MINIMUM REQUIREMENTS FOR DIGITAL AND MULTIMEDIA EVIDENCE

A document for emerging laboratories

International Forensic Strategic Alliance
Version 1

IFSA
International Forensic Strategic Alliance

INTERNATIONAL FORENSIC STRATEGIC ALLIANCE

MINIMUM REQUIREMENTS FOR DIGITAL AND MULTIMEDIA EVIDENCE

A document for emerging laboratories

IFSA MRD 4

IFSA

International Forensic Strategic Alliance

CONTENTS

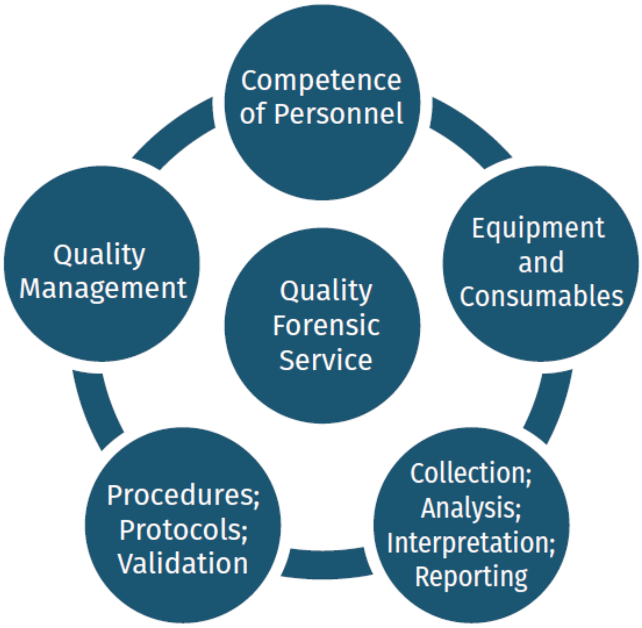
INTRODUCTION

The International Forensic Strategic Alliance (IFSA) has developed this document to be minimum requirements which will enable emerging forensic providers in developing countries to produce scientific services to the Criminal Justice System.

The purpose of this document is to establish a baseline or starting point that must be followed in order to achieve reliable results. Forensic providers should build on this foundation and strive to continually improve the quality of services provided.

This document describes the minimum requirements Digital and Multimedia Evidence Investigation. It addresses the following framework:

1. Competence of Personnel.
2. Equipment and Consumables.
3. Collection, Analysis, Interpretation, Reporting.
4. Procedures, Protocols, Validation.
5. Quality Management.


Competence of Personnel
Equipment and Consumables
Collection; Analysis; Interpretation; Reporting
Procedures; Protocols; Validation
Quality Management
Quality Forensic Service

FOREWORD

The International Forensic Strategic Alliance (IFSA) is a multilateral partnership between the six regional networks of operational forensic laboratories:

- the American Society of Crime Laboratory Directors (ASCLD)
- the European Network of Forensic Science Institutes (ENFSI)
- the National Institute of Forensic Science Australia New Zealand (NIFS ANZ)
- la Academia Iberoamericana de Criminalística y Estudios Forenses (AICEF)
- the Asian Forensic Sciences Network (AFSN)
- the Southern Africa Regional Forensic Science Network (SARFS).

IFSA works closely with its three strategic partners, Leverhulme Research Centre for Forensic Science, United Nations Office on Drugs and Crime (UNODC) and INTERPOL.

IFSA recognises the importance of a quality management framework in forensic laboratories to provide quality and standardised results, be it procedures undertaken in the field or in the laboratory.

In February 2012, at the special IFSA meeting hosted by UNODC and convened in Vienna to discuss the needs of the emerging forensic laboratories in developing countries, a decision was taken to create a set of minimum requirement documents (MRD) filling the gap in recommendations available for the current management of these laboratories.

In October 2014, the first series of three documents in the specific areas of identification of seized drugs, DNA analysis, and crime scene investigation were created. These documents have focused on the critical quality areas, using simple terms and illustrations. All three MRDs have now undergone update and further review with version 2 of these documents published in December 2020. Two MRDs on document examination and toxicology were released in 2023 and at the time of writing, further MRDs including in the areas of anthropology and latent fingerprint analysis are currently in development.

These MRDs are meant to act as a start-up guide for emerging forensic laboratories to quickly establish their quality management system and scientific/technical capabilities. Once achieved, the laboratories should continue to build on this foundation and strive to continually improve the quality of services through undergoing accreditations to established standards.

In the drafting of these documents, scientific working groups and experts from the six regional forensic science networks, as well as IFSA strategic partners, made valuable contributions during the various rounds of consultation. The final MRDs presented in this series would not be possible without the involvement of all.

It is IFSA’s hope that these documents will play an important role for emerging forensic laboratories in their journey towards building quality forensic services.

IFSA Board

November 2023

1 COMPETENCE OF PERSONNEL

All laboratory staff must have a clear understanding of their duties and responsibilities and should fulfil these at all times according to a code of ethics (see the examples in the footnote below) adopted by the laboratory[1].

This section recommends minimum education and training required for laboratory staff to conduct Digital and Multimedia Evidence analysis.

1.1 EDUCATION

This forensic specialty is often complicated by the fact that educational requirements are non-traditional. The needs that have developed for the examination, searching, extraction, presentation, interpretation, and preservation of digital evidence dictate sophisticated and diverse skills not only in more traditional forensic sciences but found commonly in other industries outside the Criminal Justice System, like banking, multi-media, telecommunications, software engineering etc.

This often complicates the development of a singular minimum training curriculum for forensic practitioners responsible for digital evidence examination. Specialists can operate equally comfortably (for example) as multi-media experts employed in the entertainment industry as well as in the forensic science environment.

Higher education requirements although non-specific should be based on the nature and complexity of the tasks to be performed and practitioners (examiner / technicians) should hold a University Degree or an equivalent alternative qualification (e.g. Proprietary System Certification in network, audio video, programming, etc. or a certification strongly focussing on digital forensics from an accredited provider) with a strong emphasis in information technologies. It however remains incumbent upon the Forensic Service Provider to demonstrate laboratory education, training, and experience commensurate with the examination conducted in the laboratory.

The maintenance and development of skill sets of existing digital forensics examiners are a key priority given the highly evolving technical environment. Opportunities for continued education (such as conference attendances, webinars, and review of relevant scientific literature) must be actively sought and should include engagement with like-minded practitioners though professional networks such as those collaborating within IFSA, and formal and informal forums.

In addition to the technical skills pertaining to digital forensics, accomplished practitioners, depending on their role, should have education pertaining to:

- Managing complex investigation environments;
- Preservation and recording of evidence;
- Evidence photography and videography skills;
- Case management systems;

[1] Examples of Code of Ethics adopted by regional forensic science networks:

- The American Society of Crime Laboratory Directors (ASCLD) – www.ascld.org
- The European Network of Forensic Science Institutes (ENFSI) – www.enfsi.eu
- The National Institute of Forensic Science Australian New Zealand (NIFS ANZ) – www.anzfss.org
- la Academia Iberoamericana de Criminalística y Estudios Forenses (AICEF) – www.aicef.net
- The Asian Forensic Sciences Network (AFSN) – www.asianforensic.net

- Strong communication skills (both written and oral), and the ability to convey complex topics in simple terms;
- Ability to present evidential findings in a judicial (legal process) setting.

1.2 TRAINING

The laboratory should have a documented formal training program for the people in charge of carrying out the technical work. The training should be delivered by proficient, competent and experienced practitioners, and consider examiner progression from a generalist through to specialism in a sub-discipline (sub-disciplines are extensive, and include audio and visual processing, encryption, industrial control systems, advanced mobile phone forensics etc.). However, before the laboratory reach this level of expertise, it should consider outsourcing complex analysis and seeking cross-laboratory collaboration.

The type and level of training should consider the service delivery model for the DF team for each agency (e.g. field attendance or laboratory based only).

Consideration could be given to outsourcing of training programs either in its entirety or sections where the Forensic Service Provider lacks commensurate skills and experience (e.g. analyses of financial data, multi-media, etc.) or where the number of examiners to be trained does not justify the creation and maintenance effort required to develop and deliver internal courses. However, this approach should only be considered if it results in a qualification. If all that is provided is a certificate of attendance, then there is no guarantee that someone returning from training will be any more skilled than before they went on the training.

The effectiveness of the training should be evaluated as part of the laboratory's quality system.

Technical skills acquired through formal and informal training courses, obtained through either internal, outsourced, or external courses, should be well documented. Emphasis should be placed on frequency of training considering the constant advancement in the Information Technology field. Wherever a commercial or in-house programme is delivered, examiners undertaking the training should receive certifications following assessment that clearly articulate the area of competence and any timeframes for expiry of that competence. Whilst non-assessed training courses have obvious value in the development of examiners, they should not solely be relied upon when developing new staff members.

Staff or Method should be assessed as competent as well as proficient prior to assuming independent casework and ongoing certification should be ensured through regular evaluation and testing.

Documentation of certification and ongoing professional development is essential.

Training programs should aim to develop the following skills:

- Basic identification, preservation and safe handling of common digital evidence sources;
- Forensic acquisition of digital data for examination;
- Familiarity of cryptographic hashing techniques to enable evidence integrity, and a familiarity with common algorithms (MD5, SHA1,[2] SHA256);
- Validation of file integrity and maintenance of chain of custody at all steps of examination (through the application of cryptographic signing, enventually by a trusted and separately secured third party);
- Preservation of original data in cryptographically-signed "mirror" image(s);
- Examination and analysis of working copies of evidence evidence pertaining to the scope of the analysis;
- Documentation of findings and relevant information to enable reproducibility;
- Interpretation and reporting of results;

[2] Prefer SHA256 rather than MD5 or SHA1

- Detecting abnormalities in results and feeding them back into the quality system; and
- Presentation in Court

2 EQUIPMENT AND CONSUMABLES

2.1 FACILITIES

Wherever possible evidential receipt, handling and storage facilities should be separated from exhibit examination areas (to prevent confusion and potential for loss of evidence, as many digital items look similar).

Areas used for the purpose of acquiring and analysing digital evidence should be connected where possible to uninterruptible power supplies (UPS) to minimise data corruption and evidential loss. An adequate number of power points, anti-static matting, lighting, temperature/humidity control and access control are all considerations.

Food, drink and uncontained liquids should be excluded from any area undertaking processing of electronic evidence.

If undertaking audio processing, the provision of a specialised "sound isolated" environment will greatly enhance the ability of examiners. Similarly, the provision of specialised lighting or shielding thereof will aid the review of video material.

All areas involved in storage, handling and analysis should be secure and access controlled, with all non-authorised people to be always escorted within the facility. They should also sign in/out of a register so that there is a record of when they were in the controlled area

Specific search rooms that can be easily cleaned are advantageous and enable the simultaneous processing of electronic items (a laptop for example) for both electronic and biometric (e.g. fingerprints, DNA) evidence.

The area where electronics device will be stored and handled should be ESD protected to prevent damaes to the evidence.

2.2 EQUIPMENT

The equipment used in the handling, acquisition and processing of electronic evidence is extensive. Equipment that is considered critical for electronic evidence includes (but is not limited to):

- Networks infrastructure and ICT architecture (storage and backup of acquired data);
- Cameras (still and video) for the recording of scenes, exhibits and findings;
- Computers for scene (laptop) and laboratory processing of electronic exhibits;
- Write-blocking equipment (hardware and/or software) to allow the safe connection of electronic exhibits to analysis computers;
- Software (open source, commercial and/or freeware) to allow for the acquisition of cryptographically-signed copies of evidence stores;
- Bootable media and/or other required hardware to allow for interaction and acquisition of exhibits WITHOUT analysis computers;
- Up to date Software (open source, commercial and/or freeware) to allow for the processing and analysis of evidential copies; The software should also propose to fully documented and reproduce the process it uses.
- Mobile telephone extraction devices; and
- Equipment to allow for production of evidence in court formats (e.g. DVD burners)
- Acquisition-related hardware and cables, for more exotic devices

Examiners should maintain and be familiar with multiple operating systems (including Windows, MacOS and Linux).

All analysis laptops, write-blocking equipment and software should be assessed as suitable for the required task. Maintenance and check logs of all critical equipment should be maintained for quality and traceability purposes.

Only members trained in the safe use of such equipment are to connect it to, and interact with, evidential items.

2.3 CONSUMABLES

Common consumable items utilised in electronic evidence examinations include:

- Media for the storage of evidential copies and images:
  - Flash media for use in camera and recording equipment;
  - Flash/USB media/DVDs/Tapes for storage and presentation of smaller-to-mid-size data sets;
  - Loose hard drives for storage of larger data sets;
- Disposable gloves, worn to protect the examiner from hazardous item contamination as well as to preserve integrity of other forensic (usually biometric) evidence, in the case where digital investigation must be done first; and
- Disposable face masks to preserve integrity of other forensic (usually biometric) evidence;

When reusing data storage between examinations and cases, there should exist policies and procedures to protect against data-leakage and contamination of storage media between jobs. For example, records of disk wiping and related verification procedures should be maintained as part of the case file. When disk wiping the procedure must be validated before use to ensure it does correctly wipe disks, with addition check to ensure it works for disks of sizes 4TB+.

3 COLLECTION, ANALYSIS, INTERPRETATION & REPORTING

A modern digital forensics capability can be defined as the expertise to:

- identify,
- preserve,
- acquire,
- examine,
- analyse; and
- report on digital evidence.

3.1 COLLECTION

Searches are conducted to locate and select data of possible evidential value to a case. This often follows extensive examination of storage devices, local area networks, wide area networks, cloud environments, virtual private networks and telecommunication devices in order to determine whether specific devices or environment should be included or excluded as possible exhibit(s). The decision as to why an item was or was not searched and seized should be recorded as a critical decision in the case file.

Electronic evidence consists of data generated or recorded on electronic devices in many of ways. Common data types typically identified during electronic evidence examinations include:

- Active/Logical Data and Metadata (This is data that is visible to a normal user of a system. This document is an example of “active data”);
- Embedded File Metadata and File/Operating System Metadata (This includes information about files stored by a system and can include times and dates, locations and serial numbers of hardware and software) Some types of metadata, like with DVR, could be stored in a non-standard fashion and thus be accessible only through the manufacturer’s software or domain-specific software);
- Backups (This includes data from formal enterprise backups of critical data, mobile telephones or cloud data[3]);
- Inactive (Deleted) Data (This generally includes data which is not visible to a normal user of a system, but which can be recovered using specialised knowledge and tools. Data may be deleted through user activity or automated systems);
- Volatile Data (This is data that disappear when the computer shuts down. The most common example of volatile data is the information stored in the system memory); and
- Telecommunications data (this includes network traffic sent and received as part of a system’s interaction with the internet or intranet).

Common types of electronic items that can provide digital evidence include computers, laptops, mobile devices, mobile app data, cloud data, network data, enterprise systems, CCTV systems, vehicle systems, drones, marine navigation systems, etc.

Consideration of the characteristics of the different types of data is important as these pose different challenges in terms of interpretation of data, extraction of data, recording of results, preparation to present evidential value, containment and storage of evidence, presentation as evidence in Courts of Law, etc. Further, the order of

[3] An examiner must ensure that they do not break national guidelines/laws when dealing with cloud data.

examination should be carefully planned to ensure that volatile, transient data is collected prior to turning off a system, or interacting with it to collect active data (wireless telecommunication isolation).

During collection and processing of electronic items, it is common to encounter information that may be protected or privileged in some way (e.g. under attorney-client privilege, legal professional privilege, or to do with parliamentary/government matters). Facilities should have a process in place to allow for the safe handling of such material, including restricting it to only those members with a need-to-know.

The financial implication of the handling of electronic evidence both for the Forensic Service Provider as well as the Client (e.g. victim, accused, third party, etc.) is an important consideration as it may limit the quality, extent and value of the evidence to the Criminal Justice System.

Hardware and software designed to deal with the sophisticated data encountered in front-end electronic devices as well as enterprise systems are growing in number as these tools aim to manage the exponential growth in generated data, and it is essential the tools used must consider aspects unique to forensic science. Whatever tool is chosen, free or commercial, should be validated before use to ensure it meets all the forensic requirements Imposed on the laboratory

The collection process shall be designed to contemplate the unique challenges faced in Information Technology and should consider the following aspects:

- Identify what you are looking for (prior to commencing an examination);
- Meet the legal requirement for seizure of data and electronic exhibits (such as the conditions of a search warrant);
- Minimize disruption of operations, especially to third-party or data storage facilities;
- Minimize financial implication of collection. This includes the identification and elimination of extraneous data sources at the scene, to prevent the collection and storage of unnecessary data;
- Use separate, specialist forensic examiner systems and networks to store and analyse evidence;
- Adhere to protocols and processes created by the laboratory; and
- Keep records of collection processes and critical decisions.

3.2 ANALYSIS

Once the relevance and possible value of the data present or stored on a device or environment has been determined, an extraction process is designed to maximise the collection of evidence. Careful consideration should be given to the volume of data, preservation of data, risk of data loss and/or destruction and potential risks to all parties affected by the extraction of the data in question.

3.3 INTERPRETATION

3.3.1 Arrange Results:

In considering the unique requirements of the Criminal Justice System relevant to the jurisdiction undertaking the examination, the reporting of findings in for example Courts of Law requires meticulous planning as the production of traditional reporting methods often are impractical when electronic evidence is presented.

3.3.1.1 Organize:

The nature of data present on electronic devices may appear unorganized due to the different storage algorithms. Almost always it will be derived and analysed data that is presented in a Court of Law, as opposed to raw data. Organization of the said data should produce clear and concise information without in any way altering the nature or impact of the metadata.

3.3.1.2 Reduction of Data Volume and filtering:

With the increase in data storage device sizes, and the sheer number of files in a typical system, it has become impossible for an examiner to look at everything that is present on a device. As such, the use of keywords, search terms and file signatures are critical in reducing the data volume to a manageable level. Such data reduction strategies should always be applied with the goals of the investigation in mind and should be recorded as critical decisions so that reproduction of the analytical pathway is possible by a third party. Even with data reduction strategies the quantity of data obtained from enterprise systems often fall outside the capability of even the most developed Forensic Service Provider and requires special consideration and disclosure.

3.3.1.3 Format:

When generating reports consideration should be given to the target audience, and with this in mind data should be presented in a format that they can readily read and understand. If this is not done, then there is a risk of important information being missed or misinterpreted. When converting data for increased readability, links should always be maintained to the original, unconverted data source to allow for traceability.

A common example of this is “timelining” when presenting telecommunication data like call logs found on mobile devices. Without a chronological presentation of the evidence, confusion is likely.

3.3.1.4 Review:

The examination of data extracted from electronic devices often requires comprehensive review of raw data in conjunction with Investigating Officers, clients, legal officers during pre-trial meetings to determine relevance and guard against sweeping collection of irrelevant data, and release of protected data types. A peer review of any generated report should also be part of the process. This feeds into the laboratoty’s quality system, and helps to ensure the report contains suitable information.

3.3.2 Preservation:

Examiners of electronic evidence have a duty to preserve evidence to prevent loss and destruction of data and should approach this duty as followsfollows:

- Maintain custody and control of data acquired from sources;
- Locate and preserve the digital evidence, including Backups & Disaster recover details;
- Document evidence presentation strategies and critical decisions;
- Evaluate jurisdiction issues, data volume, and specificity/scope of requests.
- Wherever possible limit data collection to specific keywords, dates, file names etc.;
- Extract data into designated dedicated folder(s) and use cryptographical hashing functions to ensure data integrity at every transfer.
- Engage with investigators to ensure that requests will not result in data seizures that are too large and cumbersome.

3.3.3 Interpretation of Multimedia:

Signal processing software can be applied to enhance audio and video evidence for investigative purposes, particularly where evidence recordings have been made under less than optimum conditions. It is normally recommended to process the original retrieved evidence, so as not to lose any data. When this is not possible, working on a converted media could be acceptable, provided the conversion process is justified and fully disclosed. The selection of signal processing techniques, such as filtering, is dependent on analysis of the signal, noise and distortion characteristics of the audio-video recording. If enhanced material is presented for Court purposes, examiners will be required to explain the signal processing methodology and the limitations of that methodology. Generally, forensic multimedia examiners do not present interpretations of speech or video content unless they can demonstrate competency in using a method that has been sufficiently validated for the specific case circumstances, and the limitations and assumptions associated with that methodology are understood.

Similarly, interpretations about the source of audio or video recording, or activity associated with producing a recording should only be presented where the examiner can demonstrate competency in applying a relevant and sufficiently validated methodology.

3.3.4 Challenges:

Examiners of electronic evidence may experience the following challenges:

- Sampling of data collection, where total collection is prohibited or impossible;
- The requirement to keep up increasingly complex data sources;
- Increased use of encryption;
- The obligation to use enterprise examination systems to view data;
- The obligation to combine enterprise examination systems to process multiple systems;
- Exposure of digital evidence examiners to disturbing l digital data and imagery, as commonly identified in child exploitation and counter terrorism investigations; and
- The need to acquire cloud-based evidence (legislative power to access remote data).

3.4 REPORTING

Laboratory managers should ensure that any report or statement prepared[4] by an examiner contains the following, minimum items of information:

- A unique case identification number or reference;
- The full name and role of the examiner;
- Details of any relevant information and reference material relied upon;
- Any limitations in the examination (whether imposed by the examiner or investigator) and any assumptions made by the examiner in respect to the analysis;
- A clear laying out of procedures and actions taken by the examiner, including any findings of relevance;
- Clear delineation and identification of factual evidence as opposed to opinion evidence the examiner is authorised to make;
- Reference to the chain of custody for any evidence referred to in the report or statement; and
- Any relevant logs or original evidence attached to the report or statement (whether in paper or digital form) should be specified, or be made available on demand

3.5 DATABASES

To minimise the exposure of examiners to offensive and indecent image material (which can result in undue stress and affect mental health) the use of hashes databases is highly recommended.

These can be simply created and maintained by individual jurisdictions and agencies; however, commonly available databases such as those distributed by Interpol and Project VIC should be considered.

Hashes databases should never be solely relied upon for file identification and processing as human error may result in an incorrect classification, or classifications may be different between jurisdictions.

[4] ILAC G19:2014 S4.9

4 PROCEDURES, PROTOCOLS AND VALIDATION

4.1 PROCEDURES AND PROTOCOLS

The development of protocols by the Forensic Service Provider responsible for examination of electronic evidence should aim to ensure relevance and consider the evolving characteristics of the Information Technology sector aimed at the following:

- Proper communication between stakeholders in investigation is essential and will ensure:
  - Full identification and discovery of all sources;
  - The evidence retained is relevant; and
  - Relevant evidence is produced.

Communication protocols may include processes for consultation with investigators to help determine the type or level of assistance required which will assist focus the Examiner to develop an examination strategy (dates/times, type of evidence) and identify any particular considerations that may impact on the processes or methods (e.g. need to access to cloud data).

The protocols that define and document procedures need to ensure that:

- Examiners must understand and adhere to the protocols that guide processes;
- Examiners must understand the infrastructure that underpin the process;
- Examiners must understand and adhere to the prescribed procedures in all relevant examinations;
- Examiners must understand and document the limitations of their examinations;
- The risks associated with electronic evidence examination should be considered and all procedures should always consider financial implications, disruption of operations, degradationdegredationdegredation of evidence, potential obstruction of Justice, and loss of control and over broadness due to issuance of blanket access orders. Typical considerations are:
  - Identify relevant documents;
  - Notify document owners or custodians;
  - Agree with parties on the examination procedures especially when enterprise system examination is necessary;
  - Preserve relevant documents;
  - Monitor preservation compliance; and
  - Document the process

Certain steps are required when handling electronic evidence and these mainly consist of:

- Collection of electronic evidence;
- Arrangement and organization of case meta-data;
- Review of extracted data for determine relevance; and
- Production of results and reporting.

4.2 VALIDATION

Any tool (open source, freeware or commercial) that is used to process and analyse evidence should be regularly updated when the update improves the existing method or reduces the known risk(s). After each update, it should be assessed for suitability via validation. This ensures that the results can be relied upon and that the error rates of the tools used are known and understood by all parties.

As commercial tools are not always available to deal with every situation, it is common for examiners to produce and develop one-off software tools (commonly called “scripts”) to aid in the processing of evidence. Any such tools should also be tested against a collection of known (ground truth) datasets (where applicable) under variations of both implicit and explicit parameters that define the nature of the specific datasets to ensure that they are operating in the correct manner, and that any derived information or evidence can be relied upon and that the error rates of the tools used are known and understood by all parties. Records of the testing should be maintained.

Write-blocking tools, Associated PSUs and data cables used for the protection of evidential data sources should be periodically checked for proper operation, to ensure that evidence sources cannot be inadvertently changed by the examiner. This is particularly important when a new write-blocking tool is used, or an existing tool is upgraded (whether by software or firmware upgrade). Logs showing the correct operation of write-blocking tools should be maintained for production as necessary in a Court of Law or review process.

5 QUALITY MANAGEMENT

Quality management is a process by which the validity of the work of the electronic evidence examiner can be relied upon. Quality Management should be built in at each step of the process and not checked in at the end. Overall the process should also reflect continuous improvement efforts.

Electronic evidence is somewhat different than the traditional forensic sciences in that many jurisdictions and facilities do not seek or maintain a quality system endorsement such as ISO/IEC 17020 or ISO/IEC 17025. Even if full accreditation is not desirable, consideration should be given towards adoption of parts of such international standards as they can greatly assist enhancement of the quality of laboratory work. As a minimum, a facility should seek to comply with ILAC G19:2014.

At a minimum, the electronic evidence examiner should have a check list of key actions that they monitor (e.g. exhibit details, techniques/processes, software/hardware used) as they are processing the scene and any derived exhibits to assist in maintaining the integrity of the evidence and evidence management (or chain of custody).

The facility should maintain and follow a procedure regarding document retention that specifically addresses:

- Proficiency tests;
- Practitioner competence;
- Validation of the analytical results uaing ground truth datasets;
- Sample receipt and processing records;
- Data retention;
- Corrective actions;
- Audits;
- Training records;
- Continual professional development; and
- Court testimony monitoring.

The quality management program should specify and document the responsibility, authority, and interrelation of all personnel who manage, perform or verify work affecting the validity of the digital investigation.

The use of certified proficiency tests should be considered for the validation of procedures, laboratories and individuals undertaking digital evidence examinations. These proficiency tests, when they are available, should cover a wide range of topics ranging from generic digital evidence handling skills through to highly specialised sub-disciplines. Error rates should be known and reported for all stages of the digtal evidence examination process.

When certified proficiency tests are not available, Collaborative Exercises with similar laboratories should be sought. The main purpose of those should be review of laboratory processes for consistency and validity of work undertaken using known ground truth data. It is an examination of laboratory methods, not an examination of individual staff members.

6 GLOSSARY

The following glossary is not to be considered an exhaustive list of terminology encountered in Digital and Multimedia Evidence however these terms are widely utilized in the forensic community.

DVD	Digital Versatile Disk.
USB	Universal Serial Bus.
ELECTRONIC EVIDENCE	Electronic evidence is any information stored or transmitted in digital or analogue form that is relevant to an investigation or Court matter.
DIGITAL EVIDENCE	Digital evidence is often interchangeable with electronic evidence but can be used to specifically refer to information stored or transmitted in digital form that is relevant to an investigation or Court matter.
MULTIMEDIA EVIDENCE	Electronic evidence pertaining to audio and video recordings and images.

IFSA MEMBERS

ENFSI

NIFS

STRATEGIC PARTNERS

INTERPOL

UNODC
United Nations Office on Drugs and Crime

Leverhulme Research Centre
for Forensic Science
LEVERHULME
TRUST

CONTACT:

International Forensic Strategic Alliance: http://www.ifsa-forensics.org