiency tests should be designed to provide useful feedback to the laboratory to help continually verify that the existing laboratory process human-based risks remain within acceptable bounds. If the user trend deteriorates, then either the risk assessment(s) must be adjusted accordingly or the process re-validated.

---

[10] Proficiency testing is likely to be part of a national regulatory requirement to achieve accreditation, in which case they may specify a maximum allowed acceptable interval.

[11] If using an external company for proficiency testing then please refer to their specific terms and conditions for compliance information.

[12] Internal proficiency testing may be termed as ‘Competency Testing’ within particular accreditation systems.

If a proficiency test highlights a problem with a process, or a specific function within a process, then that may also indicate that there is a problem with the associated current validation or verification process (see section 6.5).

7.2 Staff Training and Proficiency Testing

If the result of a user proficiency test is consistently close to 100% for all staff, then it may indicate that the test is either too '*simple*', or that the risk assessment(s) can potentially be relaxed to accommodate the improvement in staff skill level.

Similarly if the staff results are below the assigned threshold then it may indicate that staff haven't received sufficient training, in which case the risk assessment(s) should be modified to account for the increased risk.

Note: It may alternatively indicate that the test is to complex, or detailed, for the time assigned to complete the test.

Staff training is a very important part of staff development, however in most cases it does not, in itself, constitute an evaluation of staff proficiency.

Therefore, the development of laboratory staff competency and proficiency should be considered a combination of formal training and on-the-job experience.

On completion of training, staff should be formally evaluated on what they have learnt, this may be conducted either as a peer review by a suitable qualified member of staff, or by assessing new local techniques which arise as a result of the course undertaken.

Formal training, monitoring, and testing of staff shall be in place to ensure they are fully conversant with all the required local processes they are expected to comply with. This is especially true if a staff member is:

- Conducting a new examination type;
- Relocated from another laboratory; or
- Returning from a long absence.

If it is anticipated that staff are likely to have to perform subjective analysis (opinion) during an investigation, then the appropriate proficiency tests should be sufficiently stringent to cover the additional subjective requirements that need to be factored in.

7.3 Focused Proficiency Testing

Large, complex, inter-laboratory proficiency testing and collaborative exercises can be very beneficial, enabling laboratories to assess and develop their methods with respect to other similar laboratories. Whilst they are of significant value, the level of complexity can cause problems for both the creator and participant laboratories to readily absorb the time penalty with the need to complete existing casework.

It is therefore also recommended that laboratories should consider atomising some of the complex scenarios into more focused versions which independently test specific aspects of staff proficiency within a shorter timeframe.

In this way, individual tests can also be constructed and marked in a considerably shorter timeframe, and can more readily be combined and re-used in multiple proficiency tests of staff with different levels of knowledge.

As an example, proficiency tests which previously incorporated acquisition and analysis could easy be split into two separate proficiency tests.

- Acquisition (including exhibit continuity); and
- Analysis.

8 HANDLING ITEMS

8.1 General

Within the context of this document 'handling items' relates to the physical seizure, protection, transportation and archiving of the exhibits for subsequent analysis either at scene or at the laboratory.

For information detailing data prioritization, extraction and analysis please refer to section 9 (Case Assessment) through to section 12 (Evaluation and Interpretation), and all the Appendices.

8.2 At the Scene

Before attending a scene, forensic IT staff involved should be aware of, and fully understand, their laboratory's predefined procedures concerning Pre-Scene Preparation (section 9.1) and Assessment at the Scene requirements (section 9.2).

It is also fundamentally important that they remain in compliance with their local police guidelines relating to the search and seizure of evidence.

To avoid potential data contamination and destruction it is advisable that the suspect and related witnesses shall be kept away from both the potential exhibits and any communication devices that may be able to interact with them.

If at scene there is likely to be a requirement to work with other forensic departments, for example DNA or fingerprints, then the sequence of forensic work should follow an agreed pre-defined sequence that is dependent on the importance and destructive nature of each forensic process (see section 9.1).

The senior scene officer shall be advised that scenes should be searched systematically and thoroughly for digital evidence, targeting and prioritising areas which in the context of what has been alleged are most likely to contain material of evidential significance.

Contemporaneous records shall be made at the time of seizure, or as near as practically possible, of items recovered from the scene, or person, and describing the exact locations from where the items were recovered. These records shall be inserted into the resultant case file.

It is highly advisable to photograph and sketch a plan of the scene marking the locations and status of all the relevant information.

Note: Anti-ESD measures should be taken if an exhibit is prone to potential damage from ESD, and ideally a label attached to identify the risk of damage.

The risks involved with the seizure of live radio frequency (RF) network connected equipment should also be noted, and the decision as to whether to switch it off or seal it in a RF protected case must follow laboratory standard procedures.

Note: Care must also be taken when selecting a RF protected case to ensure the case is capable of attenuating the specific frequency ranges involved, and that the isolation from the network will not result in data loss due to power drain.

Risks involving the seizure of equipment capable of communication outside the RF bands (e.g. Infra-red) should also follow similar guidelines to those of RF.

Whilst the legal status and use of labels can vary, sealed items should always be labeled at the time of seizure. The minimum details that should be recorded and be directly and unequivocally attributed to each package are:

- a unique identifying reference;
- a brief description of the material with (unique) identifying marks;
- the location from where the material has been seized;
- the name of the person and organisation responsible for collecting and packaging the material; and
- the date and time the material was seized.

Specific care should be taken with the transportation of digital evidence material. Dangers include physical impact damage, vibrations, magnetic fields, electrical static and large variations of temperature or humidity.

8.3 In the Laboratory

Exhibit continuity and seal integrity must be checked, and validated, prior to the starting of any examination. Any discrepancies must be recorded and rectified before being accepted by the laboratory for further examination.

On initial receipt of an exhibit, each exhibit should be assessed to determine if storing the exhibit is likely to result in data loss. If data loss is likely to be an issue then suitable precautions to protect the data must be considered before placing the item into storage ready for analysis.

If data loss is likely to be due to power drain a risk assessment should be made as to whether the exhibit should be:

- Connected to a power source to ensure it remains charged; or
- Analysed before all the data is lost.

In cases where the data loss may occur as a result of a devices' capability to receive RF communications, the use of data attenuation / screening techniques should be made to limit its likelihood to an acceptable level whilst in the laboratories possession.

Received exhibits should always be assessed as to whether Anti-ESD measures should be taken to ensure their integrity during the subsequent analysis stages. If Anti-ESD measures are a requirement then the exhibit should be clearly labeled, and the analyst assigned to work on the exhibits should be familiar with the laboratories handling requirements (see section 4.4).

Items for which anti-contamination precautions are required should also be clearly labeled, and adhered to during the examination process.

9 CASE ASSESSMENT

9.1 Pre-Scene Preparation

In cases in which laboratory staff participate in scene attendances and evidence recovery, time at scene can usually be more effectively utilised if pre-scene preparations have been proactively made.

At its simplest, this may only involve ensuring that all the standard required equipment for scene attendances is readily available and in operational condition, both physically and electrically. All callout staff should also be aware of any relevant local guidelines followed by their police forces.

Guidance around the consideration of how to proceed in cases where other forensic disciplines are required (e.g. fingerprints, DNA, etc.) should be defined at this stage in order that consistent advice is always given.

Knowledge on how to prepare for the identification and capture of live dynamic data in memory, live encryption and remote system reset prevention will also need to be evaluated at this stage. Failure to do so may result in important data becoming irretrievable once a system is physically seized.

9.2 Assessment at the Scene

Assessment at scene in this context also extends to the support and advice provided remotely to those that are at the scene so that submitted exhibits can later be effective processed within the laboratory.

Activity at scene should be abstracted into 3 categories:

a) Identification of exhibits;
Identification includes device and network configurations.

b) Seizure of exhibits; and
Seizure need not be a physical action, and seized exhibits includes screenshots and physical and logical data that may be collected over a period of time.

c) Processing of seized exhibits.
Processing of seized exhibits may results in further seizures at a scene.

Once an exhibit has been *seized* it should be processed depending on the policy clearly defined within the laboratory, and whether or not the system being seized is currently connected to a power source.

Laboratory standard operating and pre-scene preparation procedures should describe clear formal guidelines detailing the seizure process for exhibits which are thought to be in an active state.

- Use of a trusted 3rd party, such as a system administrator, to extract specific data for subsequent processing; or
- Assume control of a system (*i.e. when doing this you may become responsibility for any damage that occurs as a result of your actions*).

Note: There is no point switching off a seized exhibit if the affect of doing so is to render all the relevant data either lost or irretrievable.

If an exhibit is to remain active during on-scene analysis or transportation then appropriate risk based electrical, optical and RF precautions should be taken to ensure the device cannot be remotely accessed.

9.3 Assessment at the Laboratory

Whether the assessment is carried out at scene or at a forensic laboratory the assessment should follow similar guidelines.

An initial risk assessment should be conducted as to the state of the seized exhibits, and any issues that may arise due to them still being active, or isolated from power and communication interference, should be recorded.

In cases where a large number of exhibits have been submitted it may be prudent to selectively prioritise the examination of exhibits. If this is the case then the documentation must clearly state which exhibits have and have not been analysed and the depth of any analysis.

9.4 Live Analysis of Remote Systems

When conducting analysis of remote live systems the analyst should be aware that remote logging of their activity may be recorded by the remote server, and made available to the owner of the files and/or web pages they are viewing.

The laboratory should consider the location of the remote server, and be fully aware of the legal cross border constraints that may be a factor in accessing any data.

There may also be additionally constraints if some, or all, of the data is considered as communications data which is subject to national legal intercept restrictions.

9.5 Initial Case Evaluation

An initial assessment of the information available and the items provided for examination should be carried out before starting formal work on any case. The assessment should include contacting the customer to check that the requirements have not changed and also to discuss the anticipated approach, and the potential risks that may arise during the investigation.

This review should be balanced to ensure the request is both proportionate to the investigation and that the customer is aware of all the analysis options available to them.

Case evaluation should also take into account if the examination will start as a complete analysis, or will be based on staged reporting methods (see section 10.3).

This formal assessment should enable the development of an action plan, based on the agreed customer requirements and the potential risks involved with the selected processes. Any changes to the original request should be formally documented to ensure an effective audit trail.

Depending on the requirements of each case, and the experience of the assigned analyst(s), the selection of available processes may vary. Where this includes a variation in the level and quantity of subjective-based methods being employed the risks shall be adjusted accordingly.

Case evaluation processes where an analyst's intuition, skills and knowledge (art) is extensively deployed will require a more careful selection of the analyst, and may require a more extensive peer review.

9.6 Case Acquisition

In cases where the media's functionality is questionable due to possible damage, a decision based on a risk analysis should be made as to whether an attempt to access the data using standard methods or more advanced media extraction methods should be considered.

The opportunity for recovery of digital evidence will depend on many factors, including:

- The volatility of the original data to be acquired;
- The age and condition of the item submitted;
- Automatic system deletion of unallocated data; and
- The level of any security features applied by the original user.

Most modern storage solutions have an interface between the physical storage and the logical sectors presented at their external interface, usually defined by the term Logical Block Address (LBA), which is the access method to stored data.

This means there are generally 3 distinct forms to data access (retrieval) available to forensic IT laboratories from modern data storage devices, these are:

- Logical File System access;
- Logical Block Address (LBA) access; and
- Physical Block access (non LBA) access;

For live memory and file acquisition a pre-scene analysis of the expected footprints of all field tools likely to be used is strongly recommended. It is also preferable that tools and process which have the least forensic footprint for the current case requirements be used in preference whenever possible to reduce potential loss of evidence.

In some cases, especially embedded systems, access to exhibit data may be restricted due to non-standard interfaces or no interface at all. In these cases it may be necessary to physically remove[13] integrated components (ICs) from the exhibit in order to acquire the data. This method is commonly known by the term "Chip-Off".

Note: IC removal is a specialist activity which should only be undertaken by suitably trained staff. Knowledge in reading and understanding datasheets is essential to both ensure the applied physical influences (e.g. heat, pressure, etc) do not damage the device, and that the data pins are known and can accessed.There is no point going to the expense and effort of removing a component if the process used destroys the data that needs to be accessed, or the technical information needed to access the data cannot be identified.

Laboratories should consider designing processes to handle circumstance where an original exhibit must be taken apart to gain access to stored data, or to attempt to repair physical damaged circuit boards before data access can be achieved.

If the laboratory does not have the necessary facilities available to conduct complex low level media repair then consideration should also be given as to whether the media should be sent for repair by an approved 3rd party before declaring the exhibit data cannot be accessed.

10 PRIORITISATION AND SEQUENCE OF EXAMINATIONS

10.1 General

Proportional consideration should be given to the following before commencing any examinations for digital evidence:

- The evidence requested by the customer (officer);
- 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; and
- The time available to carry out the examination.

13 When accessing internal components within an exhibit care should be taken to ensure the analyst is aware of the potential dangers and that standard COSHH policies are adhered to. (see section 8 - Handling Items)

It is recommended that communication with the customer (officer) be maintained throughout the examination process. This helps to both ensure that the customer is kept informed of what material may or may not be available to help with the investigation, and that the examination remains focused on the customer's requirements.

Formal consideration shall be given to ensure cross-contamination of exhibit extracts cannot occur.

10.2 Initial Review

The initial review to determine the proposed sequence of analysis may take place before any forensic examination has started, or may occur after initially *loading* the data to determine the size of the requirement being undertaken.

In all cases the agreed sequence of analysis should require the generation of a unique case based risk assessment to support the analyst's proposed solution based on the required case evidence and information supplied.

Whilst the risk assessment should take elements from a default standard, the actual assigned values must be adjusted for each case to take into account details such as, the relevant knowledge and experience of the analyst, the complexity of the request, and the time assigned to conduct the examination.

Staged based analysis can be used to provide the customer with a general overview of results within a reduced timeframe.

10.3 Stage Based Analysis

This approach can help to focus the customer's requirements for the examination, and reduce the laboratory processing time. However care must always be taken to ensure the appropriate level of provenance is recorded along with the supplied results.

Changes to all the associated risks at each stage shall be assessed on a case-by-case basis to ensure they continue to truly reflect the supplied results.

11 RECONSTRUCTION OF EVENTS

11.1 General

The analysis should be designed to determine if the submitted items contain information that can prove or disprove a proposed hypothesis.

This may include information describing what would be expected to be found if each proposition were correct, and should include an assessment of the likely evidential value of the anticipated findings.

When considering the use of proposition methodology within an examination then the ENFSI MP2010 document (STEOFRAE [8]) should be referenced for additional guidance.

All analysts should be aware and understand that stored values are not only mapped to their binary (machine readable) equivalents, but also that the methods by which the original mapping were made may vary on an application-by-application basis.

Reconstruction based on timeline analysis should always take into account the potential inaccuracy of the temporal metadata caused by either system activity, OS and application specific peculiarities, or user activity to obfuscate the true time.

11.2 Case Analysis

During the analysis of exhibits, identification of possible connections to additional external data sources (e.g. portable devices, cloud, etc) should always be considered to help to:

- Understand the usage patterns of the current system; and
- Potentially gain access to additional sources of relevant data.

Note: Additional sources of data are not limited to digital storage, but may also include printed documents and handwritten notes.

Whilst it may not always be possible to state that specific recovered data originated from a particular data source to the exclusion of all others, under certain circumstances it is possible to determine if the data was created, copied or moved to its current location. This may even extend to determining if a transfer from a different file system has occurred.

When attempting to analyse case data it is important to understand that data may be mapped in an obfuscated form and this obfuscation need not be a direct result of user intervention. Common forms of obfuscation include, but are not limited to:

- Non-contiguous storage of data blocks;
- Injection of control codes and pointers between the data;
- Storage of data in a compressed form;
- Storage of data within an archived format;
- Storage of data within an unknown file format;
- Storage of data in an encrypted form; and
- Storage of data within hidden areas.

It is therefore important to understand which forms of mapping the functions within forensic tools can natively interpret and which will require manual intervention, and how this will affect the associated risks and errors of the methods used.

Prior to attempting the final reconstruction of events it will be common to reduce a large initial dataset into a more manageable form through the use of search filters. To complete this stage effectively it is paramount that the analyst understands the effects that poor pre-mapping of the data will have on the returned search results.

A failure to understand this will directly affect the number of returned false positives and ignored false negatives increasing the risk of unmanaged errors.

When employing time / date filters it is essential that the applied filter correctly takes into account the accuracy and time zone of the original clock the time is taken from.

Analysts should always support specific timeframe associations with scientific research; if this has not been conducted then the reconstruction of timeframe events should not be presented as fact (since the assumptions used may be inaccurate).

An example of understanding the implications of this is given in Zdziarski, 2014 [(6)].

A failure to appreciate the effects of mapping and filters used within a case can ultimately result in either missing evidence, or worse, wrongly convicting an innocent member of the public.

11.3 Analysis of Artefacts Generated by 3rd Party Applications

In digital forensics it is always possible that the original application or hardware will be a closed source protected by intellectual property (IP), which is protected from reverse engineering as part of the terms and conditions.

The laboratory must consult with their legal department to determine if reverse engineering of such (for case specific) system code is out of bounds due to legal restrictions, unless authority from the supplier can be obtained.

However, it should always be possible to use standard black box techniques to provide analysis using known input data and analysing any resultant stored output.

Whilst this approach may not be able to exactly explain and reconstruct the process within the black box, it should provide enough information to make some form of acceptable factual evaluation.

All risks and uncertainties associated with the evaluated results should be formally recorded within the case notes, and declared within the report.

It must be recognised that functionality and risks measured, and attributed, to a specific subversion of an application may not be transferable to previous or subsequent subversions.

Note: It is common for applications to undergo significant changes within major version releases, and is also not unusual for subversion updates to introduce new functionality and fix reported issues.

11.4 User Activity

During a standard investigation the analyst may draw on a number of automatically generated system or application data artefacts to aid the reconstruction of user activity.

Whilst these characteristics may be very helpful, care must be taken to clearly distinguish between actual user initiated activity and automated system caching as a result of user activity.

This is especially important in cases when trying to prove possession and making, where the analysts should prove beyond reasonable doubt the provenance of the evidence they are reconstructing.

12 EVALUATION AND INTERPRETATION

12.1 General

An understanding of how both the original application and the forensic tool interpret the data is necessary in order to scientifically evaluate and interpret the findings.

The lower the level of knowledge, the greater will be the potential errors and risks.

The effects of systematic and random faults within the original data and the results returned shall also be considered as part of any evaluation and interpretation.

In all cases, the potential size of the errors present in any analysis should either be stated using an approved mathematically derived value, or as a sentence/paragraph detailing the known limitations relative to the information found.

Knowledge of the underlying mapping and/or filter functions is important in guiding and defining the decisions made during this process.

12.2 Interpretation

Where interpretation is required the analyst should consider to what extent the propositions put forward by the customer can be tested, and should assess whether recovered data could be present due to other circumstances.

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.

If limited examination methods are deployed during the analysis stages then the increased probability of evidence being missed (false negatives) within the process used should also be considered.

12.3 Verified Functions

It may not be unusual for two separate tools with similar functions to return slightly different results under certain conditions during an analysis. This will typically come down to how each tool interprets the data it is trying to evaluate.

It is important therefore to understand the functionality constraints when selecting functions for use during a specific case analysis. The reason why the selected function was chosen in preference to other alternatives shall be recorded.

If two separate tools with similar functionality are used on the same case it is important that both sets of results are declared within the notes, along with any known discrepancies that may have occurred.

If a new, unknown, discrepancy is detected then the evaluation will need to be highlighted for the peer review, and one or more of the verified tools may need to be reassessed, along with the existing validated process.

12.4 Non-Verified Functions

If no formally verified function is available to successfully complete an analysis stage then a non-verified function may be used. It is however, important to demonstrate that it provides results which exceed those capable from the verified functions available.

In cases where no verified equivalent functions are available to help make the comparison, then a far more detailed evaluation (with greater management overhead) will be required. In effect the analyst will need to verify the functionality used.

When using a non-verified function during analysis it is important that the analyst is competent enough to research the characteristics of the returned results, and can qualify them against standard validation methods employed within the laboratory (see sections 5 and 6 for guidance).

The development of scripts and software routines for use within a specific case shall also be classified as non-verified functions. In addition to including the software code within the case archive, it is also essential that a copy is retained within the laboratory software register (see section B.1 for more details).

If a non-verified tool function is routinely used then it is expected that it should undergo formal verification, and be added to the laboratory approved list.

12.5 Evaluating Files and Raw Data Mapping

All file data will ultimately be processed and based on abstract (binary) data stored as a series of '0's and '1's. This in turn will be grouped into either standard variables or more complex record structures, which in turn may be constructed as multi-dimensional arrays.

The accuracy of any evaluation at the raw data level will ultimately be based on the correct interpretation of these data types and their derivatives. Raw file classification should be based on the physical properties of the data, and not just the extension.

It is completely unreasonable to expect an existing function to be able to detect all future data structures that may be used to store data. Therefore, it is important that the output from all automated functions used by the analyst is routinely inspected as part of each case risk analysis.

Similarly, functions used within validated processes cannot be expected to be tested against all possible types of data structure corruption. Instead there is a heavy reliance of feedback from the analyst to detect this type of issue.

In order to carry out these checks it is important that the analyst is either sufficiently trained to detect and compensate for these types of unknowns, or there are procedures in place to routinely inspect the generated output for possible issues.

12.6 Evaluating Disk, Partition and Volume Mappings

The laboratory should always consider the potential for sectors to contain bit or block errors which have not been reported by the acquisition process.

This may be a result of the acquisition system, but can also be a result of undetected errors within the media itself.

Incorrect mappings of this type can corrupt the provenance of data contained on the media, and give the false impression that live data is inaccessible or inaccessible data is live.

When analysing data contained within storage arrays (e.g. RAIDs) the precise mapping used to construct them must be known in order to correctly understand the presented findings.

Additional care must be taken when analysing data from systems (e.g. SSD) that may automatically duplicate data as part of storage and processing algorithms, which have no bearing on actual user activity.

12.7 Evaluating File System Mappings

When extracting data from a file system viewer, it is important to know exactly how it will interpret the file system being viewed. Important elements that must be known include, but are not limited to:

- Sector size and additional padding/control data;
- File system specific files;
- Hidden files and folders;
- Deleted files and folders (and does it assign the correct parent folder);
- The information (i.e. is it in a raw or a parsed form);
- Files which are excessively segmented; and
- File system metadata.

If this information is not accurately known then important accessible information can be missed, or incorrectly reported as either not being present or containing more data than actually exists.

It is also important to understand if the viewer is operating at the physical device layer or at a higher logical level.

12.8 Evaluating the Results of Forensic Filters

When using filters to isolate particular data forms it is important to understand the characteristics of the filter's functionality before determining the best method. Irrespective of the filter selected both the raw data and the analyst input will have a direct impact on the results.

All filters have a set of strengths and weaknesses. Filter selection should therefore be dependent on the requirements of the analyst, the case data being processed, and the available laboratory validated processes.

Human-based review of the outputs from instruments can be expressed as a filter, the accuracy of which will depend on the quantity of data returned and the subjective understanding of each of the individual results.

For this reason it is important that the ambiguities of the chosen solution are incorporated in to the results of any evaluation made.

12.9 Errors in Evaluations and Interpretations

The degree of error must be reported, and will depend on a combination of:

- The combined errors of the processes and measurements used;
- The time constraints to analyse the data;
- The analyst assigned to the case;
- The depth of detail in the case requirements; and
- The type and quantity of evidence located.

This variation in error size based on each unique case is one of the reasons why it is recommended to conduct a unique risk analysis on each case to supplement the general process risk analysis.

Note: The case-by-case risk assessment should be based on the laboratory's available standard validated processes and should be limited to approved variations designed within these global processes.

It is not recommended that laboratories try to design complete validated processes on a case-by-case basis as this would be impossible to track effectively and most likely cripple the laboratory's ability to conduct casework.

Errors detected in evaluation and interpretation should be monitored as part of the peer review process to ensure the variation remains within acceptable constraints and does not compromise existing processes.

This is true for any forensic discipline that relies on at least some element of subjective reasoning, and is especially important in a discipline where proficiency testing is only likely to be a limited sampled subset of the available processes.

The declaration of known error and uncertainty remains vitally important, to ensure the reader of any generated report does not misinterpret or incorrectly weight the evidence the analyst provides within their report and/or statement.

13 PRESENTATION OF EVIDENCE

13.1 General

The overriding duty of those providing expert testimony is to the court and to the administration of justice. As such, evidence should be provided with honesty, integrity, objectivity and impartiality.

Evidence can be presented to the court either orally or in writing. Only information which is supported by the examinations carried out should be presented. Presentation of evidence should clearly state the results of any evaluation and interpretation of the examination.

Written reports should include all the relevant information in a clear, concise, structured and unambiguous manner as required by the relevant legal process. Written reports must be peer reviewed.

Expert witnesses should resist responding to questions that take them outside their field of expertise unless specifically directed by the court, and even then a declaration as to the limitations of their expertise should be made.

It is highly probable that the reader of a forensic report will assume that most, if not all, evaluations, interpretations and comments are factual and without question, unless otherwise stated by the author.

Within the report it is very important that the analyst not only explains all examples, but also declares the known limitations and errors to avoid misinterpretation.

It is extremely important that the context of the data is both understood and accurately represented in any generated reports and statements.

Significant care should always be given to ensure that the provenance of provided results is accurate in terms or both ownership and how the data came into existence on the media being analysed.

13.2 Staged Reports

Staged reports generally relate to an analysis and reporting strategy which is centered on focusing an investigation in an ever increasing depth depending on the strategic nature of the investigation.

Initial stage reports are likely to be a reduced version of a full standard forensic report which has been conducted within a strictly limited timeframe either at the request of the submitting officer, or as part of a standard laboratory reporting strategy.

The increased potential for uncertainty resulting from the limited scope examinations should be stated within the report to ensure the presented results are not misinterpreted or misused later in the investigation and presentation of evidence (see section 10.3).

13.3 Investigative Reports and Opinion

Investigative reports and opinion, within this context, relates to officer specific applications where the information may not be designed to such stringent levels as those that are required for court review / use.

This may be due to the requirement that information is needed urgently, such as in the case of a finding a missing person who is considered at risk, and where the time constraint is the most critical factor.

It is however obviously still important to understand, and be able to detail, the uncertainty so that the officer can make an informed decision on the reliability of the provided investigative opinion.

Note: The increase in errors and uncertainty in the analysis need to be highlighted to the officer to help them make their informed decisions on weighting the information.

13.4 Technical Reporting and Evaluative Opinion

The 2 most common elements used in reporting the findings of digital examinations for court use are:

Technical Reporting - This is the factual reporting of an analysis based solely on the actual evidence located (and competence of the individual) during the investigation.

Evaluative Opinion - An opinion of evidential weight, based upon case specific propositions and clear conditioning information that is provided for use as evidence (for additional guidance see MP2010 STEOFRAE [8]).

A report may consist of one or both elements within it, so long as the transitions in type are clearly distinguishable to any reader.

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.

If oral evidence is subsequently required it is essential that expert witnesses should restrict their evidence to what they have written in their statement / report, and to matters arising which remain within their area of expertise.

If an analyst is required to respond to questions that will take them outside their field of expertise, they must clearly state the increased error and uncertainty in any response they provide.

14 HEALTH AND SAFETY

14.1 General

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.

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.

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 members of the public (e.g. in court).

The relevant safe systems of work should be documented as an integral part of all standard operating procedures.

Laboratory personnel should be responsible for maintaining their assigned work areas in a safe, clean and orderly manner.

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.

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 formally practice these procedures once a year.

At least one designated person should be trained and competent to render “qualified first aid” to those doing casework involving digital technology.

14.2 Control of Substances Hazardous to Heath (COSHH)

Laboratories must ensure that they are compliant with their national requirements concerning the Control of Substances Hazardous to Heath (COSHH).

15 REFERENCES / BIBLIOGRAPHY

15.1 References within the Document

1. **ILAC, G19:2014.** *Modules in a Forensic Science Process.* s.l. : International Laboratory Accreditation Co-operation, 2014. G19.

2. **QCC-VAL-002.** *Guidelines for the single laboratory Validation of Instrumental and Human-Based Methods in Forensic Science.* s.l. : ENFSI\QCC, 2014.

3. **Shannon, Claude E.** *A Mathematical Theory of Communication.* 1948.

4. **NIST.** Uncertainty of Measurement. [Online] October 2000. [Cited: 7 May 2015.] http://physics.nist.gov/cuu/Uncertainty/.

5. **ISO/IEC Guide 98-3.** *Guide to the expression of uncertainty in measurement.* 2008. (GUM:1995).

6. **Zdziarski, Jonathan.** The Importance of Forensic Tools Validation. *Jonathan Zdziarski’s Domain.* [Online] 28 March 2014. [Cited: 7 October 2014.] http://www.zdziarski.com/blog/ ?p=3112.

7. **QCC-PT-001.** *Guidance on the Conduct of Proficiency Tests and Collaborative Exercises within ENFSI.* ENFSI. 2014.

8. **(STEOFRAE), MP2010.** *ENFSI Standard for the formulation of evaluative reports in forensic science.* ENFSI. 2014.

9. **Std754-2008.** *IEEE Standard for Floating-Point Arithmetic.* s.l. : IEEE, 2008.

15.2 International Standards and Guidance

General Requirements for the Competence of Testing and Calibration Laboratories, ISO/IEC 17025, International Organisation for Standardisation, 2005

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

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.

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

ISO 8402:1994 Quality management and quality assurance-Vocabulary

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

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

15.3 General Forensic and Technical Publications

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, ASTME 1459-92

15.4 Other Useful Links to Digital Forensic References

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

16 AMENDMENTS AGAINST PREVIOUS VERSIONS

16.1 Revision History

FIT-2005-001 Version 6. This document was discussed at the ENFSI FIT working group meeting held by the Guarda Civil on 1st-3rd October 2008 in Madrid. The final editing by dr. David Compton (Forensic Science Service – UK).

FIT-2005-001 Version 5. It was agreed at the ENFSI FIT working group meeting held 14th – 16th September 2005 at the Netherlands Forensic Institute. The final editing by dr. Dave Compton (Forensic Science Service – UK) and dr. Zeno Geradts (NFI).

FIT-2005-001 Version 4. This document was finally concluded in Istanbul, Turkey during the 3rd EAFS conference, on September 22-26th, 2003 and final edited by Eric Freyssinet (ICGRN) and dr. Les Russell (Forensic Science Service – UK).

APPENDIX A COMPUTER CONFIGURATIONS

A.1 General

This appendix assumes the reader is already fully aware of standard computer architectures and their electrical characteristics, and so presents the information in a compressed form. If you would like a more detailed review of the information contained within this section then please reference manufacturer's datasheets[14].

Computers are, at their most fundamental level, a binary counting device which uses a sequence of linear and/or parallel instructions to carry out a set sequence of arithmetic and comparison operations on data.

A.2 Electrical Characteristics

Data storage and communication within standard commercial Central Processing Units (CPUs) are generally stored as 2 voltage levels that are abstractly referenced as binary data ('0's and '1's).

When implementing a forensic machine for use within the laboratory analysts should be aware that it is not uncommon for some CPUs to have current ratings that may fluctuate to values in excess of 100 Amps (per CPU socket).

It is therefore, extremely important that laboratories carefully consider the quality of the Power Supply Units (PSUs) they use both for their forensic machines and any forensic acquisition units.

If a connected PSU is incapable of providing a reliable and stable voltage / current for the requirements of the entire system then there is a reasonable chance that some of the stored and transmitted data will become corrupted.

The corruption may take the form of a system crash which can easily be detected, may temporarily alter the data and results in a sporadic and undetectable manner, or may irreversible damage an important exhibit.

A.3 Power Supply Selection

The fact that a power supply states on its packaging that it supplies a specific voltage and current does not guarantee that this is in fact true.

If the PSU does not come with a calibration certificate then it is the responsibility of the purchasing laboratory to review and asses the risks associated with the use of each unique unit purchased.

How individual laboratories handle this risk and uncertainty is up to them, but they must formally acknowledge this with their validation processes and risk assessments, and must base their decision on scientifically gathered information formed from their historical observations.

A.4 Uncertainty and Risk Reduction

To minimise the risk to an acceptable level, it is highly recommended that high quality PSUs are used in all laboratories digital forensic machines.

Additionally, since most modern motherboards will modify at least some of voltages via onboard circuitry, it is advisable that motherboards with high quality power regulation are also selected for use within laboratories.

[14] the reader may also find datasheets for 8086 and 80186 processors a useful reference

The effect of data transmission errors within a system can be reduced by using Error Code Correction (ECC) memory; or equivalents, and ensuring that the memory they purchase is guaranteed to be compatible with the motherboard.

This can be achieved either by purchasing the motherboard manufacturers specific parts, or contacting the memory manufacturer to ensure the memory they resale is guaranteed to work with the specific motherboard.

When wishing to add additional memory to a system it is advisable to ensure that all the system memory is either from the same production batch or is guaranteed to work with the existing memory modules.

APPENDIX B CUSTOM (BESPOKE) DEVELOPMENT

B.1 Custom Software Development

Custom development encompasses software developed both in-house and externally commissioned by the laboratory, and relates to any functions which are used to map[15] or filter data for use by the laboratory. This includes compiled and script-based interpreter functions in the form of:

- Formulae (e.g. spreadsheet);
- Plug-ins;
- Modules; and
- Applications.

Before proceeding with custom development, an assessment should be made as to whether the overhead of development and whole-life support can be suitable offset by the benefit in flexibility and functionality it provides.

Note: The staff-hour costs of whole-life support should not be underestimated, and should always be factored in when determining whether to purchase a 3rd party product or develop a custom solution.

When commissioning an external developer, the laboratory should work with the developer(s) to agree a statement of requirements and a set of milestones early in the project.

Note: Requirements capture, and management, should be central to any development process to aid developing test strategies and whole-life support. The time spent developing this requirement not only builds confidence between both parties, but can save considerable redevelopment costs and time, and can make the difference between a product that can or cannot be used.

Where entitled, the laboratory should always retain access to original (un-compiled) source code and associated test patterns in addition to the final compiled software.

Note: The benefit of retaining access to the source code is that the code can be analysed more deeply and modified if required in the future.

Irrespective of whether the custom software is developed in-house, or via an external developer, the laboratory will remain responsible for ensuring that the developed solution is fit-for-purpose.

Laboratories should maintain a list of all forensic cases on which custom software has been used. This can significantly simplify the identification of the cases where reviews are required if the software is subsequently found to be defective.

All software developed for the laboratory should be subjected to verification, and shall be recorded within the laboratory's software register, along with a history of its version control and verification results.

Note: Special attention should be given to test coverage due to the limited arena in which the code may be assessed by others, and may require either an extended test strategy or the assignment of a higher risk category.

Custom software that is not formally verified will require a higher user competence to help to mitigate the additional risks of false results.

Note: The level of reliability will normally be proportional to the complexity and variability of the test data and the ability of the reviewer to manually verify the results returned.

[15] This also includes data transfers.

Software development practices [1] should follow the laboratory's software engineering best practice documentation. Divergence from normal practices should be restricted to those occasions where it can be shown to be of benefit and risk can be managed.

Staff assigned to write software for a forensic laboratory must be demonstrably competent to do so, and this shall be formally recorded in a competency matrix.

Staff should only be fully signed off as competent once they have demonstrated that they can competently conduct code verification[16].

Consideration should also be given to the supervision of code and test development strategies, especially when code is being developed by junior programmers.All programmers should be aware of the code compilation characteristics of the language(s) they are using. This is especially important when considering the porting of code from:

- One programming language to another;
- 32-bit to 64-bit applications; and
- Linear to parallel processing.

Staff should always be willing to open up their code, and its test strategies, for critical review by another competent developer, and potential users.

Note: Releasing test software to colleagues to try and break can be a useful, and helpfully quick, method to aid understanding the importance of proper testing. It should only be used with great care, and the results manually verified in full.

As a minimum, the amount of design effort devoted to testing the code should be equal to that of developing it, and test design strategies must be built in from the initial design stage.

Note: If this is not the case then the testing phase can increase exponentially, and even result in the code having to be completely rewritten to meet verification requirements. The results of which may mean that, the time spent regaining the trust of the user(s) and fixing the live software is ultimately greater than the time it would have spent testing it properly in the first place.

When designing code for use on a specific case, it should be designed as a generic solution that can be utilised on future casework. This approach has a number of benefits including countering the claim that the method is biased, reducing design cost, and strengthening the reliability of the solution with an ongoing review process.

Exception handling methodologies should always be deployed within created code. In cases where the language compiler does not have exception handling capability then error handling code must be added to carry out equivalent functionality.

Wherever possible it is recommended that Design Pattern [4],[5] methods are used to create modular objects based on parent classes.

Note: For additional code simplification consideration should be given to limiting inherited classes public interfaces to those of the parent class, rather than extending the number of public interfaces. Using this method enables all the unique child classes to be declared as the same parent object (variable).

[16] This includes Unit Testing and Mock[2]; and other test, objects[3] (test provided classes)

When developing script-based solutions for a specific tool care must be taken to ensure the solution is either *locked* to a specific sub-version of the tool, or warns the user that it isn't verified; beyond the tested version, to ensure version upgrades of the tool do not introduce silent (user undetectable) errors.

[1] **Eurolab.** Technical Report No. 2/2006 "Guidance for the management of computers and software in laboratories with reference to ISO/IEC 17025/2005"

[2] **Martin Fowler.** Mocks Aren't Stubs [Online] 2 January 2007. [Cited: 7 May 2015.] http://martinfowler.com/articles/mocksArentStubs.html

[3] **Sandi Metz.** GORUCO 2009 - Solid Object-Oriented Design. *GORUCO 2009.* [Online] 2009. [Cited: 7 May 2015.] http://confreaks.tv/videos/goruco2009-solid-object-orientated-design

[4] **Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides.** *Design Patterns Elements of Reusable Object-Orientated Software.* s.l. : Addison Wesley, 2005. ISBN 0-201-63361-2

[5] **Alan Shalloway, James R. Trott.** *Design Patterns Explained A New Perspective on Object-Orientated Design.* s.l. : Addison Wesley, 2005. ISBN 0-321-247148.

APPENDIX C DATA MAPPING

C.1 General

A typical CPU has no concept of human language or radix number systems. Instead it is up to the software of the system to map these characteristics in a way that can ultimately be interpreted by the user.

The function of mapping these characteristics can introduce both known and unknown errors, either by the selection of an incorrect mapping or system / software bugs.

Therefore, to reduce these types of errors, it is important that careful selection of mapping functions and their sequences are chosen.

By using abstract methods and separating the elements into their atomic structures, it should be possible to not only simplify the validation procedure, but also gain a greater understanding of how one process may affect another.

C.2 Simple Data Mapping

The simplest range based data mappings are

- Boolean (true / false);
- Unsigned / Signed Integer (8-bit, 16-bit, 32-bit, 64-bit, etc.);
- Binary Coded Decimal;
- Binary Floating Point (IEEE754).

Each of these types are range limited, that is to say they have a finite size which is a small subset of their mathematical set type. If you attempt to manipulate data outside of the limited range then errors will occur.

In the case of Binary floating point, errors in mapping will also occur within the limited range due to rounding and binary to denary (base / radix) conversion.

Please see the IEEE754 specification for a more formal description.

C.3 Extended Data Mapping

All other base data types found within a digital system are effectively complex constructs of the simple data maps used to map an abstract meaning.

Common examples include, but are not limited to:

- Character Maps;
- Hash Values;
- Dates and Times.

If the wrong mapping is selected, then an additional error will likely be resident in any results which are generated from processing the poorly mapped data type.

C.4 Array and Record Mapping

In all but the simplest types of stored data, base data types will be combined into Records, Arrays, or complex objects.

Digital forensic examples of which include:

- Logical Disk Images; and
- Files.

In reality there is no technical difference between a disk image and a standard file. (e.g. A raw digital ‘dd’ image of an item of media is commonly stored as a file).

If the exact mapping is not understood, which may be a common issue, then the error and uncertainty will increase proportionally relative to the error of the mapping applied.

The more complex the required mapping structure, the more likely it is that errors (bugs) may exist within either the original algorithm or the current implementation of the algorithm being used.

APPENDIX D FILTERS

D.1 General

The quality of the results returned by a filter will be directly dependent on the accuracy of the mapping currently applied.

It is therefore very important that the potential risks associated with any filter process are identified and where necessary additional processes are put in place to reduce this risk.

There are common elements for any type of filter, which can be used to help simplify the acceptance testing and validation.

The 2 most common groups of filters, which are used extensively within computer and phone based digital forensics are:

- Block Data filters; and
- Search String Filters.

These filters are designed to help the analyst reduce the original amount of raw data to a form which is easier to analyse and hopefully will present the relevant information that is required.

Analysts should always be aware that any filter process is likely to generate unknown errors (uncertainty) in the form of both:

- False Negatives; and
- False Positives.

False negatives are the more dangerous of the two, in that information that could be important to the case will be removed by the filter.

The affect of a false positive is that more data will be presented to the user. This will extend the time and cost required to process the case and may; due to the number of search hits, obfuscate relevant data.

D.2 Semi-Automated Filters

The benefit of these types of filters are that they enable vast amounts of data to be processed in times several orders of magnitude quicker than that which can be achieved by a human.

Automated filter types will generally still rely on interaction from a user to determine the mapping and characteristics of the filter.

These types of filters have elements of uncertainty in both the automated stages and user subjectivity stages.

D.3 Manual User Filters

Any results presented to an analyst; or reader, will be subject to manual filtering either intentionally or subconsciously (cognitive bias [1],[2]) depending on their knowledge and interpretation of the data in front them.

Therefore, care should be taken to try to understand how readers external to the laboratory may interpret the presented results, and try to introduce methods of presenting the data that should help to guide the reader to minimise misinterpretation.

It is important to understand that there will always be an element of uncertainty that cannot be controlled by the laboratory.

D.4 Decreasing the Risk

The level of risk reduction should be proportional, but should also be relevant to processes being undertaken.

The amount of risk present will be directly dependent on the quality of the data that has been identified during the examination.

If the quality of the data is high and abundant then the risk will be much lower and may be sufficiently proportional to not warrant additional analysis stages.

[1] **Itiel Dror**, Practical Solutions to Cognitive and Human Factor Challenges in Forensic Science. Forensic Science Policy & Management 4(3-4):1-9,2013. Copyright © Taylor & Francis Group, LLC ISSN: 1940-9044 print / 1940-9036 online DOI: 10.1080/19409044.2014.901437.

[2] **Itiel Dror and Robert Rosenthal**, Meta-analytically Quantifying the Reliability and BIasability of Forensic Experts. AAFS, Journal of Forensic Science July 2008, Vol 53, No.4 900-904.

APPENDIX E STATEMENT OF REQUIREMENTS

E.1 General

A validated process is one which demonstrably conforms to its statement of requirements. A technical process may be considered to be validated for a particular purpose if, when tested, it meets the stated requirements for that purpose.

The statement of requirements defines the problem to be solved by a technical process. It should provide explanatory text to set the scene for a lay reader, summarising the problem, noting the scope and acceptable risks or limits of any solution and acknowledging the relevant stakeholders. It should be created independently of and without regard to any particular implementation or solution.

The statement must include a list of well-formed, testable requirements.

A requirement is a statement which expresses a need and its associated constraints and conditions. Constraints are restrictions on the design or implementation of the solution, such as interfaces to existing systems, physical size limitations or local policies. Conditions are measurable qualitative or quantitative attributes which can be used to qualify requirements.

Each requirement defines an essential capability, characteristic or quality factor. Each individual requirement statement should be necessary, implementation-free (i.e. it states only what is required, not how the requirement should be met), unambiguous, complete, singular and consistent with the remainder of the requirements in the set.

Requirements vary in intent and in the kinds of properties they represent. They can be grouped together into similar types to aid in analysis and verification.

Examples of types of requirements include:

- Functional – describe the functions or tasks to be performed and will include such considerations as expected inputs and outputs;
- Performance – defines the extent, how well, and under what conditions a function or task is to be performed;
- Interface – defines how the solution interacts with external systems, or how elements within the solution (including human elements) interact with each other;
- Process – include compliance with local laws and processes or administrative requirements;
- Non-functional – define how a solution is supposed to be, including quality requirements such as portability, reliability, maintainability and security, or human factors requirements such as safety, efficiency or health and wellbeing.

Undertaking an exercise to verify the requirements will ensure that the specified requirements are well formed and that the needs of the investigative method have been adequately expressed. It involves an analysis of the recorded requirements to identify problems such as conflicting, missing, incomplete, ambiguous, inconsistent or incongruous requirements. Any identified problems should be resolved before moving on to subsequent assurance stages.

It is important to note that a poorly crafted statement of requirements can lead to a validated process that does not satisfy the needs of stakeholders. Conversely, a well crafted statement of requirements can be used to succinctly convey to a third party the scope and limitations of what may be achieved with the validated process.

If, when tested, a technical process does not meet the statement of requirements, then the process is by definition invalid for that purpose. In such situations:

- The process design or implementation may be modified such that the requirements may be met.
- The statement of requirements itself can be refined to convey more pragmatic or realistic expectations.
- The process could be struck off as invalid for that purpose.

E.2 Non-Standard Technical Processes

In order for standard Instrument-based validation plans to be in compliance with a Statement of Requirements the following must be true (see QCC-VAL-002 S3.1).

Equipment must be within specification, working correctly, and adequately calibrated.

This means that in the case where any equipment is not designed to a nationally recognised traceable standard, (i.e. most forensic IT hardware and software), addition test requirements and risk mitigation shall need to be deployed in order to pass a technical validation plan.

Failure to implement these additional requirements is likely to render a validation plan incompatible with the agreed Statement of Requirements with respect to its agreed technical suitability (in terms of both accuracy and precision).

In the worse case, this could result in a validated process that on-the-surface looks suitable, but on technical assessment is significantly worse than all the completely un-validated methods.

Methods to compensate for the use of non-standard tools within technical processes are detailed in section 6 (Validation and Estimation of Uncertainty of Measurement) through to section 13 (Presentation of Evidence).

E.3 Example Statement of Requirements

The follow statement of requirements example is based on the acquisition of logical block data using the standard LBA method for conventional hard disk drives (HDDs).

Note: The is provided to represent an example of what a statement of requirements could look like and include – rather than specifying exact requirements which are mandatory universal best practice for all laboratories across Europe who are imaging HDDs

For example, incorporating the specific acquisition of data contained within the Host Protected Area (HPA) and / or Device Configuration Overlay (DCO) may not be required; or may even break a specific agreed statement of requirements.

Statement of Requirements (Example) – 'Imaging a conventional HDD'

The following requirements relate to the acquisition of data by 'imaging' a 'conventional hard disk drive', such as may be found in desktop or laptop computing systems, games consoles or task specific systems such as digital video recorders for closed circuit television systems.

The acquisition of data from digital devices which have been lawfully seized from suspected criminals, or provided by witnesses to a crime, is a key initial step in a digital investigation. It is important to ensure that an appropriately comprehensive and accurate extraction of data from the digital device in question is achieved, whilst maintaining the integrity of the evidential chain. This initial acquisition of data forms the foundation of a digital forensic investigation; missed items or mistakes in the acquisition will affect any subsequent digital forensic analysis related to the device.

Stakeholders for this process include the forensic analyst, investigating officers, prosecutors and defence teams, the judicial system and the owner of the digital device.

Definitions:

Conventional hard disk drive: a device which stores user-addressable data on rigid spinning platters coated in a ferromagnetic material. It communicates with a host device via an onboard disk controller over an ATA storage interface (a standard which is maintained by the INCITS technical committee T13). *Note that devices relying upon non-mechanical storage systems are not within the scope of this particular process*.

Imaging: the acquisition of an exact bit-stream copy of the persistently stored user-addressable data, as presented to the host by the disk controller using the Logical Block Address (LBA) scheme at the time of creation of the image. The acquired image will replicate the structure and contents of the user-addressable storage regardless of any file systems which may be present on the device. Data present in ATA-protected areas (HPA, DCO) which are masked by the disk controller will be captured. *Data present in firmware or other vendor-specific areas which are masked by the disk controller (e.g. service areas, servo labels, cached memory stores) will not be captured; they are outside the scope of this particular process*.

Initial high-level customer requirements:

- *To obtain an appropriately comprehensive and accurate read-out of the information stored on the evidence item*;
- *To maintain continuity of the evidence item*.

These high-level items can be translated into the more specific and testable technical requirements set out below.

Requirements:

1. *A complete copy of the persistently stored user-addressable data on the evidence item, as presented at the time of examination by the disk controller using the Logical Block Address (LBA) scheme, shall be acquired.*
2. *The acquired image shall replicate the structure, order and contents of the user-addressable storage on the evidence item at the time of creation of the image.*
3. *Areas hidden by the disk controller using widely recognised standard methods (Host Protected Area, Device Configuration Overlay) shall be acquired*.
4. *Vendor-specific storage areas such as reserved firmware addresses or service modules will not be acquired.*
5. *The process shall interact with a conventional hard disk drive via an ATA interface.*

6. *All unresolved errors encountered during the acquisition of data from the evidence item shall be recorded.*
7. *An auditable link shall be maintained between the acquired data and the original physical evidence item.*
8. *The integrity of the acquired data shall be maintained in a manner which is traceable back to the original acquisition from the physical evidence item.*
9. *The imaging procedure shall not add to, remove or modify the original user-addressable data which is stored on the evidence item.*

   RISK NOTE – In certain circumstances (e.g. a damaged disk or one which features a high degree of data fragmentation) the disk controller may cause changes to occur to the user-addressable data independently of any command or interaction from a host system or imaging process.

   RISK NOTE – In certain circumstances, it may be necessary to modify the behaviour of the disk controller in order to access hidden areas such as Host Protected Areas or Device Configuration Overlays. Any such changes shall be noted in the audit trail.

APPENDIX F MINIMAL REQUIREMENTS FOR TOOLS

F.1 General

In order to determine the ability of a tool to meet the desired requirements it is generally necessary to understand the operational characteristics of the applications that create the original data, in order that the requirements are meaningful.

The purpose of this appendix is to provide the reader with a set of minimal checks that should be applied when considering the verification of specific tool functions used within a full validation method or process.

The common minimal questions that should be asked of any tool function reporting to analyse a specific solution are:

a) What types does the function specify it can handle?

b) Is it capable of handling the complete specification, or is it limited to a subset of the full specification?

c) Can you demonstrate that it does match its reported capability?

d) What are the known conditions under which it is known to fail?

e) How detailed is the information for encountered exceptions?

f) What skill level is required by analysts to use the function?

g) How well does each individual analyst know the tool?

h) What are the affects of data corruption within original information?

i) What external elements can affect the operation of the function?

j) Is the function self contained or reliant of addition user equipment?

k) If it requires the use of a PSU, what are the affects if it is not sufficiently stable?

This information should be at the heart of any created reference sample (test set), and is vitally important in order to ensure what kind of issues will need to be tested in order that the validation method can start to be applied.

F.2 Standard Data Transfer Analysis

The process of message (data) transfer is fundamental to all digital forensic disciplines. Each time data is transferred from one location to another there is the potential that some of the message will either become corrupted or lost.

Note: It is important to remember that during a typical forensic examination on a single forensic computer the amount of data transfer between the storage media, memory modules, graphic card and the CPU will be vast.

Therefore, when selecting a forensic computer solution the following questions should also be asked:

a) What error densities may be present during a data transfer?

b) Are the correct data and power cables being used?

c) What is the probability of undetected errors occurring?

d) How many data transfers are predicted during a standard case?

e) Are methods readily available to help detect and reduce these errors?

f) What affect will modification to the installed software have?

F.3 Data Acquisition Analysis

When evaluating an acquisition process the following minimal question should be asked:

a) Is the power within the quoted manufacturer's specification of the exhibit being acquired?

b) Can the solution detect; and acquire, HPA and DCO areas?

c) Can it overcome encountered data protection and encryption?

d) Can it detect Read errors caused by the source media?

g) Is the solution susceptible to acquisition Write errors?

e) Will it modify the original data on the source media?

f) Does the Acquisition software contain errors?

g) How are read errors stored in the resultant image file?

h) Does the stored image file format allow for bit/byte error detection?

i) Can any tampering of the stored image file be with detected?

F.4 Raw Disk / Volume Analysis

Raw disk analysis in this context covers the ability to combine raw disk data into a form that can be understood by any tool that can interpret a standard partition map or file system.

Raw disk data can be in the form of Logical Disk and Volume controllers / device drivers; and RAID solutions which are map to a set of volumes, which can reside either on physical disks or in the form of virtual disks whose specification may or may not be publically known.

a) Does the tool automatically detect the raw disks?

b) Can it determine if the disk/volume set is incomplete?

c) If parity information is available does the tool make use of it?

d) Does it analyse the mapped file systems and files to ensure the mapping is valid?

e) What information does it return to the user to indicate its level of success?

f) Can multiple raw disks/volumes be processed at the same time, or is a new instance required for each?

g) Can it separate the raw disk metadata from the virtual disk/volume?

h) How does it display raw disks it cannot interpret?

F.5 File System Analysis

Within this context a file system relates to any physical and virtual volume (including databases and container files) that can be used to store user and system files.

The ability of a forensic tool to interpret available file systems is generally fundamental to the success of determining both the construction of all files contained within it, and the investigation of provenance of any identified data.

When analysing any tool reporting to be able to handle specific file systems the results of the following information must be known:

a) What file systems is it capable of interpreting?

b) What variations of specific file systems can it interpret?

c) Can it handle working variants that don't fully comply with the original standard?

d) Can it determine the current status of the file system?

e) Does it give the analyst access to the special system files?

f) Can it show files marked as hidden by the file system?

g) Can it show deleted information in its original form?

h) Does it associate deleted files with the correct parent folder?

i) Is any of the deleted data duplicated within unallocated clusters

j) Can it show data contained within unallocated clusters/sectors?

k) How are the unallocated sectors / clusters grouped?

l) How does it represent metadata that isn't contained with a specific file system but is still assigned a column within the forensic tool?
(e.g. modified and deleted dates and times).

F.6 File Analysis

Within this context file analysis relates to all files stored within a file system, including file images of disks, volumes and file systems

Answers that should be determined at the review stage include:

a) Which files are interpreted (mapped) before processing?

b) Which files are processed as simple byte streams?

c) Can all the file information be accessed?

d) Is encryption and protection information displayed to the user?

APPENDIX G REPORT REQUIREMENTS

G.1 General Requirements

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;
- Details of the Analyst laboratory(s);
- the identity, status and qualifications of the Analyst;
- the signature of the Analyst;
- 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 description of the condition of sealed submitted material and its packaging when received;
- 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;
- whether the processes used are validated or not;
- the results of the examination;
- the provenance of the salient details;
- Details of known limitations in the analysis process;
- Details as to possible uncertainty of specific presented results;
- an assessment of the significance of the results in the context of the information provided;
- Comments covering any items not examined, and the reasons why;
- Details of any submitted items, or parts of such items, not being returned to the submitter, and the reason for this.

G.2 Digital Evidence

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

- Details of the target data sought;
- Presence or absence of data found on the various items; and
- Effects of the examination on the working order of the device. e.g. during the examination the item was (partially) dismantled and the laboratory cannot restore the item to its original state.

G.3 Peer Review

A peer review of a report should include consideration of the validity of all the critical examination findings and should include ensuring that the correct level of provenance is provided.

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 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 the exhibit continuity intact?
- Is the case specific risk assessment available and valid?
- Is there adequate documentation relating to all the items examined?
- Have all the appropriate examinations been carried out?
- Have the relevant procedures and processes been followed?
- Are there complete notes on all the target items?
- Is the statement / report accurate and refer to all items submitted?
- Are the conclusions reached justified and appropriate?
- Was the analysis proportionate?

APPENDIX H EXAMPLE RISK ASSESSMENT

H.1 General

The risk assessment describes the potential risks that can occur in the process, and procedural methods which are in place to limit or detect them.

The columns that should typically be considered when creating a Risk Assessment are:

Header	Description
Unique ID	The ID enables each Risk to be easily referenced.
Category Description	This is the Title of each individual Risk which is to be described.
Associated Risk	A full description of the titled risk which enables the reader to understand the potential Risk that is known to exist.
Likelihood of Risk	A score, typically with a value ranging from 1 to 5 (but can be lab definable range), which describes the likelihood of the risk occurring within the currently implemented control strategy.
Severity of Risk	A score, typically with a value ranging from 1 to 5 (but can be lab definable range), which describes the severity of risk if it was to occur, and its impact on the entire process as a whole.
Risk Factor	An identifier which details the risk by categorizing the multiple of the Likelihood and Severity of Risk, typically given the markings of [L]ow, [M]edium, [H]igh. An example might be: L < 8 (Likelihood * Severity) M < 16 (Likelihood * Severity) H ≥ 16 (Likelihood * Severity) Ideally the Risk Factor should not exceed a Medium level.
Control Strategy	The procedure that is in place to limit the risk to an acceptable level. The information described in this column is designed to reduce the Likelihood of the risk occurring or to implement strategies which can detect when the risk occurs. Through this the risk factor can be reduced to acceptable levels.

Each risk assessment will require the signature and date of the approving technical officer which will typically be the Laboratory Manager.

A further countersigning signature of a higher grade should also be present.

If an assigned signatory does not agree with the generated risk assessment then they should not sign the document. Instead either the document should be amended accordingly or the document signed by someone else of equivalent knowledge and understanding who does agree.

H.2 Example Categories

The following tables contains a list of some of the more common risks associated with the acquisition process.

Note: The Risk Severity given is provided as an example only.

Category Description		Justification	Risk Severity
PSU	PSU Voltage Tolerances	Out of tolerance voltages / Currents can damage both the write blocker and the media being acquired. They can also result in misreading of data from the media.	5
	PSU Current Tolerances		5
	PSU Ripple	Excessive ripple can take the voltage out of specification and damage the media being acquired.	5
Write Blocker	Power switch	A faulty power switch may power on/off temporarily, cause a power down during the acquisition process	3
	Cable wear and tear	Connection/Disconnection cycles will wear the cables	3
	Interface connections	Each Connection/Disconnection cycle has the potential to damage the connector interface.	5
	Anti-static measures	Static discharge may damage both the imaging system and the media being acquired.	3
	Display	Faulty displays may hide deeper problems with the write blocker, or may result in misinterpreted details.	3
	Voltage / Current overload protection	Media requiring power in excess of that supplied by the write blocker will cause problems.	5
	Firmware upgrades	Firmware upgrades have the potential to completely alter the write blocker operational characteristics.	5
BIOS	BIOS updates Motherboard	Upgrades to the motherboard or expansion BIOSs have the potential to alter the way data transfer requests are interpreted / reported to the acquisition tool.	5
	BIOS updates Expansion Cards		5
Software	Operating System	Changes to the OS in the form of updates may alter the acquisition characteristics of the acquisition tool.	4
	Forensic Acquisition Tools	DLL changes and Memory leaks by acquisition tools may alter the acquisition characteristics.	3
	Acquired file Characteristics	Raw image files have the potential to be become altered by user activity.	5

Category Description		Justification	Risk Severity
PSU	PSU Voltage Tolerances	Out of tolerance voltages / Currents can damage both the write blocker and the media being acquired. They can also result in misreading of data from the media.	5
Media	Password protection	Password protected media may be either unreadable or may report misleading data	5
	Spin-up failure	Media spin-up issues may result in corrupt blocks or can irreparable damage the media being acquired.	5
	Bad Sectors	Misreporting of bad sectors may go undetected, and may lead to addition acquisition errors.	4
Media	Hidden Sectors (HPA/DCO)	Data areas obfuscated by HPA/DCO media configuration may result in accessible portions of the media going un-imaged.	4
	SSD Over Provisioning	SSD over provisioning is standard practice from some manufacturers. This data may only be acquired by physical reading of the flash chips.	3
Acquisition	Local Disk	Errors when acquiring to a local storage area.	5
	Network	Errors when acquiring to a network storage area.	5
	Data Movement	Errors when transferring data between storage media.	3

Risk Severity range = 1 – 5

H.3 General Layout Rules

Typically a risk assessment will be orientated in landscape view to enable all the required columns to be easily read.

Best Practice Manual for the Forensic Examination of Digital Technology

ENFSI-BPM-FIT-01

Version 01 - November 2015