Digital Forensic Standards for Digital Forensic Practitioners in South Africa

ACFE™

Association of Certified Fraud Examiners

South Africa Chapter #91

TABLE OF CONTENTS

SECTION A ---- 3

1. OVERVIEW ON THE FORENSIC STANDARD FORUM ---- 3

2. THE ACFE ---- 3

2.1 Background on the ACFE SA Chapter ---- 3

2.2 The Preamble of the ACFE SA ---- 4

2.3 Applicability of Code ---- 4

2.4 Standards of Professional Conduct ---- 4

2.5 Standards of Examination ---- 6

2.6 Standards of Reporting ---- 7

3. ACFE CODE OF ETHICS ---- 7

SECTION B ---- 8

1. BACKGROUND FOR THE DIGITAL FORENSIC STANDARD ---- 8

1.1 Overview of the South African Legal Framework ---- 8

1.2 Overview of International Standards ---- 10

1.3 Digital Forensics as a Science ---- 17

1.4 Standing Operating Procedure ---- 18

1.5 SA Caselaw on Expert Status ---- 18

SECTION C ---- 19

1. DIGITAL FORENSIC STANDARD FOR SA ---- 19

1.1 Introduction ---- 19

1.2 Investigation Methodology and Reporting ---- 19

SECTION D ---- 21

1. GUIDELINES WHEN APPOINTING DIGITAL FORENSIC PRACTITIONERS ---- 21

1.1 Introduction ---- 21

1.2 Qualifications, Knowledge & Experience ---- 22

1.3 Capacity and Infrastructure ---- 26

1.4 Risk Management and Data Protection ---- 27

REFERENCE LIST ---- 28

SECTION A

1. OVERVIEW OF THE FORENSIC STANDARD FORUM

The aim of the Forensic Standard Forum under the auspices of the Association of Certified Fraud Examiners, South Africa Chapter (ACFE SA) is to standardise scientific methodologies employed in the course of forensic investigations, which are carried out in conjunction with criminal or civil legislation. Such investigations include almost all disciplines and practices involved.

It is instrumental to lead the way in terms of setting standards in all the disciplines of forensics applied during any given investigation. Although there are well-known and international standards in most of the disciplines, some changes may be required to address the situation in South Africa and Africa in the context of our environment and applicable legislation and/or legal systems and frameworks.

Forensic scientists and criminal investigators need to be guided with acceptable standards and procedures for carrying out such examinations. This document sets forth standards for digital forensic practitioners in South Africa. Although the Association of Certified Fraud Examiners (ACFE) refers to Certified Fraud Examiners (CFEs), it recognises the fact that a strong association exists with forensic examiners and practitioners. All forensic disciplines will accordingly be included in the Forensic Standard Forum.

2. THE ACFE

2.1 Background on The ACFE SA Chapter

The need to raise the standard of fraud examination in South Africa and for a professional body not limited to a specific profession such as accounting or law, resulted in the establishment of a local chapter with the mission to provide a community environment in which local forensic examination practitioners can associate. Local membership provides several benefits including a network of experienced professionals; a training framework for practitioners with "how-to" guidance; technical updates and ethical standards; regular discussion forums on issues relevant to the local environment; annual workshops on fraud examinations; and a video library with case studies. This chapter is a body of individuals in South Africa from all industries, who all have a single goal mind; the reduction of white-collar crime in South Africa.

***(ACFE Professional Standards**:* www.acfesa.co.za)

2.2 The preamble of the ACFE SA

The ACFE is an association of professionals committed to performing at the highest level of ethical conduct. Members of the Association pledge themselves to act with integrity and to perform their work professionally.

Members have a professional responsibility to their clients, the public interest and each other; a responsibility that requires subordinating self-interest to the interests of those served.

These standards express basic principles of ethical behaviour to guide members in the fulfilling of their duties and obligations. By following these standards, all CFEs will be expected to, and all Associate members will strive to demonstrate their commitment to excellence in service and professional conduct.

2.3 Applicability of Code

The CFE Code of Professional Standards applies to all members of the ACFE. The use of the word "member" or "members" in this Code refers to Associate members as well as regular members of the ACFE.

2.4 Standards of Professional Conduct

a. Integrity and Objectivity

- Members will conduct themselves with integrity, knowing that public trust is founded on integrity. Members will not sacrifice integrity to serve the client, their employer or the public interest.
- Before accepting the fraud examination, members will investigate potential conflicts of interest. Members will disclose any potential conflicts of interest to prospective clients who retain them or their employer.
- Members will maintain objectivity in discharging their professional responsibilities within the scope of the engagement.
- Members will not commit discreditable acts and will always conduct themselves in the best interests of the reputation of the profession.
- Members will not knowingly make a false statement when testifying in a court of law or other dispute resolution forums. Members will comply with lawful orders of the courts or other dispute resolution bodies. Members will not commit criminal acts or knowingly induce others to do so.

b. Professional Competence

- Members will be competent and will not accept assignments where this competence is lacking. In some circumstances, it may be possible to meet the requirement for professional competence by use of consultation or referral.
- Members will maintain the minimum Continuing Professional Education (CPE) requirements as set out by the ACFE. A commitment to professionalism combining education and experience will continue throughout the member's professional career. Members will continually strive to increase the competence and effectiveness of their professional services.

c. Due Professional Care

- Members will exercise due professional care in the performance of their services. Due professional care requires diligence, critical analysis and professional scepticism in discharging professional responsibilities.
- Conclusions will be supported with evidence that is complete, reliable and relevant.
- Members' professional services will be adequately planned. Planning controls the performance of a fraud examination from inception to completion and involves developing strategies and objectives for performing the services.
- Work performed by assistants on a fraud examination will be adequately supervised. The extent of supervision depends on the complexities of the work and the qualifications of the assistants.

d. Understanding with Client or Employer

- At the beginning of a fraud examination, members will reach an understanding with those retaining them (client or employer) about the scope and limitations of the fraud examination and the responsibilities of all parties involved.
- Whenever the scope or limitations of a fraud examination or the responsibilities of the parties change significantly, a new understanding will be reached with the client or employer.

e. Communication with Client or Employer

- Members will communicate significant findings made during the normal course of the fraud examination to those who retained them (client or employer).

f. Confidentiality

- Members will not disclose confidential or privileged information obtained during the fraud examination without the express permission of proper authority or order of a court. This requirement does not preclude professional practice or investigative body reviews as long as the reviewing organisation agrees to abide by the confidentiality restrictions.

2.5 Standards of Examination

a. Fraud Examinations

- Fraud Examinations are conducted by professionals/ Fraud Examiners defined as follows: Individuals who make use of specialised skills in the prevention, detection and investigation of fraud and white-collar crimes. Fraud Examiners are registered on the occupational framework as a formal occupation with Organising Framework of Occupations (OFO) code 2019-242215.
- Fraud examinations will be conducted in a legal, professional and thorough manner. The fraud examiner's objective will be to obtain evidence and information that is complete, reliable and relevant.
- Members will establish predication and scope priorities at the outset of a fraud examination and continuously re-evaluate them as the examination proceeds. Members will strive for efficiency in their examination.
- Members will be alert to the possibility of conjecture, unsubstantiated opinion and bias of witnesses and others. Members will consider both exculpatory and inculpatory evidence.

b. Evidence

- Members will endeavour to establish effective control and management procedures for documents. Members will be cognizant of the chain of custody including origin, possession and disposition of relevant evidence and material. Members will strive to preserve the integrity of relevant evidence and material.
- Members' work product may vary with the circumstances of each fraud examination. The extent of documentation shall be subject to the needs and objectives of the client or employer.

2.6 Standards of Reporting

a. General

- Members' reports may be oral or written, including fact witness and/or expert witness testimony, and may take many different forms. There is no single structure or format that is prescribed for a member's report; however, the report should not be misleading.

b. Report Content

- Members' reports will only contain information based on data that is sufficient and relevant to support the facts, conclusions, opinions and/or recommendations related to the fraud examination. The report will be confined to subject matter, principles and methodologies within the member's area of knowledge, skill, experience, training or education.
- No opinion regarding the legal guilt or innocence of any person or party will be expressed.

3. ACFE CODE OF ETHICS

All CFEs must meet the rigorous criteria for admission to the ACFE. Thereafter, they must exemplify the highest moral and ethical standards and must agree to abide by the bylaws of the ACFE and the CFE Code of Professional Ethics.

- An ACFE Member will, at all times, demonstrate a commitment to professionalism and diligence in the performance of his or her duties.
- An ACFE Member will not engage in any illegal or unethical conduct or any activity which would constitute a conflict of interest.
- An ACFE Member will always exhibit the highest level of integrity in the performance of all professional assignments and will accept only assignments for which there is a reasonable expectation that the assignment will be completed with professional competence.
- An ACFE Member will comply with lawful orders of the courts and will testify to matters truthfully and without bias or prejudice.
- An ACFE Member, in conducting examinations, will obtain evidence or other documentation to establish a reasonable basis for any opinion rendered. No opinion w be expressed regarding

the guilt or innocence of any person or party.

- An ACFE Member will not reveal any confidential information obtained during a professional engagement without proper authorisation.
- An ACFE Member will reveal all material matters discovered during an examination which, if omitted, could cause distortion of the facts.
- An ACFE Member will continually strive to increase the competence and effectiveness of professional services performed under his or her direction.

SECTION B

1. BACKGROUND FOR THE DIGITAL FORENSIC STANDARD[1]

1.1 *Overview of the South African Legal Framework*

Digital forensics and the legal system are inseparable life partners. US-Cert (2005:1) defines this relationship as "... the discipline that combines elements of the law and computer science to collect and analyse data from computer systems, networks, wireless communications and storage devices in a way that makes it admissible as evidence in a court of law".

The ultimate goal of digital forensic analysis is to establish reliable facts. If the evidence is questioned, it should withstand scrutiny − most often scrutiny in judicial processes. If the evidence fails the scrutiny of judicial processes, all of the efforts up to that point are wasted.

Casey (2011:23) states that each segment in a digital forensic process should be performed to maintain the integrity of the evidence and to ensure its admissibility. In the case of S v. Ndiki (2008), the court held that digital evidence should be submitted in South African courts as real or documentary evidence and that the relevant rules of evidence should be applied accordingly. The measurement of the integrity of digital evidence is done via the requirements of the regulatory framework.

The statutory requirements of digital evidence in South African courts are set out in the Electronic Communication and Transaction Act (25 of 2002), which is based on the UNCITRAL Model Law on Electronic Commerce (1996) of the United Nations Commission on International Trade Law adopted in 1996 (South African Law Reform Commission, 2010:29).

Some of the most relevant statutory requirements for the authenticity and admissibility of digital

[1] This section contains extracts and adaptations from Nortjé JGJ and Myburgh DC "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" PER / PELJ 2019(22) - DOI http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886.

evidence are set out in Sections 14 and 15 of the Electronic Communication and Transaction Act (25 of 2002). The importance of these two sections in relation to the search and seizure of digital evidence relates to the fact that during searches and seizures, the originality, integrity and reliability of evidence should be maintained. In other words, the actions of police officials on a scene and their subsequent interactions with digital evidence can have a direct impact on the acceptance of evidence in court procedures. Nieman (2009:19) comments on the fact that digital evidence differs drastically from other types of evidence and that the very process of collecting digital evidence can change this evidence in significant ways.

Section 14 and 15 of the Electronic Communication and Transaction Act (25 of 2002) provide requirements for the measurement of digital evidence − normal aspects of the rules of evidence or the subsequent evaluation thereof are not excluded. Section 14 of the Electronic Communication and Transaction Act (25 of 2002) relates to the originality of data messages and stipulates that where the law requires information to be presented or retained in its original form, requirements should be met if the integrity of digital evidence − from the time it was first generated to its final form − has passed the assessment. The integrity of digital evidence is assessed by considering whether the evidence has remained complete and unaltered except for the addition of endorsements, or any changes which can be caused in the normal course of communication, storage or display.

Section 15 of the Electronic Communication and Transaction Act (25 of 2002) relates to the admissibility and evidential weight of data messages. It states that the rules of evidence should not be applied so as to deny the admissibility of data messages. This Act also stipulates that in assessing the evidential weight of data messages, the reliability of how the data messages were generated, stored or communicated and the reliability of how the integrity of data messages should be maintained. The period in which these assessments of reliability takes place should be specified. It is argued that it is logical that the reliability of data should be assessed from the point where data is collected by the forensic investigators or seized from suspects to the point where data is presented in a court.

It will be seen later in this document how Section 14 and 15 of the Electronic Communication and Transaction Act (25 of 2002), actually support international standards − no actions performed by investigators should change evidence and maintaining the reliability of evidence is of the utmost importance. From these Sections, it can be concluded that South African courts test the integrity of digital evidence by assessing whether the evidence was changed by the actions of analysis, and reliability is tested by assessing the methods used in collecting and processing digital evidence.

1.2 Overview of International Standards

Nieman (2009:22) states that it is ironic that digital forensics first and foremost concerns forensic procedure, rules of evidence, legal concepts, precedents and processes and second to this, computers. It is because of this, that standards in this field play such an important role.

In light of the important role standards should play in digital forensics as a science, it is surprising that there has not been a prior drive to adopted or set standards, rules or protocols for the handling of digital evidence and that technical processes applied to digital evidence "do not have to pass any formal test" for digital evidence to be placed before courts (Scholtz, 2009:60). It is, therefore, understandable that the digital forensic industry has largely been self-regulated within a framework of international advised practices, case laws, guidelines and industry groups.

There are too few absolute international standards to standardise the processes and procedures to be followed during digital forensic investigations. This is mainly due to the ever-changing information and communication technology environment and differences in local and international legislation relating to investigation methodology, rules of evidence and court procedures. The majority of standardised processes and procedures are compiled as guidelines as opposed to set standards (International Organisation of Standardisation, 2014:vi).

Some of these that could impact on digital forensics include the American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST) and Scientific Working Group on Digital Evidence (SWGDE). Digital Practitioners should have a sound knowledge of these standards.

a. ACPO Principles

The Good Practice Guide for Computer-Based Electronic Evidence (1997) of the Association of Chiefs of Police (ACPO) was drafted in 1997 and set out principles which digital forensic practitioners should adhere to. These principles were reviewed during an International Hi-Tech Crime and Forensic Conference in October 1999 and were further formalised and accepted in 2001 at the 13th International Criminal Organisation's (Interpol) Forensic Science Symposium of which South Africa is a member.

The ACPO principles have long been a guideline for digital forensic investigators in formulating digital forensic procedures to ensure that the requirements as listed above are met when evidence is collected, handled and managed. The guide contains the following four principles concerning the collection and management of digital evidence (Association of Chief of Police Officers, 1997:4):

- **Principle 1:** No actions taken by investigators should change the data which may be subsequently relied upon in court.
- **Principle 2:** Only in exceptional situations should investigators work with or access the original data and only if they are competent to do so and in a position to provide evidence explaining the relevance and the implications of their actions.
- **Principle 3**: All processes applied to the digital evidence by investigators should be fully recorded to enable independent third-party experts to follow these processes and reach the same results.
- **Principle 4:** Investigators should ensure that all legal principles are adhered to during the analysis of digital evidence.

The principles provide guidelines so that the actions of investigators do not change the digital evidence under investigation and if original evidence is accessed, it should be done by competent persons. A complete audit trail should be maintained so that the actions of investigators could be reviewed, assessed and evaluated against local legal requirements. The SALRC (2010:7) affirmed the importance of these principles when the commission stated that by accessing files, the actions of forensic investigators are not neutral and it is not easy to prove the integrity of digital evidence given the volatile nature of digital evidence. It was also stated that crime-scene protocols and procedures not properly followed, can be rendered digital evidence unusable or vulnerable to claims of prejudicial distortion by the defence.

b. International Organisation of Standardisation

The ISO standards are very well-known, but even the ISO standards seem to shy away from setting rigid standards in a digital forensic environment. In the opening line of the scope of the ISO/IEC DIS 27037 Standard (International Organisation on Standardisation,2012:1), it is stated that it merely provides "guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence".

ISO/IEC 27043 Standard on Information Technology − Security techniques − Incident investigation principles and processes.

In March 2015, ISO 27043 Standard on Information Technology − Security techniques − Incident investigation principles and processes were approved and published. The ISO/IEC

27043 Standard sets out the different phases of a digital investigation. It is divided into two main areas, namely digital investigation processes and concurrent or parallel processes depicted below (International Organisation of Standardisation, 2014).

Digital forensic processes (International Organisation of Standardisation, 2014:14)

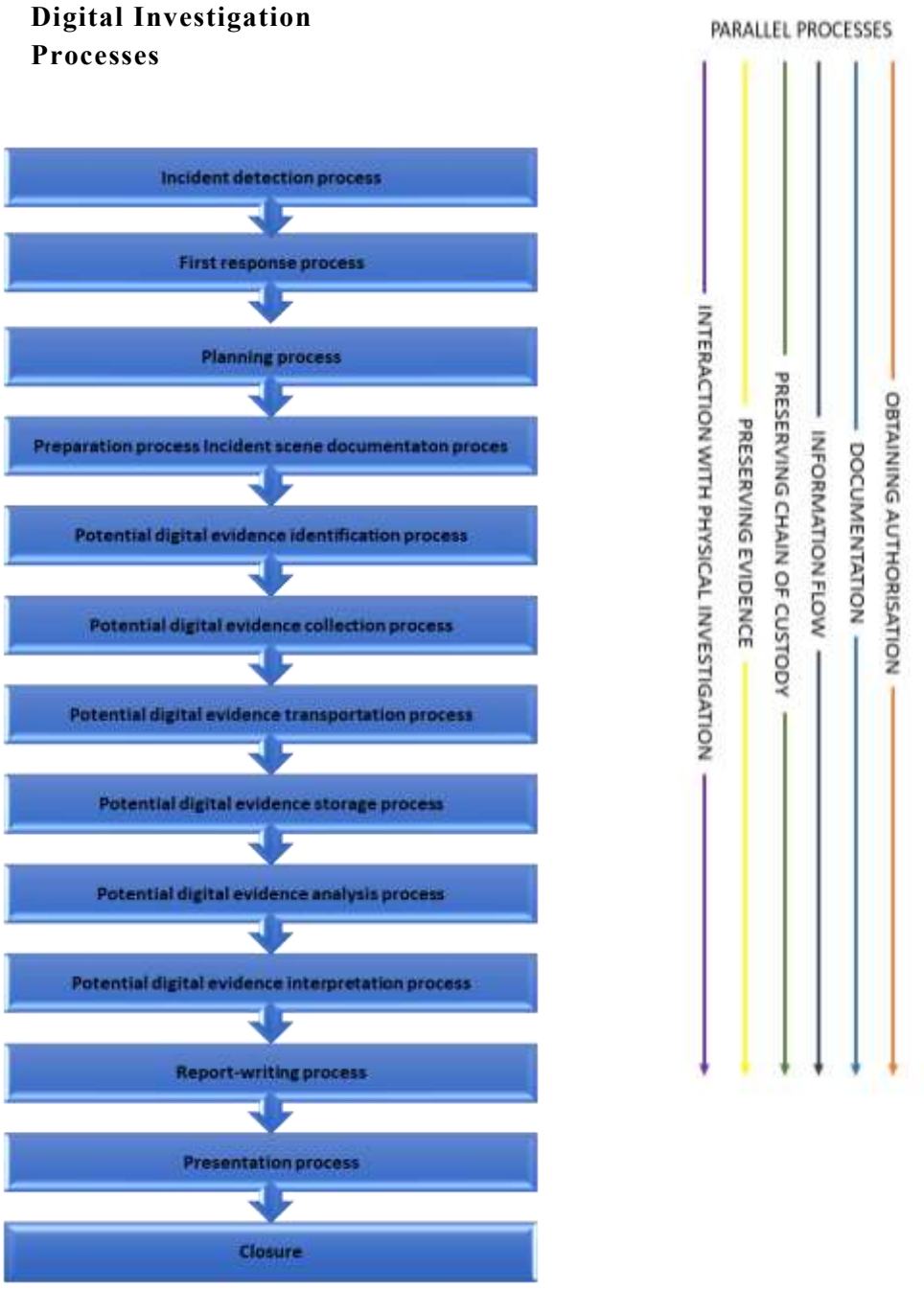

Figure 1

A summary of the different phases of a forensic investigation (International Organisation of Standardisation, 2014:14-21), as depicted in the Figure above include:

- *Detection phase:* incidents are detected.
- *First responder phase:* digital forensic investigators attend to incidents.
- *Planning phase:* investigations of incidents are planned.
- *Preparation phase and scene documentation phase:* preparation steps are taken to investigate incidents and document actions are taken on scenes.
- *Evidence identification phase:* potentially relevant evidence is identified.
- *Evidence collection phase:* evidence is collected.
- *Evidence transportation phase:* evidence is transported from scenes to digital forensic laboratories.
- *Evidence storage phase:* digital evidence is securely stored.
- *Evidence analysis phase:* evidence is analysed to determine relevance.
- *Evidence interpretation phase:* evidence is interpreted in relation to its evidential value.
- *Reporting phase:* evidence is reported on.
- *Presentation phase:* testimonies or overviews are provided regarding evidence.
- *Closure phase:* cases are archived.

The parallel processes include:

- Obtaining authorisation to investigate incidents.
- Documentation of all actions during investigations.
- Continual information flow between digital forensic investigators and forensic investigators.
- Maintaining chain-of-custody.
- Preserving the integrity of evidence.
- Interaction with physical investigations.

A number of the parallel processes set out by the standard is of paramount importance:

Obtaining authorisation:

Proper authorisation should be obtained for each process performed during an investigation.

Authorisation may be required from government authorities, system owners, system custodians and principals. This will influence the format in which authorisation is obtained, which could include, for example, consent or a search warrant in terms of Section 20 or 21 of the Criminal Procedure Act (51 of 1977). The digital forensic practitioner should be aware of relevant requirements in these instances and current case law.

Preserving the chain of custody:

A traditional requirement for proving the integrity of evidence is the chain of custody. Van der Merwe et al. (2008:85) states that the prosecution needs to convince the court that the evidence was not interfered with from the time it was seized to the presentation in court. It is, therefore, critical that forensic investigators should ensure that digital evidence remains secure throughout the analysis (Cross, 2008:211).

A chain of custody requirements was expanded upon in the ISO/IEC DIS 27037 Standard and these requirements relate to the ability of digital forensic investigators to account for all the acquired evidence from the point when it was within their custody (International Organisation of Standardisation, 2012:10). A chain of custody can be viewed as a record that chronologically captures the movements and handling of evidence. A chain of study should contain:

- A unique identifier.
- When, where and by whom the evidence was accessed.
- By whom, under whose authority and for what reason the evidence was checked in or out of storage.
- Any unavoidable changes made to the evidence, by whom the changes were made and a justification for introducing the evidence to the court.

ISO 27037 − Security Techniques − Guidelines for identification, collection, acquisition and preservation of digital evidence.

In October 2012, the ISO 27037 Standard on Information Technology − Security Techniques − guidelines for the identification, collection, acquisition and preservation of digital evidence were approved and published.

The processes specified in the standards set guidelines ensure that digital forensic investigators maintain the integrity of digital evidence during the collection phases of investigations by following analysis methodologies aimed at advancing the admissibility of evidence during legal processes. The importance of the integrity of evidence is supported by Kanellis (2006:58) who emphasises that evidence should be managed correctly so that it cannot lose value and, as a result, be inadmissible in courts. The ISO/IEC DIS 27037 Standard sets forth four fundamental principles for procedures to be followed in collecting digital evidence (International Organisation of Standardisation, 2012:8). Digital forensic investigators should:

- Minimise the handling of original evidence.
- Document all actions that were taken and account for any alterations in the data to allow experts to express an opinion regarding the reliability of the data.
- Adhere to local rules of evidence.
- Not take any actions beyond their competence.

The ISO/IEC DIS 27037 Standard specifies that in most jurisdictions, digital evidence is governed by three primary principles (International Organisation of Standardisation, 2012:6):

Relevance:

A standard requirement is that only relevant data should be collected. In other words, the data collected should assist in examining incidents or aspects of matters at hand and there should be a need and reason for collecting the data. This requirement is supported by Section 28, 31 and 210 of the Criminal Procedure Act (51 of 1977), which regulates wrongful searches and seizures, the inadmissibility of irrelevant evidence and the return of articles not required for criminal proceedings. Digital forensic investigators should be in a position to explain the procedures followed and validate the reasons and grounds for specific data collected. Francoeur (2003:3) explains that the admissibility of any evidence should have an adequate level of relevance to the matter investigated.

Reliability:

All processes followed in handling and analysing of digital evidence should be auditable and repeatable. The result of applying these processes should be reproducible by independent parties when they follow the same process. Hofman (2006b:7) highlights that digital evidence should

satisfy ordinary requirements related to the admissibility of documents. Documents should be authentic, reliable and original.

Sufficiency:

Digital forensic investigators should ensure that all relevant information is collected to ensure that the matter at hand can be sufficiently analysed and considered. Digital forensic investigators should be able to provide an indication of how much data was considered, and justify the basis upon which decisions were made on what data and how much data to acquire.

The ISO/IEC DIS 27037 Standard specifies that all processes concerning digital forensic processes should be (International Organisation of Standardisation, 2012:7):

Auditable:

All processes, procedures and results should be auditable by independent forensic investigators to evaluate the activities performed by digital forensic investigators. Audits can be facilitated if the processes and actions followed by digital forensic investigators are sufficiently documented. Digital forensic investigators should be able to explain the basis upon which decisions were taken on what methodology to follow during analyses.

Repeatable:

Repeatability is established when the same results are obtained in the following situations:

- When the same procedures and methods are used.
- When the same equipment under the same conditions is used.

It should be noted that repeatability is not possible in all situations, for example when live data was analysed or volatile memory. In this case, digital forensic investigators should ensure that acquisition processes are reliable.

Reproducible:

Reproducibility is established when the same test results are produced under the following conditions:

- When the same method is used.
- When different equipment is used under different conditions.

- When the same results can be reproduced at any time after the original test.

Justifiable:

Digital forensic investigators should be able to validate all actions and methods used in identifying, collecting, analysing and managing potential digital evidence. Justification can be achieved by demonstrating that their decisions were best practice in a specific case in obtaining all of the potential digital evidence in existing circumstances.

1.3 Digital Forensics as a Science

ISO/IEC 27043 Standard on Information Technology − Security techniques − Incident investigation principles and processes.

The American Academy of Forensic Sciences identified digital forensics as a forensic science (American Academy of Forensic Sciences, 2008). As a scientific discipline, digital forensics should meet the same standards as other scientific and technical evidence to be admissible in court (Kessler 2010:20). In many instances, it will be required that a person testifying, depending on the nature of the investigation and the level of testimony, should be an expert in the field.

In America, the opinions, theories, processes, procedures and tools used by experts should be evaluated against the Daubert test (Daubert v. Merrell Dow Pharmaceuticals, Inc, 1993), which has for long been the de facto test in the United States of America and is applied by courts to scientific procedures used to prepare or uncover evidence. The Daubert test comprises of the following factors that should be taken into account to ensure the integrity of evidence (Daubert v. Merrell Dow Pharmaceuticals, Inc, 1993):

- The theories and techniques used by experts should have been tested.
- The theories and techniques should have been subjected to peer review and should appear in publications.
- Any error rates should be known to the experts and should have been reported.
- Experts should be governed by standards governing their applications.
- The theories and techniques used by experts should enjoy widespread acceptance.

1.4 Standing Operating Procedure

Standard Operating Procedures (SOPs) are organisational unique documents for digital forensics, describing the methods, guidelines and procedures that should be followed in performing functions aimed at collecting, analysing and reporting on digital evidence for judicial processes. A digital forensic practitioner should have documented SOPs to ensure that processes are performed consistently. The importance of these procedures is highlighted in the Cybercrimes Act, as at the time of drafting this document;

> "(1) The Cabinet member responsible for policing, in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the Cabinet member responsible for the administration of justice must, after following a process of public consultation, within six months of the commencement of this Chapter, issue Standard Operating Procedures which must be observed by — (a) the South African Police Service; or (b) any other person or agency who or which is authorised in terms of the provision of any other law to investigate any offence in terms of any law, in the investigation of any offence or suspected offence in terms of Chapter 2 or section [16,] 17 [or], 18 or 19…"

SOPs are essential to improve the accuracy and quality of the collection and analysis of digital evidence and to implement uniform processes for conducting digital forensic tasks in a precise, comprehensive, accurate and judicially acceptable manner. SOPs should consist of both Guidelines and Procedures. The Digital Forensic Investigator (DFI) has a sound knowledge of all SOPs.

1.5 SA Caselaw on Expert Status

The final draft of the ISO/IEC 27043 Standard on Information Technology – Security techniques − Incident investigation principles and processes (International Organisation of Standardisation, 2014:4), specifies that persons can be considered experts based on their experience, knowledge, skill, training or education. This is in line with the Litigation Skills for South Africa Lawyers (Pg. 213) that states that an expert is a person who, by virtue of his academic qualifications, experience or research (or combination of them), is able to gather evidence that is generally not available to the public.

In SA, two kinds of experts are recognised: one gives evidence on his own investigation, and expresses opinions based on the aspects established, the other is required to give an opinion on facts provided by others (Litigation Skills for South African Lawyers CG Marnewick 2nd Edition Lexis Nexis 2007).

SECTION C

1. DIGITAL FORENSIC STANDARD FOR SA[2]

1.1 Introduction

The prevalence of computers and the attractiveness that the digital medium and the internet holds for perpetrators are well known. The cyber environment has become the playground of syndicates and fraudsters. This digital environment in which crimes are now being committed has resulted in a "new" type of evidence, namely digital evidence. This prompted the beginning of a "new" type of forensic science, namely digital forensics (Kerr, 2005b:86).

Several definitions exist for digital forensics. Palmer (2001:16) captured the main aspects as the use of scientifically derived and proven methods in locating, collecting, preserving, analysing, interpreting, documenting and presenting digital evidence relating to incidents, often to present evidence during hearings. The objective of the process must be to preserve evidence in its most original form while performing a structured process of collecting, identifying, validating and interpreting digital information for the purpose of reconstructing past events connected with the crime.

The ACFE SA adopts and underwrites the International Organisation of Standardisation's - ISO/IEC DIS 27037 and 27043 for digital forensics in South Africa as discussed in section 2.2 supra. The following sets out a framework for inter-alia the adherence to these standards:

1.2 Investigation Methodology and Reporting

- A digital forensic practitioner should not accept assignments for which he is not qualified and experienced.
- A digital forensic investigation should be aimed at establishing facts. It could be that there is insufficient evidence to prove the guilt of a party. It is not up to the digital forensic practitioner to find a person guilty, but to establish facts and to assist the court in arriving at a correct conclusion.
- All aspects of a digital forensic investigation should be performed in accordance with a

[2] This Section contains extracts and adaptations from Nortjé JGJ and Myburgh DC "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" PER / PELJ 2019(22) - DOI http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886.

documented SOP designed to adhere to these specifications.

- Digital forensic evidence must be collected and managed in such a way that it adheres to the requirements of Section 14 and 15 of the ECT Act, Act 25 of 2002. No actions taken by investigators should change the data which may be subsequently relied upon in court.
- Only in exceptional situations should investigators work with or access the original data, and only if they are competent to do so and in a position to provide evidence explaining the relevance and the implications of their actions.
- A digital forensic practitioner may not infringe on a person's right to privacy by accessing data unless duly authorised to do so.
- A digital forensic practitioner may not access information without the authority to do so and may not access data outside the jurisdiction of SA without the authority of the owner.
- Chain of custody should be maintained regarding digital evidence.
- Digital evidence must be collected in a reliable manner and it is advisable that it is done in a sound forensic manner, immune to changes or alterations, and that the forensic copy is maintained throughout the digital forensic process as the original copy of what the data consisted of at the point of collection.
- Only relevant evidence should be collected, subject to the possibility of segregation of relevant and non-relevant data.
- All processes followed in handling and analysing digital evidence should be auditable and repeatable.
- Sufficient evidence should be collected to place a digital forensic practitioner in a position to conduct a comprehensive investigation and to place a digital forensic expert in a position to express an opinion if required.
- All phases of a digital forensic investigation should be performed, documented and reported on, to allow the process to be auditable, repeatable and reproducible by a third party independently, in line with ISO/IEC DIS 27037.
- The digital forensic practitioner should be able to justify all decisions and actions taken during his investigation.
- If a digital forensic practitioner is acting as part of a larger investigation or under instruction from an investigator, he must ensure that no person gains access to more information than what they are entitled to in accordance with their mandate or legal instruction.
- During an investigation by a digital forensic practitioner, care should be taken to limit or focus access on relevant information only and not access all files unnecessarily when such

action can be restricted yet still meet the objective of the investigation.

- Special care should be taken to prevent access to privileged information.
- The theories and techniques used by experts should have been tested.
- The theories and techniques should have been subjected to peer review and should appear in publications.
- Any error rates should have been reported and should be known to the experts.
- The theories and techniques used by experts should enjoy widespread acceptance.
- A digital forensic expert should not testify on the work product of others without validating facts against the original. General forensic practitioners should not be permitted to testify on digital work products but must rely on a digital forensic practitioner to testify on digital evidence.
- A digital forensic practitioner's report should be of such a detailed level that an external expert could validate and test the findings in line with ISO27037. Provision is made that different reports could be issued based on the assignment for example:
  - a scene report – documenting the actions taken during collection;
  - a findings report – documenting the findings of the analysis to be reported to the client;
  - an expert report – aimed at being used during a judicial matter;
  - reports in statement or affidavit format – this can be in a normal format or in accordance with Section 212 or 213 of the Criminal Procedure Act (51 of 1977).

SECTION D

1. GUIDELINES WHEN APPOINTING DIGITAL FORENSIC PRACTITIONERS

1.1 Introduction

We acknowledge the fact that digital forensics is a field that is relatively new within the forensic environment. As such, there are very few, if at all, training courses at South African training institutions that could take a person from novice level to expert level. We therefore also acknowledge that a digital forensic practitioner should have a variety of qualifications and/or

experience in several fields/courses to be considered an expert in this field. The field of digital forensics is wide and could range from simple investigations to large-scale, cross-border sophisticated system compromises.

When considering appointing a digital forensic practitioner/firm, we strongly propose that individuals and organisations be assessed on the following criteria, not all of equal importance:

(it should be noted, that the aim of this document is not to exclude persons/firms, but to be as inclusive as possible. A person cannot be born an expert in a field - it is a never-ending journey of learning and development. A person/firm should not be excluded from evaluation for appointment on a specific assignment based on the following criteria, the aim is rather to select what criteria is important on a specific assignment and then in accordance, to utilise the relevant criteria to evaluate the candidates.)

- Qualifications, Knowledge and Experience
- Experience and Career History
- Lecturing and Publications
- Affiliations
- Capacity and Infrastructure
- Risk Management and Data Protection

1.2 Qualifications, Knowledge and Experience

In general:

- If a person is required to work with the hardware he should have an A+ or equivalent qualification.
- If a person is using accredited or off-the-shelve software such as FTK, Encase, XRAY, Cellebrite or Nuix, he should be trained and if there is an accreditation exam available, he should attain the qualification.
- If open-source software is used, it should adhere to the test if it is widely recognised and accepted by peers, it should have been tested in the industry, the techniques should have been subjected to peer review and should appear in publications, any error rates should have been reported and should be known to the experts.

International Standards:

- The United National Office on Drugs and Crime, the Netherlands Register for Court Experts, and the European Forensic Science Institute, and the American Academy of Forensic Science, all set a minimum requirement of a degree in Computer Science, IT, Engineering or Information Systems. The UK Forensic Science Regulator, the SWGDE, and NIST all recommend a degree in Computer Science, IT, Engineering or Information Systems. The US National Academy of Science says in their research into forensic science standards that the minimum academic qualification in digital forensics must be a degree in Computer Science.
- In terms of minimum training levels, SWGDE generally recommends 80 hours of digital forensics (non-vendor) training.
- A person who only has vendor training e.g. FTK, ENCASE, CelleBrite, Xray, generally does not meet minimum qualifications.
- According to the international standard, you would need to have a degree in Computer Science, IT, Engineering or Information Systems, at least 80 hours of Digital Forensic training (certifications recommended), and regularly pass competency tests, in order to be a qualified practitioner.
- It is however acknowledged that many different function levels exist and not all are required to testify as an expert in court. These practitioners may be assisted by forensic technicians (essentially first responders and people trained to use various tools to extract data only), who would have to be suitably trained to do their jobs but would always have to work under the supervision of a qualified digital forensics practitioner.

Functional Positions	Description	Minimum Years' Experience	Qualification*
First Responder	The person responsible for attending to scenes and/or the forensic collection of digital evidence	1	CFE: Certified Fraud Examiner Trained by a recognised institution/qualified person, or completion of an internship at such an institution in the creation of forensic copies including the utilisation of software and hardware to

			create such forensic copies. If vendor-specific software and hardware is used such as FTK, ENCASE, CelleBrite, Xray, the person should be trained therein and if there is an accreditation examination available, he should attain the qualification.
Digital Forensic Technician	The person responsible for performing functions such as data validation, case indexing, data conversion, data preparation, etc.	2	CFE: Certified Fraud Examiner Trained by a recognised institution/qualified person, or completion of an internship at such an institution in the utilisation of software for such functions. If vendor-specific software is used such as FTK, ENCASE, CelleBrite, Xray, the person should be trained therein and if there is an accreditation exam available, he should attain the qualification.
Digital Forensic Practitioner	A collective name for individuals performing various functions in the digital forensic field with sufficient experience and qualifications in a specific area to which makes him competent to perform such investigative/analysis functions	3 – 5 years	CFE: Certified Fraud Examiner Approved Postgraduate Degree or diploma **Functional** (job-related) • Approved technical certifications • Approved professional certifications including inter-alia: ACE ENCE

			CFCE MCSFS SANS GCFE GCFA GCIH GCCC
Digital Forensic Expert**	A person who is able to perform some or all of the functions in the digital forensic field with sufficient Qualifications, Knowledge, Experience, Career history, Lecturing & Publications and Affiliations in a specific area to express an expert opinion on such field	More than 5 years	CFE: Certified Fraud Examiner Approved Master's Degree **Functional** (job-related) • Approved technical certifications • Approved professional certifications including inter-alia: ACE ENCE CFCE MCSFS SANS GCFE GCFA GCIH GCCC
Incident Responder	A person who responds to a situation where a live security breach is taking place to contain and manage such a situation, this could include forensic, security and ICT network functions	More than 5 years	CFE: Certified Fraud Examiner CEH: Certified Ethical Hacker CISM: Certified Information Security Manager CompTIA Security+

			CISSP: Certified Information Systems Security Professional GSEC: SANS GIAC Security Essentials

* The ACFE notes the international requirements for a degree in computer science, IT, Engineering or Information Systems, while recognising that formal and non-formal prior learning (incorporating experiential learning) might provide functional equivalence to these academic qualifications. As such academic qualifications are regarded as proof of functional, practical and reflective competency, this construct demonstrates the minimum competencies required.

** It is not the intention to qualify a person generically as an expert by setting certain criteria. A person can be an expert in email analysis, while not being an expert on mobile forensics. The criteria as set out in ISO/IEC 27043 Standard on Information Technology - Security techniques − Incident investigation principles and processes (International Organisation of Standardisation, 2014:4), specifies that persons can be considered experts based on their experience, knowledge, skill, training or education, it is advised that such persons be utilised on the specific subject field of an investigation.

Additional requirements:

- Adherence to the ACFE Code of Ethics and Professional Standards;
- Exemplify the highest moral and ethical standards; and
- Abide by the professional CPD / CPE requirements set by the ACFE.

1.3 Capacity and Infrastructure

The complexity of computer systems and cybercrimes is increasing. As a result, both the level of expertise required, and the duration of the investigations are also increasing. In selecting a digital forensic practitioner, it is highly advised that the capacity, infrastructure, lab environment and setup of the practitioner be inspected and consideration be given, in line with the scope and size of the specific investigation, to aspects such as but not limited to:

- The amount of staff of the digital forensic service provider – is it enough to conduct the collection and investigation in a timely manner?
- Whether the digital forensic service provider's staff have relevant experience and qualifications for the specific investigation.

- The number of first responders of the digital forensic service provider.
- The number of computers the digital forensic service provider has with which to conduct investigations.
- Whether the forensic service provider can handle all types of digital evidence – computers, network, mobile devices, social media.

1.4 Risk Management and Data Protection

- Does the digital forensic service provider have sufficient physical and digital security measures in place to protect data and seized devices?
- Is the digital forensic service provider's digital security tested in on a regular basis?
- Does the digital forensic service provider have a date security policy?
- Does the digital forensic service provider have PI and cyber insurance?
- Does the digital forensic service provider guarantee maintaining the integrity of the forensic copy to the point of prosecution?

Reference List

American Academy of Forensic Sciences. 2008. AAFS digital & multimedia sciences. http://www.aafs.org/students/choosing-a-career/types-of-forensic-scientists-disciplines-of-aafs/ Date of access: 5 Jan. 2016.

Association of Chief Police Officers. 1997. Good Practice Guide for Computer-Based Electronic Evidence version 5. http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf Date of access: 27 Dec. 2015.

Casey, E., ed. 2011. Digital evidence and computer crime: Forensics science, computers and the Internet. 3rd ed. Amsterdam: Elsevier Academic Press.

Cross, M. 2008. Scene of the cybercrime. 2nd ed. Arlington: Syngress Publishing.

Kanellis, P. 2006. Digital crime and forensic science in cyberspace. London: Idea Group Inc.

Francoeur, J. 2003. The principles of electronic agreement legal admissibility. http://www.scribd.com/doc/276157/ The-Principles-of- Electronic-Agreement-Legal- Admissibility-WP-8-07 Date of access: 14 Jun. 2016.

Hofman, J. 2006b. Electronic evidence in South Africa. http://hofman@law.uct.ac.za Date of access: 2 Nov. 2014.

International Organisation of Standardization. 2012. Information technology − Security techniques − Guidelines for identification, collection, acquisition, and preservation of digital evidence. Switzerland ISO/IEC (ISO/IEC DIS 27037).

International Organisation of Standardization. 2014. Information technology − Security techniques − Incident investigation principles and processes. Switzerland ISO/IEC (ISO/IEC DIS 27043).

Kerr, O.S. 2005b. Search warrants in an era of digital evidence. Mississippi Law Journal, 75(1):85-108.

Marnewick C.G. 2007 Litigation Skills for South African Lawyers 2nd Edition Lexis Nexis 2

Nieman, A. 2009. Cyberforensics: bridging the law/technology divide. Journal of Information, Law & Technology, (1):1-29.

Nortjé JGJ and Myburgh DC "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" PER / PELJ 2019(22) - DOI http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886.

Palmer, G. 2001. A road map for digital forensic research. Technical report DTR-T001-01, DFRWS, Report from the first digital forensic research workshop (DFRWS). https://isis.poly.edu/kulesh/forensics/docs/DFRWS_RM_Final.pdf Date of access: 10 Nov. 2015.

Kessler, G. 2010. Judges' awareness, understanding, and application of digital evidence. Fort Lauderdale, Florida. Nova Southeastern University, Graduate School of Computer and Information Sciences. (Thesis − PhD).

Scholtz, J. 2009. Towards an automated digital data forensic model with specific reference to investigation processes - A survey of actual and desirable practice. Auckland, New Zealand: Auckland University of Technology. (Thesis − Masters).

Scientific Working Group on Digital Evidence. 2012. SWGDE and SWGIT Digital & Multimedia Evidence Glossary. https://www.swgit.org/pdf/SWGDE%20and%20SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary?docID=60 Date of access: 3 May 2015.

South Africa. 1977. Criminal Procedure Act 51 of 1977.

South Africa. 2002. Electronic Communication and Transaction Act 25 of 2002.

South Africa. 2016. Cybercrimes and Cybersecurity Act.

South African Law Reform Commission. 2010. Issue Paper 27, Project 126 Review of the Law of Evidence Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues. Pretoria

United States of America. 1993. Daubert v. Merrell Dow Pharmaceuticals, Inc. (92-102), 509 U.S. 579 (1993).

United Nations. 1996. United Nation's Commission on International Trade Law's (UNICITRAL) Model Law on Electronic Commerce with Guide to Enhancement. https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf Date of access: 23 Nov. 2015.

US-Cert. 2005. Digital Forensics. https://www.us-cert.gov/sites/default/files/publications/forensics.pdf Date of access: 15 Oct. 2016.

Van der Merwe, D., Roos, A., Pistorius, T. & Eiselen, S. 2008. Information and communications technology law. Durban: LexisNexis.

Document compiled by and date: DC Myburgh, 26 October 2020

Document approved by and date: Jaco de Jager, 29 January 2021