The Current State of Digital Forensic Practitioners in South Africa

Examining the Qualifications, Certifications, Training and Experience of South African Digital Forensic Practitioners

Jason Jordaan
Security and Networks Research Centre
Rhodes University
Grahamstown, South Africa
jason@dfirlabs.com

Dr Karen Bradshaw
Security and Networks Research Centre
Rhodes University
Grahamstown, South Africa
K.Bradshaw@ru.ac.za

Abstract—**Recent high profile court trials around the world, including South Africa, have highlighted the importance of forensic science evidence in court. They have also show what can happen when forensic science is handled poorly in court leading to incorrect convictions or acquittals. Most often the problems have been linked to the qualifications, training, competency and experience of the forensic practitioners who examined and analysed the evidence. With digital forensics being recognised as a forensics science and criminal trials such as Casey Anthony and Julia Amero dominated by errors in the digital forensics process attributed to the examiners, it is crucial to understand what the current situation is in South Africa with regards local digital forensic practitioners, so as to identify any strengths or shortcomings which could impact on digital evidence in a court of law. The research focused on understanding the academic qualifications, digital forensics training, competency, and experience of South African digital forensic practitioners. General trends were identified through the research showing that South African digital forensic practitioners often lacked the necessary academic qualifications, training, competency and experience required of a digital forensics practitioner, raising concerns about the quality of digital forensics practice in South Africa. When contrasted against international standards, the research identified areas of improvement, and suggested potential remedial actions to address the situation.**

Keywords-digital forensics, digital forensic practitioners, digital forensic standards

I. Introduction

Digital forensics is the forensic science discipline that combines various methods from science, technology, and engineering, to acquire and interpret the data stored on digital devices to answer questions in a court of law. While initially focused on cases destined for the courtroom, digital forensics has been used in other applications such as pure and applied research, policy enforcement, information security incident response, and even intelligence gathering [1].

Digital forensics is a critical component in bringing digital evidence to court, as the use of digital forensics follows certain standard processes and procedures, which tend to persuade the court to admit digital evidence and give due and proper evidential weigh to it [2]. In assessing the weight of digital evidence in South African courts, digital forensics plays an increasingly important role [3].

In recent years, courts began to recognise digital forensics as a legitimate scientific method for proving facts that can be used to prove matters in a court of law. This emphasis on digital forensics as a forensic science is important in that it shows that digital forensics is based on generally accepted scientific methods [4], including quality assurance practices. Quality assurance is a crucial aspect of digital forensics as a forensic science discipline, with the quality of the work done being considered the most important aspect [5] owing to the actual or potential consequences of poor quality. The work of a forensic practitioner plays out in a court of law, where defects in the forensic process can produce a flawed product, which can result in an innocent person being punished (having to pay either a fine, receive a prison sentence, or both), as well as having to wrongfully pay out money in a civil lawsuit, or even resulting in a person who actually committed the transgression going unpunished to transgress again. It is important that forensic evidence is correct as the consequences of mistakes can have a very real human cost, and in addition to that cost, public confidence in the courts and justice system itself is damaged [6]. There is a fundamental legal and philosophical maxim that states that it is better for ten guilty people to go free rather than let one innocent person suffer. The innocent can most certainly suffer when there is poor quality in forensic science, and this can never be acceptable. To avoid this happening, the competency of digital forensics practitioners, must be beyond reproach.

In recent years, there has been significant interest in problems in forensic science. While some of the research is generalised to the broader field of forensic science, many of the same problems can be applicable to digital forensics as a specific discipline within the forensic science field. Recent research in the United States identified a number of problems with the practice of forensic science in that country, including inadequate or inappropriate academic qualifications, training, and competency of forensics practitioners [7].

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

The need for continuing professional development for forensic practitioners to remain current and advance to an elevated level of expertise in their chosen discipline is crucial. When forensic practitioners have not kept up-to-date through continuing professional development, their skills and knowledge become outdated, and as a result many forensic cases are flawed owing to a lack of training and contemporary knowledge [8]. The need for continuing professional development is especially critical in the field of digital forensics owing to the rapid changes not only in technology, hardware, and software that must be examined and analysed by digital forensic examiners, but also in the rapid development of tools and methodologies used in the digital forensic process itself, as well as in the legal landscape.

A common mistake that can be made by digital forensic examiners, which can render digital evidence inadmissible, is when they fail to realise that they have reached the limits of their knowledge [9]. One of the basic principles developed in the United Kingdom for computer-based digital evidence [10] which are commonly used throughout the world is that digital forensics practitioners should be competent. The International Organisation on Digital Evidence also set a number of principles to ensure the integrity of digital evidence, including that digital forensic practitioners should be specially trained and have sufficient and relevant experience [11].

Forensic science is compromised if the competency of individual forensic examiners is not assured. A fundamental determination of quality in a forensic laboratory is the technical capabilities of the laboratory, as well as the abilities of the staff members [8]. Quality in forensic science can only be achieved by using competent forensic practitioners that work under the guidance of a quality system. Competence is defined as the mixture of knowledge and skills, application thereof by a forensic practitioner, and the appropriate attitudes and behaviours of the practitioner [5]. Another important element of ensuring the quality of digital forensic processes is to ensure that all digital forensic examiners are technically competent in the field of digital forensics, and do not simply have training in the use of specific forensic tools [12].

Previous research into quality assurance practices in digital forensics in South Africa [13] identified the qualifications, training and certification as an area of concern, however the focus of this research was not on these areas.

With an increasing use of digital forensics in South African courts of law to assist the courts in reaching legal decisions, it is crucial that the best evidence obtained through properly competent and qualified digital forensics practitioners, is presented. The hypothesis of this research is that digital forensic practitioners in South Africa may not have achieved the level of academic qualification, training and competence necessary for the courts to be able to rely upon their findings with confidence due to them meeting objective benchmarks

II. INTERNATIONAL STANDARDS FOR DIGITAL FORENSIC PRACTITIONERS

A number of international standards bodies and digital forensics standards bodies have developed a number of minimum criteria for digital forensics practitioners to address the competency of digital forensics practitioners.

A. Academic Qualifications

The ASTM establishes three essential entry points into a digital forensics career. Two of them require no degree. The first of these is for sworn law enforcement officers who have been assigned to digital forensics duties. The second is for highly skill technical practitioners. The last entry point is for those practitioners who have either an undergraduate or postgraduate degree in digital forensics [14].

The Scientific Working Group on Digital Evidence recommends that digital forensics practitioners should have a relevant bachelor's degree, but does not make it an absolute requirement [15]. The European Network for Forensic Science Institutes recommends that a digital forensics practitioner have a least a degree in a relevant science or engineering discipline [16].

The United Nations Office of Drugs and Crime recommends that digital forensic practitioners have at a minimum a degree in information technology, computer science, mathematics, science or electrical engineering [17].

B. Training

The ASTM and the European Network of Forensic Science Institutes recommends that regardless of which entry path a digital forensics practitioner enters the field, that they must receive appropriate training in the practice of digital forensics before being allowed to perform digital forensics work. Besides this initial training, they must receive regular on-going training to ensure continuing professional education [14]. This is supported by the Scientific Working Group on Digital Evidence, which in addition to the requirements of the ASTM also requires that digital forensic practitioners must complete a minimum of 40 hours of discipline specific training annually [15].

C. Certifications and Competency Testing

The ASTM and the European Network of Forensic Science Institutes recommends that before a digital forensics practitioner be allowed to perform digital forensics work, they be certified as competent through a competency assessment and that these should be regularly conducted [14]. This is supported by the Scientific Working Group on Digital Evidence, which in addition to the requirements of the ASTM also requires that digital forensic practitioners must complete a competency assessment annually [15].

III. THE QUALIFICATIONS, CERTIFICATIONS, TRAINING AND EXPERIENCE OF SOUTH AFRICAN DIGITAL FORENSICS PRACTITIONER

A. Research Methodology

Previous research, which had a limited scope, identified some concerns with regard to the qualifications, training and competence of digital forensics practitioners in South Africa, however this was not examined in depth. This research builds on this initial research and explores these issues in depth. As such an exploratory study is highly relevant .

The research makes use of a structured questionnaire to collect quantitative data from South African digital forensic practitioners for analysis. Quantitative research is appropriate when trying to identify trends and generalisations that can be applied to a whole population [18].

Owing to practical issues such as the nature of the research and the time available to conduct the research, the research was limited in the following respect. The exact size of the population of digital forensic practitioners in South Africa is not known. As a result, the sample size needed to ensure that the sample is statistically representative so that generalisations can be made with regard to the entire population of digital forensic practitioners in South Africa, could not be accurately determined.

Email invitations were sent to the managers/heads of the various digital forensic capacities within all state institutions with a digital forensics capacity, as well as to private sector organisations having a digital forensics capacity, requesting that the invitation be forwarded to all of their employees asking for their participation in the survey. In total, emails were sent to six state institutions and 19 private organisations. A total of 56 responses were received, which were then collated and analysed. Based on the number of responses received, it is felt that the sample represented by the respondents is a fair representation of the total relevant population.

B. Secondary School Education

Digital forensics is a forensic science discipline. Expertise in the field of digital forensics requires far more than product knowledge; it requires a wide range of expertise within the computer science discipline, ranging from basic concepts such as number systems and mathematics through to complex skills in computer science [19]. Many of these foundation skills and expertise are developed in the secondary school system in South Africa, and as such understanding the extent to which digital forensic practitioners have mastered these skills and expertise provides a clearer picture of the foundation skills of digital forensic practitioners.

All of the respondents had completed Grade 12. Thirty-seven had completed Grade 12 with a University exemption (34%), and 19 had completed Grade 12 without a University exemption (66%). Just over a third of the respondents did not pass Grade 12 with a pass mark that would enable them to study at a tertiary academic institution for degree studies. This does have an impact on tertiary studies that are important in the field of digital forensics.

Digital forensics as a forensic science, which itself is considered an applied science, is influenced by the STEM subjects at secondary school level, that is, all subjects in science, technology, engineering, and mathematics. In the context of this research, understanding the core STEM subjects completed by the respondents at secondary school level, establishes the levels of certain foundation skills, which are generally considered important in the practice of science.

Forty-eight respondents had passed mathematics (not mathematics literacy) in Grade 12 (86%), two respondents had failed mathematics in Grade 12 (3%), and six respondents did not have mathematics as a subject in Grade 12 (11%). Thirty-six respondents had passed physical science in Grade 12 (64%), while 20 respondents did not have physical science as a subject in Grade 12 (36%). Fifteen respondents had passed information technology in Grade 12 (27%), while 41 respondents did not have information technology as a subject in Grade 12 (73%).

The majority of the respondents had completed mathematics as a subject at secondary school, which is considered an important foundation in the field of computing. Although physical science is not always considered important in computing, it does make students familiar with scientific principles such as the scientific method, and experimentation, and almost two thirds of respondents had completed this subject. Just under a third of the respondents had completed information technology as a subject, which is understandable considering the age demographics of the respondents, with none of the respondents in the 40-49 and 50-59 age categories having studied information technology at school. For many of the respondents in the 40-49 and 50-59 age categories, information technology would not generally have been available as a school subject.

C. Undergraduate Tertiary Education

While secondary school provides the foundation skills in key STEM subjects crucial for a digital forensic practitioner, additional tertiary study is necessary in general to develop expertise and knowledge.

The National Academy of Science in the United States has recommended that as a minimum, digital forensic practitioners should have a Bachelor of Science degree in computer science or computer engineering [7]. The European Network of Forensic Science Institutes recommends that digital forensic practitioners have a minimum of a degree in computer science or computer engineering [16]. The United Nations Office on Drugs and Crime recommends that digital forensic practitioners should have a degree in information technology, computer science, mathematics, science, or electrical engineering [17].

Thirty-three respondents had completed an undergraduate degree or diploma (59%), while 23 of the respondents had not completed an undergraduate degree or diploma (41%). While 59% of the sample had completed an undergraduate degree or diploma, only 34% had passed matric with a university exemption, which would normally allow them to register to study for a university qualification. However universities do allow mature entry based on age, and not all of the old Technikons required a university exemption to register for a National Diploma. Twenty of the respondents had actually studied National Diplomas.

A breakdown of the undergraduate qualifications of those members of the sample who had completed undergraduate qualifications is given in Table 1.

Table 1 - Undergraduate Qualifications

Undergraduate Qualification	Number of Respondents
National Diploma (Information Technology)	14
National Diploma (Policing)	6
BCom (Information Systems)	3
BSc (Computer Science)	5
BTech (Policing)	1
BTech (Forensic Investigation)	1
BTech (Information Technology)	3
BCom (Forensic Accounting)	1
BCom (Accounting)	1
National Diploma in Datametrics	1
BEng (Civil Engineering)	1
Diploma in Criminal Justice and Forensic Investigation	1

The various undergraduate qualifications were then grouped into specific categories as illustrated in Figure 1.

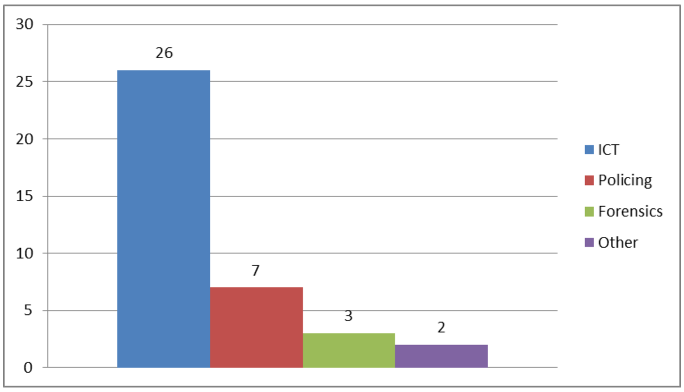

Figure 1 Undergraduate Qualifications by Category

It should be noted that a few respondents had more than one undergraduate qualification and these are shown separately in Figure 1. Next the respondents were grouped into three categories: those with a qualification recommended by the National Academy of Science or the European Network of Forensic Science Institutes, or the United Nations Office on Drugs and Crime; those with other undergraduate qualifications; and those with no undergraduate qualifications. Twenty-three respondents (41%) had no undergraduate qualifications, nine respondents (16%) had an undergraduate qualification not recommended for digital forensics, and 24 respondents (43%) had an undergraduate degree in the subject areas recommended for the practice of digital forensics.

Of the 24 respondents with an undergraduate qualification in one of the fields recommended, only five have a Bachelor of Science degree in Computer Science, which is one of the specific qualifications recommended for digital forensics, while the others have a combination of other ICT qualifications, mostly National Diplomas.

In general, computer science as an undergraduate degree is recommended in the field of digital forensics, as it provides the necessary scientific foundations in the field of computing upon which the practice of digital forensics is based. In essence, computing or computer science is the foundation science for the specialised forensic science of digital forensics.

Not only is computer science a key foundation, a key aspect of computer science graduates is the fact that they never stop learning and continue to be deeply engaged in the learning process post completion of their initial degree in computer science. This is mostly by necessity, because the field of computing is far broader and deeper than that for which any formal education could prepare them and owing to the constantly changing and expanding computing environment.

D. Postgraduate Tertiary Education

Sixteen respondents had completed a postgraduate degree or diploma (29%), while 40 respondents had not completed a postgraduate degree or diploma (71%). A breakdown of the postgraduate qualifications is given in Table 2.

Table 2 - Postgraduate Qualifications

Postgraduate Qualification	Number of Respondents
BScHons (Computer Science)	2
BComHons (Information Systems)	10
MTech (Information Technology)	2
PhD (Information Systems)	1
HDip (Accounting)	1
HDip (Taxation)	1
BComHons (Forensic Accounting)	1

The various postgraduate qualifications were then grouped into specific categories as illustrated in Figure 2.

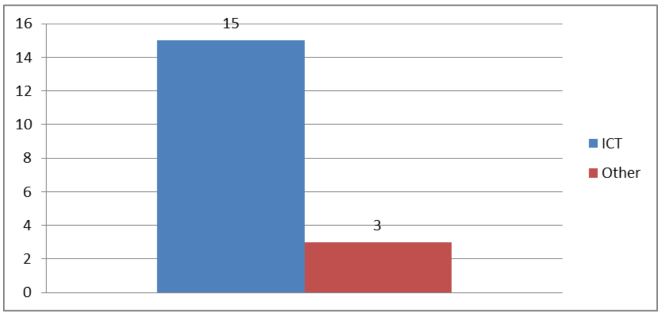

Figure 2 Postgraduate Qualifications by Category

Note that one respondent had more than one postgraduate qualification. Next the respondents were grouped according to their postgraduate qualifications into the following three categories: those with a postgraduate qualification recommended by the National Academy of Science, or the European Network of Forensic Science Institutes, or the United

Nations Office on Drugs and Crime; those with other postgraduate qualifications; and those with no postgraduate qualifications. As shown in Figure 3, 40 respondents (72%) have no postgraduate qualifications, three respondents (5%) has a postgraduate qualification that is not recommended for digital forensics, and 13 respondents (23%) have a postgraduate degree that is at least in the subject areas recommended for the practice of digital forensics.

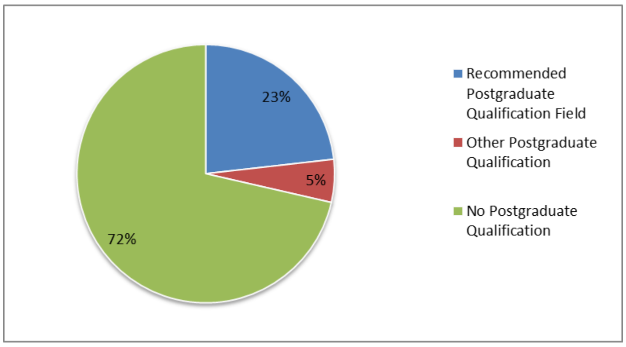

Figure 3 Relevant Postgraduate Qualifications

In South Africa, three tertiary academic institutions currently offer postgraduate taught modules in digital forensics. The University of Pretoria offers an Honours level module in Digital Forensics and Investigations as part of the BScHons Computer Science program [20], the University of Johannesburg offers and Honours level module in Computer Forensics as part of the BScHons Computer Science Program [21], while the University of Cape Town (UCT) also offers an Honours level module in Computer Forensics as part of the Postgraduate Diploma and BComHons degree in Information Systems [22]. It must be pointed out that neither of these three degrees is a digital forensics degree, but either a computer science or information systems degree with a digital forensics module.

Eleven of the respondents with a postgraduate diploma or degree had completed a taught module in digital forensics. Ten respondents had completed the Computer Forensics module at the University of Cape Town and one had completed the Digital Forensics and Investigations module at the University of Pretoria.

The prerequisites for registration for the University of Cape Town course are a three year undergraduate degree in computer science or information systems and at least three years relevant commercial experience; a degree or NQF[1] level 7 diploma in another field and at least three years commercial experience with some IT exposure; or a minimum of five years relevant high-quality full time IT work experience [22].

The prerequisites for registration for the University of Pretoria course are a BSc degree in Computer Science (or equivalent) with an average of 60% in all of the third-year computer science modules [20].

Figure 4 shows the previous academic qualifications of those respondents who had completed the respective postgraduate degrees from either the University of Cape Town or the University of Pretoria.

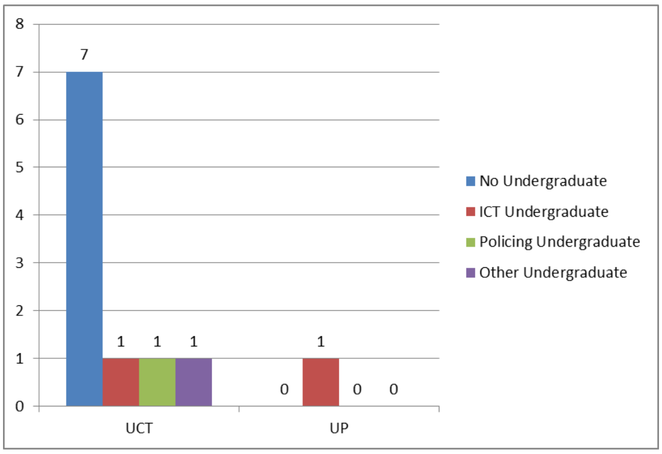

Figure 4 Undergraduate Degrees of Relevant Postgraduate Degree Holders

Nine of the respondents who obtained the University of Cape Town qualification had no undergraduate qualification in any of the fields recommended by the National Academy of Science, the European Network of Forensic Science Institutes, or the United Nations Office on Drugs and Crime, while seven had no undergraduate qualification at all. Of the respondents that had completed the University of Cape Town course, 90% did not have a relevant undergraduate qualification. The researcher is of the opinion that this is a cause for some concern, as while the UCT qualification teaches digital forensic fundamentals, students do not have the necessary computer science fundamentals from an appropriate undergraduate degree. Digital forensics is seen as a specialisation of computer science, and having a student complete a postgraduate degree in digital forensics without the appropriate academic foundation would be similar to allowing a student to study an advanced medical specialisation such as neurosurgery, without them having ever studied medicine or surgery. Forensic science is an applied version of the foundation scientific discipline on which it is based, and so for example, forensic toxicology would be the application by a toxicologist of his/her scientific knowledge of toxicology to a legal application [23]. Similarly, in a computing environment, digital forensics would be the application of scientific knowledge from the field of computer science to a legal application. This position is supported by other research, which compared the general discipline of forensic science to computer forensics [24].

It must however be stated that 4 of the respondents who had completed the University of Cape Town course without an appropriate undergraduate qualification did have five or more years' experience in the field of digital forensics, which did meet the entrance criteria for the qualification. The remaining 5 candidates however had less than 5 years' experience.

E. Digital Forensics Training

As has been established by the literature, the training of digital forensic practitioners in the field of digital forensics is crucial and a key determinant of quality. It is thus important to

[1] NQF (National Qualifications Framework) is the framework used in South Africa which groups all education and training activity into specific levels. An NQF level 7 diploma is considered the equivalent of a Bachelor's degree in this framework.

understand the training that digital forensic practitioners in South Africa have received. Before a digital forensic practitioner (or any forensic science practitioner for that matter) examines and analyses any evidence, they should have the basic scientific education in the form of an appropriate Bachelor's degree, as well as discipline specific training [7].

Forty respondents had received some form of formal digital forensics training (71%), while 16 respondents had not received any formal digital forensics training (29%).

It is concerning that 29% of the sample, almost a third, had received no formal training in the field of digital forensics.

Digital forensics training was classified in two categories. The first category related to vendor training, which is digital forensics training provided by vendors of specific hardware or software tools used in digital forensics, and focuses on the use of those tools in digital forensics. The second category of digital forensics training was vendor neutral training. Vendor neutral training is training that is provided by organisations other than vendors of specific hardware or software tools used in digital forensics, which focuses on the practice of digital forensics.

Thirty-six respondents had attended vendor training courses, while 21 respondents had attended a vendor neutral training course. This is illustrated in relation to those respondents that had received no formal digital forensics training in Figure 5 which clearly shows the dominance of vendor training in the sample.

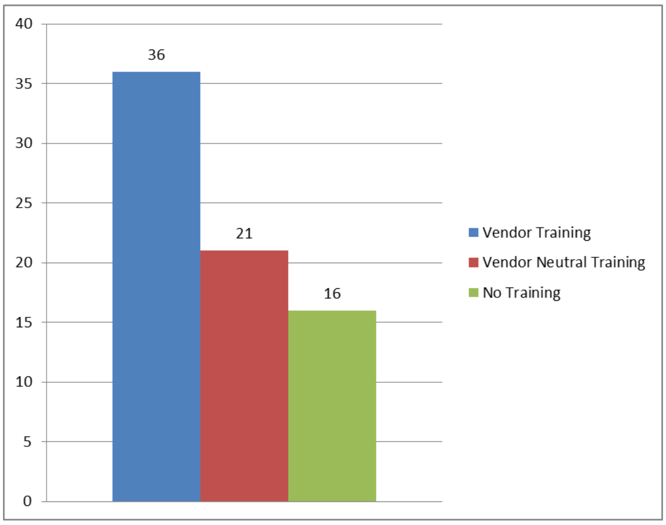

Figure 5 Vendor vs Vendor Neutral Training

The specific vendor courses that members of the sample had attended, and how many had attended each course are reflected in Table 3.

Table 3 - Vendor Courses Attended

Training Course	Number of Respondents
EnCase Computer Forensics I	23
EnCase Computer Forensics II	21
EnCase Advanced Computer Forensics	11
Accessdata Bootcamp	19
Accessdata Forensics	15
Accessdata Windows XP Forensics	2
Accessdata Windows 7 Forensics	1
Accessdata Windows Registry Forensics	1
Accessdata Internet Forensics	2
Accessdata Mac Forensics	1
Accessdata Applied Decryption	1

The vendor courses attended reflect the courses available in South Africa that are offered by the vendors of the two most common digital forensic suites used in South Africa, namely EnCase and FTK.

Another important element in ensuring digital forensic quality is that the competency of digital forensic practitioners must not be limited only to training in the use of specific forensic tools [12]. Digital forensics training has been dominated by vendor specific training, which is little more than training on how to use specific tools, but this does little to develop the overall skills and competencies of a digital forensics practitioner owing to the often narrow product specific curriculum [19].

The specific vendor neutral courses that members of the sample had attended, and how many had attended each course are reflected in Table 4.

Table 42 - Non-Vendor Courses Attended

Training Course	Number of Respondents
EC Council Computer Hacking Forensic Investigator	3
SANS408 Windows Forensics In-Depth	15
SANS508 Advanced Incident Response	1
SANS610 Malware Analysis	1
Ernst and Young Computer Forensics	2
KPMG Computer Forensics	1
GDN (French Police) Computer Forensics	1
FLETC Seized Computer Evidence Recovery Specialist	1

F. Competency Testing

None of the sample (0%) conducted competency or proficiency testing within their workplaces as recommended by the Scientific Working Group on Digital Evidence [15], European Network of Forensic Science Institutes [16], or ASTM [14].

G. Digital Forensics Certification

Digital forensics certifications were classified into two categories. The first was vendor certification, which certifies the competency of a holder of the certification in using a particular digital forensics tool. The second category was technical certifications that certifies the competency of the holder of the certification either in the general practice of digital forensics, or specialised practice in a specific area of digital forensics.

Seventeen respondents had earned a vendor certification (30%), and 6 respondents (11%) had earned a technical certification. This is illustrated in relation to those respondents that had no digital forensics certifications. While respondents having no certifications dominates, it is clear in Figure 6 that in as far as those respondents that have digital forensics certifications, that vendor certifications are the dominant type of certification.

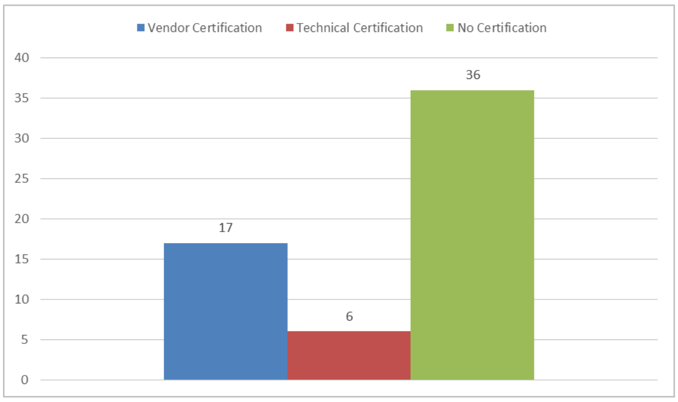

Figure 6 Types of Certifications

The specific vendor certifications that members of the sample hold are reflected in Table 5.

Table 5 - Vendor Certifications

Vendor Certification	Number of Respondents
EnCase Certified Examiner (EnCE)	2
Accessdata Certified Examiner (ACE)	15

The EnCE tests competency in the use of the EnCase software suite and consists of a written and practical test, which once earned must be renewed every three years [25]. To maintain the certification, holders must complete 32 hours of continuing professional education within those three years [26]. There is no need to retake the examination.

The ACE tests competency in the use of the FTK software suite and consists of a written test with a theoretical and practical component. The certification is valid for 2 years and the examination must be retaken every 2 years to retain the certification [27]. They are not required to complete any continuing professional education.

The specific technical certifications that members of the sample hold are reflected in Table 6.

Table 6 - Technical Certifications

Vendor Certification	Number of Respondents
GIAC Computer Forensic Examiner (GCFE)	6
GIAC Computer Forensic Analyst (GCFA)	1
GIAC Reverse Engineering of Malware (GREM)	1

All 6 held the GCFE and 1 held that and the GCFA, and another that and the GREM.

The GFCE tests competency in the examination of Windows computers. The GCFA tests competency in conducting advanced enterprise incident response, and the GREM tests competency in the examination of malware. Each of these certifications consists of a written test and is valid for 4 years. To retain the certification the holder must complete 36 hours of continuing education in 4 years, or rewrite the examination [28].

H. Digital Forensics Experience

Four respondents had less than one year's experience as a digital forensic practitioner (7%), one respondent had between one and two years' experience as a digital forensic practitioner (2%), 17 respondents had between three and five years' experience as a digital forensic practitioner (30%), 17 respondents had between six and ten years' experience (30%), 15 respondents had between eleven and fifteen years' experience (27%), and two respondents had more than fifteen years' experience (4%).

Twenty-three respondents had worked as digital forensic practitioners in a government law enforcement, intelligence, or military agency (41%); four respondents had worked in other government agencies (7%); 40 respondents had worked for private organisations that provided digital forensic services to other organisations (71%); and 13 respondents had worked for private organisations providing digital forensic services within their own organisations only (23%).

The majority of the sample had at 6 or more years' experience, and as such the sample represented a fairly experienced group of digital forensics practitioners.

Digital forensic science, as all forensic sciences, is considered by many to have its own intrinsic quality metric, namely, the evidence admitted into court and which stands up to vigorous cross examination [9]. Testifying in court is a key and crucial part of the digital forensics process and experience in this activity is crucial. Only respondents had testified in a court of law in their capacity as digital forensic practitioners (45%), while 31 respondents had not testified in court (55%). This is a cause for significant concern. If digital forensic practitioners are not testifying then they are not being challenged at all about their competency.

IV. FINDINGS

The data received from the respondents tends to confirm the initial hypothesis that that digital forensic practitioners in South Africa may not have achieved the level of academic qualification, training and competence necessary for the courts to be able to rely upon their findings with confidence due to them meeting objective benchmarks

A. Academic Qualifications

While there is no absolute requirements that a digital forensics practitioner should have a degree in computer forensics, there is a strong recommendation that they should. The National Academy of Science report into the state of forensic science in the United States however makes it clear that to improve forensic science, including digital forensics, forensic practitioners should hold appropriate scientific degrees. Based on this only 46% of the sample have an appropriate undergraduate degree, while 23% of the sample have an appropriate postgraduate degree.

B. Digital Forensics Training

Formal digital forensics training is a requirement in all the international standards examined, and specifically vendor neutral training on core digital forensics skills and knowledge. Only 37% of the sample had received this type of training, with the majority of these having attended the SANS408 Windows Forensics In-Depth course in the last four years. 64% of the sample had at least attended training in the use of specific digital forensics software, but this is not substitute for the type of digital forensics training required. What is concerning is that 29% had received no training at all.

Of even greater concern was the fact that only 4 respondents (7%) had attended multiple training courses which would suggest a certain level of continuing professional education. This means that 93% were not engaging in continuing professional education which is required by the international standards examined.

C. Competency Testing

Regular independent competency testing is a requirement in terms of all of the international standards examined, however none (0%) of the sample did any type of competency testing. This is cause for significant concern as there is a crucial method to objectively demonstrate competency.

D. Digital Forensics Certification

Digital forensics certifications can at least provide a certain objective measure of competency that could go party to meet competency testing requirements, provided that there is mandatory retesting. Only 6% of the sample had earned a technical certification which did cover digital forensics fundamental skills, however none of these required mandatory retesting provided the holder completed a 36 hours in a four year cycle (9 hours per year). These certifications would thus not meet the requirements for competency testing as identified in the international standards examined. 30% of the sample had earned a vendor certification which would not be adequate to show digital forensics competency in general. However of the two certifications that members of the sample had earned in this area, at least one, the ACE, required mandatory retesting.

V. RECOMMENDATION

The research illustrates the general poor state of digital forensic practitioners in South Africa when it comes to comparing qualifications, training, competency, and certifications to international standards. The reality is that digital forensic practitioners in general to not match up to objective standards.

While we have some academic courses addressing digital forensics, it would be prudent to research the need for a formal academic program in digital forensics which could meet the necessary academic requirements of digital forensics practitioners. Coupled with this would be the need to research the development of a competency framework for digital forensics practitioners, as well as the development of a continuing education framework for this field in South Africa.

REFERENCES

[1] G. C. Kessler, “Advancing the Science of Digital Forensics,” *Computer,* vol. 45, no. 12, pp. 25-27, December 2012.

[2] D. Van Der Merwe, A. Roos, T. Pistorius and S. Eiselen, Information and Communications Technology Law, Durban: LexisNexis, 2008.

[3] L. Meintjes-Van der Walt, “Electronic Evidence,” in *Cyberlaw@SA III*, S. Papadopoulos and S. Snail, Eds., Pretoria, Van Schaik, 2012.

[4] L. Volonino, R. Anzaldua and J. Godwin, Computer Forensics Principles and Practices, Upper Saddle River: Prentice Hall, 2007.

[5] M. J. Fereday and I. Kopp, “European Network of Forensic Science Institutes (ENFSI) and Its Quality and Competence Assurance Efforts,” *Science & Justice,* vol. 43, no. 2, pp. 99-103, 2003.

[6] House of Commons Science and Technology Committee, “Forensic Science on Trial,” The Stationary Office Limited, London, 2005.

[7] National Research Council, Strengthening Forensic Science in the United States: A Path Forward, Washington DC: National Academies Press, 2009.

[8] C. R. Swanson, N. C. Chamelin, L. Territo and R. W. Taylor, Criminal Investigation, 9th ed., New York: McGraw-Hill, 2006.

[9] A. Jones and C. Valli, Building a Digital Forensic Laboratory, Burlington: Syngress, 2009.

[10] Association of Chief Police Officers, Good Practice Guide for Computer-Based Electronic Evidence, 2nd ed., London: Association of Chief Police Officers, 2007.

[11] R. McKemmish, “When is Digital Evidence Forensically Sound?,” in *Advances in Digital Forensics IV*, I. Ray and S. Shenoi, Eds., Boston, Springer, 2008.

[12] A. Philipp, D. Cowen and C. Davis, Hacking Exposed: Computer Forensics, 2nd ed., New York: McGraw-Hill, 2010.

[13] J. Jordaan, “A Sample of Digital Forensic Quality Assurance in the South African Criminal Justice System,” in *Information Security for South Africa*, Johannesburg, 2012.

[14] ASTM, “Standard Guide for Education and Training in Computer Forensics,” ASTM, West Conshocken, 2014.

[15] Scientific Working Group on Digital Evidence, “Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence,” SWGDE, Washington DC, 2010.

[16] European Network of Forensic Science Institutes, “Guidelines for Best Practice in the Forensic Examination of Digital Technology,” ENFSI, Poland, 2009.

[17] United Nations Office on Drugs and Crime, “Staff Skill Requirements and Equipment Recommendations for Forensic Science Laboratories,” UNODC, New York, 2011.

[18] M. Saunders, P. Lewis and A. Thornhill, Research Methods for Business Students, 5th ed., Harlow: Prentice Hall, 2009.

[19] C. Valli, “Establishing a Vendor Neutral Skills Based Framework for Digital Forensics Curriculum Development and Competence Assessment,” in *Proceedings of the 4th Australian Digital Forensics Conference*, Perth, 2006.

[20] University of Pretoria, “Computer Science Honours Degree,” 2013. [Online]. Available: http://www.cs.up.ac.za/courses/COS783. [Accessed 19 December 2013].

[21] University of Johannesburg, “Faculty of Science Postgraduate Courses,” 2013. [Online]. Available: http://www.uj.ac.za/EN/Faculties/science/Students/Documents/Fac_Science_Postgraduate%20Courses%20and%20Research%20Projects.pdf. [Accessed 2 January 2015].

[22] University of Cape Town, “Postgraduate Diploma in Management in Information Systems (CG022). INF4016W: Computer Forensics (Curriculum),” 2013. [Online]. Available: http://www.commerce.uct.ac.za/InformationSystems/Courses/inf4016w/. [Accessed 19 December 2013].

[23] A. D. Irons, P. Stephens and R. I. Ferguson, “Digital Investigation as a Distinct Discipline: A Pedogogic Perspective,” *Digital Investigation,* vol. 6, no. 1-2, pp. 82-90, 2009.

[24] R. Hankins, T. Uehara and L. Jigang, “A Comparative Study of Forensic Science and Computer Forensics,” in *Third IEEE International Conference on Secure Software Integration and Reliability Improvement*, 2009.

[25] Guidance Software, “EnCE Certification Program,” 2014. [Online]. Available: https://www.guidancesoftware.com/training/Pages/ence-certification-program.aspx?cmpid=nav. [Accessed 16 April 2015].

[26] Guidance Software, “EnCase Certified Examiner (EnCE) Program Renewal Requirements,” 2014. [Online]. Available: https://www.guidancesoftware.com/training/Pages/ence-certification-renewal.aspx. [Accessed 16 April 2015].

[27] Syntricate, “Computer Forensics - Certification,” 2015. [Online]. Available: https://www.syntricate.com/computer-forensics-certification.html. [Accessed 16 April 2015].

[28] Global Information Assurance Certification, “Certification Maintenance Guidelines & Requirements,” 2014. [Online]. Available: http://www.giac.org/certifications/renewal. [Accessed 16 April 2015].