A Sample of Digital Forensic Quality Assurance in the South African Criminal Justice System

Jason Jordaan: CFCE, CFE, PMCSSA, ACE
MTech, BComHons, BSc, BTech
Special Investigating Unit, Cyber Forensic Laboratory
East London, South Africa
Security and Networks Research Group, Department of Computer Science, Rhodes University
Grahamstown, South Africa
jjordaan@siu.org.za

***Abstract*—Criminal investigations and the resulting criminal prosecutions are dependent on quality evidence to ensure convictions. With the increasing number of digital devices in our society, a significant amount of evidence is digital, and the discipline of digital forensics, as a forensic science, should ensure the validity of this digital evidence in court. As a forensic science, quality assurance is crucial in the practice of digital forensics, to assure the court that the evidence can be trusted. The research explored the current state of digital forensic quality assurance in the criminal justice system in South Africa to determine what quality assurance practices were used, to identify any problems, as well as possible causes of any shortcomings. The research identified significant deficiencies with regard to quality assurance in digital forensics, and identified areas that potentially could impact negatively in the court environment if contested. In summary, the general state of quality assurance practice in digital forensics was poor. Reasons identified for this included a lack of training in digital forensic science fundamentals, lack of training in quality assurance in digital forensics, high case loads, and poor supervision.**

Keywords-digital forensics; forensic science; quality assurance; evidence

I. INTRODUCTION

Crime is a topic of some interest in contemporary South Africa, and there is a general sense in our society that crime is one of the biggest problems in our country. The criminal justice system seeks to address crime through various processes, including the investigation thereof, and ultimately finding and prosecuting the offender in a court of law. A key element necessary to prove a case in court is evidence, and without evidence, no conviction is possible. As our society has become more information based, and computers and digital devices have become a fundamental part of our society, so too has their role, and the information contained thereon, become part of the crime problem.

Digital evidence is now a fundamental part of many investigations. Digital evidence is defined as information of a legal probative value that is either stored, or transmitted in a digital form [1]. The proliferation of digital devices and the Internet has meant that digital evidence can be present in virtually any case, and is not limited simply to computer crimes, but is relevant to the investigation of almost any crime [2]. Over half of the cases investigated by the Federal Bureau of Investigation use some type of digital evidence [3]. In the United States of America, digital evidence has become common in courts, and cases are frequently decided on digital evidence [3].

The Electronic Communications and Transactions Act 25 of 2002 guides the issue of digital evidence in South African law, and has allowed the use of digital evidence as evidence in a South African court of law [4]. When assigning evidential weight to digital evidence, Section 15(2) of the Electronic Communications and Transactions Act 25 of 2002 guides a court in how to evaluate the evidence [4]. A key factor to be considered in this is the reliability of the digital evidence and how the integrity of it was maintained.

Digital forensics plays a critical role in establishing this, and there is a symbiotic relationship between digital evidence and digital forensics. As a forensic science, digital forensics has the power to persuade in a court of law, and as such it is crucial that the courts assess the validity of a scientific process before accepting its result [1]. The power of science in a court of law arises as a result of the supposed objectivity of its methods [5]. In other words, the fact that evidence is scientific in nature often adds weight to it in a court of law. A central assumption in this is the fact that the court of law assumes that the scientific evidence is produced through an objective scientific process.

A key factor in any court case, especially a criminal one, is the importance of quality evidence. This is especially important when considering that the standard of proof which must be satisfied to obtain a conviction in a criminal court is beyond a reasonable doubt [6], and where evidence that is not considered quality evidence may be enough to create reasonable doubt of guilt. While traditional investigative practices have developed to ensure the quality of physical evidence, this is not necessarily the case with digital evidence. With the growing importance of digital evidence in criminal prosecutions, and the use of digital forensics in obtaining that evidence, there is a need to assure the quality thereof to improve its value and use in our legal system.

II. THE IMPORTANCE OF QUALITY ASSURANCE IN DIGITAL FORENSICS

According to the National Academy of Science in the United States quality assurance procedures are necessary in the practice of forensic science to identify mistakes, scientific fraud, examiner bias, and to confirm the continued validity and reliability of forensic processes and to improve on processes that need to be improved [7]. In relation to digital forensics practice, with a particular emphasis on digital forensic laboratories, a comprehensive quality assurance system is a mandatory requirement to ensure credibility [8].

It is critical that digital forensic units or laboratories have a quality management system in place, as quality assurance is a critical requirement in the field of digital forensics [9]. This means that in practical terms at the very least that documented procedures and practices are used which are linked to appropriate standards, and which must be followed to ensure the production of a quality product [9].

Two of the most critical properties of digital evidence are its reliability and completeness, and if either of these are questionable, then the evidentiary value is greatly diminished [10]. Quality assurance can ensure that the evidence presented in court is both reliable and complete. It can be argued that digital forensic science has its own intrinsic quality metric, which is the evidence which is admitted into court and stands up to vigorous cross examination [11], however, quality assurance can increase the likelihood that the evidence and the processes applied to it can successfully stand up to this vigorous cross examination.

III. THE CONSEQUENCES OF POOR QUALITY IN FORENSIC SCIENCE

Defects in the digital 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 [12].

In the case of State of Connecticut v. Julie Amero, a primary school teacher was convicted of contributing to the delinquency of a minor because a spyware-infected school computer in her classroom displayed pornographic sites' pop-ups during her lectures [3]. The conviction resulted from incorrect assumption made with regards the evidence, and while the conviction was ultimately overturned on review, the damage had already been done to an innocent person [3].

This not only illustrates the power that forensic science evidence has to determining guilt in a court of law, but also highlights how important it is to ensure that forensic evidence is correct, as the consequences of mistakes have a very real human cost. Even if problems as a result of convictions based on flawed scientific evidence are rare, the human cost and damage to public confidence in the criminal justice system and the courts is significant [13]. There is a fundamental legal and philosophical maxim which states that it is better for ten guilty people to go free rather than let one innocent person suffer [14]. When there is poor quality in forensic science, the innocent can most certainly suffer, and this can never be acceptable. To avoid this happening, the quality of forensic science examinations, including digital forensics, must be beyond reproach.

IV. EXAMINING SOUTH AFRICAN DIGITAL FORENSIC QUALITY ASSURANCE PRACTICES

The researcher conducted an exploratory research study to identify current quality assurance practices in the field of digital forensics by digital forensic examiners that worked within the South African criminal justice system, and to identify any shortcomings in this regard which could potentially negatively impact on the digital evidence and the digital forensic processes before court.

The population represents the full set of cases from which a sample can be obtained [15]. In the context of this research, the population can be defined as all full-time digital forensic practitioners supporting criminal investigations and prosecutions. This population is a very small one. The researcher estimates that the total population of digital forensic practitioners within the criminal justice system in South Africa is currently less than 100 practitioners. This is based on the known numbers of digital forensic examiners in South African law enforcement agencies which have a digital forensics capacity, including the South African Police Service, the Directorate of Priority Crime Investigation, the Special Investigating Unit, and the South African Revenue Service, as well as the known capacities of private sector organisations to which these agencies outsourced digital forensics examinations.

Due to the qualitative and exploratory nature of the research, and the fact that statistical generalisation from the research was not an objective, judgemental sampling was considered the most appropriate sampling method to use, as this would allow the researcher's judgement to select cases that would best enable the research questions to be answered [15]. The advantage of the method is that it allows the selection of cases that are information rich, and support the qualitative focus of the research.

To ensure that an appropriate sample size is used, the research will continue to collect qualitative data until such time as data saturation is reached, which is defined at the point where collected data reveals few, if any, new insights [15].

To achieve this, potential respondents were contacted directly by the researcher and informed of the nature of the research, and to determine whether or not they would be willing to participate. Those that wished to participate were interviewed and data collated, and the process repeated until the respondent's data revealed no significant new insights. Those individuals that chose not to participate cited time constraints due to workloads for not participating.

The final sample size was ten (10) respondents, which equates to approximately ten percent of the estimated population. Each member of the sample was interviewed to collect the relevant data in this research.

A. Sample Profile

The respondents were grouped into three categories based on what type of organization they were employed by and what

their digital forensics practice focus was. There three categories were:

- Government/Law Enforcement Investigation (6 respondents)
- Private Sector: External Service Provider (2 respondents)
- Private Sector: Internal Service Provider (2 respondents)

Respondents in the Government/Law Enforcement Investigation category are employed as full-time digital forensic practitioners in government agencies that have statutory law enforcement or investigation mandates to address criminality. Respondents in the Private Sector: External Service Provider category are employed as full-time digital forensic practitioners in private sector (for profit) businesses that provide digital forensic services as part of their service offerings to their clients for the purposes of addressing criminality affecting their clients. Respondents in the Private Sector: Internal Service Provider category are employed full-time as digital forensic practitioners in private sector organizations and provides digital forensic services to their organization to address criminality occurring within their organization, or targeting their organization.

The majority of the respondents are from the Government/Law Enforcement sector, which supports the assertion of Beckett & Slay [16] that the main practitioners of digital forensics are in the field of government law enforcement agencies.

The respondents practiced as digital forensic examiners in various provinces throughout South Africa, and reflect the provinces in which their laboratories are located:

- Gauteng (5 respondents)
- Western Cape (2 respondents)
- Eastern Cape (1 respondent)
- Free State (1 respondent)
- Kwa-Zulu Natal (1 respondent)

The respondents had a wide range of experience from 1 year to 12 years. The average number of years' experience of each respondent in the field of digital forensics was 5 years and six months. The sample thus represents a fairly broad range of experience of the digital forensic practitioner respondents.

Digital forensic practitioners in the Private Sector: Internal Service Provider category had an average of 9 years and six months experience as digital forensic practitioners, while those in the Private Sector: External Service Provider category had on average 8 years' experience as digital forensic practitioners. The average experience of digital forensic practitioners in the private sector categories is significantly higher than that of digital forensic practitioners in the Government/Law Enforcement Investigation category which has an average of 3 and a third years' experience. Fifty percent of the respondents in the private sector had previously been employed as digital forensic practitioners in the Government/Law Enforcement Investigation category.

Three (3) of the respondents were employed in a management or supervisor capacity within their laboratory or workplace, and had a responsibility to supervise the work of other digital forensic practitioners. The remaining seven (7) respondents were not responsible for the supervision of other digital forensic practitioners. The sample thus represents a balance between digital forensic practitioners with supervisory responsibility over other practitioners, and those that do not.

B. The Relationship Between Digital Evidence and Digital Forensics

The respondents were questioned as to their understanding of the concept of digital evidence as defined by Casey [1], Carrier [17], and Solomon, Barrett, and Broom [18]. Evidence is the raw material used by a court of law to reach a decision on a criminal case brought before it. Digital evidence is the focus of digital forensics, and as such the concept of what digital evidence is, is a fundamental concept for digital forensic practitioners to understand. Eight (8) of the respondents demonstrated their understanding of the concept of digital evidence, while two (2) of the respondents did not demonstrate and understanding of the concept. The two respondents that had not demonstrated understanding of the concept had equated digital evidence with only "unlawful data", and "evidence from devices used to commit crimes", and did not consider exculpatory evidence. The majority of the sample understood what digital evidence was.

Understanding of the concept of digital forensics means that digital forensic examiners understand that digital forensics is a scientific or applied scientific discipline as stated by Vacca [19], Swanson, Chamelin, Territo and Taylor [2], Jones and Valli [11], McKemmish [10], and Zatyko [20]. Seven (7) of the respondents demonstrated their understanding of the concept of digital forensics, while three (3) of the respondents did not demonstrate an understanding of the concept. The three respondents that had not demonstrated understanding of the concept had equated digital forensics with only "the recovery of evidence", and "the search for evidence". It was observed that these responses came from respondents working in the Private Sector: External Service Provider category.

Digital forensics is fundamentally a process consisting of a number of defined components as identified by Casey [1] and Carrier [17]. If one of these components is missing, then the digital forensic process itself is deficient. Nine (9) of the respondents demonstrated their understanding of the various component of the digital forensic process and the process models in use, while one (1) of the respondents did not demonstrate an understanding of the concept. The respondent that had not demonstrated understanding of the concept had stated that digital forensics consists only of "the acquisition, examination, and reporting processes", and did not consider the analysis of evidence to be part of digital forensics.

All of the respondents felt that there was a relationship between digital evidence and digital forensics. Seven (7) of the respondents felt that this was due to the belief that to have admissible digital evidence, it should be obtained and produced through the application of digital forensic processes, which supports Van Der Merwe, Roos, Pistorius and Eislen [4]. Three (3) of the respondents felt that this was due to digital forensics being the process used to collect and present digital evidence. While these two different viewpoints on the relationship are

very similar, the former looks at the relationship in terms of the legal outcome of the process, while the latter looks only at the process and what it is applied to.

To further explore the relationship between digital evidence and digital forensics, the respondents were asked about what factors they felt could negatively affect the admissibility or reliability of digital evidence. Six (6) of the respondents felt that the inadequate or poor skill and knowledge of the person who initially responded to a digital crime scene, the person who acquired the evidence, or the digital forensic practitioner who examined the evidence could impact negatively of the admissibility and reliability of digital evidence. Three (3) of the respondents felt that not following accepted digital forensic practices in relation to digital evidence acquisition and examination could impact negatively of the admissibility and reliability of digital evidence. Six (6) of the respondents felt that not maintaining a chain of custody could impact negatively of the admissibility and reliability of digital evidence. Two (2) of the respondents felt that the limited knowledge of digital forensics, digital evidence, and general "cyber" aspects by legal practitioners including prosecutors, defence lawyers, advocates, magistrates and Judges could impact negatively of the admissibility and reliability of digital evidence. Only one (1) of the respondents did not identify any factors that they felt could negatively impact on the admissibility and reliability of digital evidence in court, and could potentially be explained by the fact that this respondent had the least amount of digital forensics experience of the entire sample.

The significance of these negative factors is that three of them fall within the domain of digital forensics, and as such it can be said that certain issues within digital forensics if not done correctly can negatively impact on the admissibility or reliability of digital evidence, which supports the position that there is a definite relationship between digital evidence and digital forensic.

C. The Relationship Between Digital Forensics and Forensic Science

Digital forensics is an emerging forensic science discipline and has been formally recognised as such in recent years [7], [17]. Considering that digital forensics is a forensic science discipline, it is important for digital forensic practitioners to understand exactly what forensic science is.

Two (2) of the respondents demonstrated their understanding of the concept of forensic science as defined by Swanson, Chamelin, Territo, and Taylor [2], and Hankins, Uehara, and Jigang, [21], while eight (8) of the respondents did not demonstrate an understanding of this concept. This was in contrast with the fact that all of the respondents were of the opinion that digital forensics was a forensic science.

According to Pollitt [22] and Vacca [19] forensic science, as a discipline, consists of guiding principles which are applicable to all forensic science disciplines. As a forensic science discipline, digital forensics will be guided by these principles, as would the work of all digital forensic practitioners. As such, knowledge of these principles are important to digital forensic practitioners. The respondents were asked which applicable forensic science principles they felt were applicable to digital forensics. Two of the respondents (2) stated that Locard's Principle was applicable, two (2) of the respondents stated that the principle of reproducibility was applicable, and two (2) of the respondents stated that the forensic process must not contaminate the evidence in any way. Four (4) of the respondents could not identify any applicable forensic science principles. Of the six (6) respondents that identified applicable forensic science principles, none identified more than one principle.

Forensic science, and all of its various sub-disciplines, is an applied science, and like any other scientific field, the scientific method, which forms the philosophical basis of science, is applicable in the field of forensic science, and thus digital forensics. Two (2) of the respondents demonstrated their understanding of the scientific method, while eight (8) of the respondents did not understand what the scientific method was.

D. Understanding the Importance of Quality Assurance in Digital Forensics

According to the National Research Council [7], Chen, Tsai, Chen and Yee [8], and the Association of Chief Police Officers [9], quality assurance is deemed to be a critical issue in the practice of forensic science. Digital forensics is a sub-discipline of forensic science, and thus quality assurance is critical in digital forensics practice as well.

The concepts of quality, quality control, and quality assurance, must be understood if any quality assurance practices are to be effective, and as such respondents were questioned as to their understanding of these concepts. Six (6) of the respondents demonstrated their understanding of the concept of quality, while four (4) of the respondents did not. Five (5) of the respondents demonstrated their understanding of the concept of quality control, while five (5) of the respondents did not. Four (4) of the respondents demonstrated their understanding of the concept of quality assurance, while six (6) of the respondents did not demonstrate an understanding of quality assurance.

Two (2) of the respondents were of the opinion that quality assurance was important in digital forensics as it ensured the use of consistent processes, while eight (8) of the respondents were of the opinion that quality assurance was important in digital forensics as it resulted in reliability of the processes involved as well as the end product. One (1) of the respondents did not identify any reasons why quality assurance was important in digital forensics, and could potentially be explained by the fact that this respondent had the least amount of digital forensics experience of the entire sample.

Eight (8) of the respondents were of the opinion that a consequence of poor or no quality assurance in digital forensics would be that digital evidence may be ruled as inadmissible in court. Seven (7) of the respondents were of the opinion that a consequence of poor or no quality assurance in digital forensics would be that the digital forensic practitioners would lose their reputation and credibility. Nine (9) of the respondents were of the opinion that a consequence of poor or no quality assurance in digital forensics would be that the State would lose its case in court, resulting in a potentially guilty perpetrator going free. One (1) of the respondents was of the opinion that a

consequence of poor or no quality assurance in digital forensics would be that it could lead to a wrongful conviction where an innocent person was actually found guilty and punished. Three (3) of the respondents were of the opinion that a consequence of poor or no quality assurance in digital forensics would be that digital forensic practitioners would make incorrect conclusions.

While the majority of the respondents could not adequately demonstrate an understanding of the concepts of quality, quality control and quality assurance, the majority were of the opinion that quality assurance was important and that there were identifiable potential consequences for having no or poor quality assurance in place in the digital forensic process.

Three (3) of the respondents stated that they had encountered quality assurance problems during their course of their digital forensic examinations. All three had encountered instances where image hashes had not been validated, as well as where the failure to keep backup copies of evidence had caused problems when the hard drives containing the evidence had become faulty or damaged. The remaining seven (7) respondents claimed that they had never encountered any quality assurance problems. All of the respondents stated that they had not actually experienced the actual impact of no or poor quality assurance in an actual court case, but all felt that it was simply a matter of time.

E. Quality Assurance Practices in Digital Forensics

The respondents identified a number of quality assurance practices used by themselves or their laboratories or work places. Two (2) of the respondents kept contemporaneous documentation of all the processes and actions done by themselves during the course of the forensic process. Three (3) of the respondents followed standard operating procedures. Five (5) of the respondents made use of a consistent standard examination methodology. Four (4) of the respondents made use of peer review mechanisms. One (1) respondent stated that he did not use any quality assurance practice. None of the identified practices were unique to South Africa, and were the same as some of the digital forensics quality assurance practices carried out in more mature digital forensic communities.

Standard operating procedures are considered a crucial component of digital forensic quality assurance practices. Four (4) of the respondents had standard operating procedures in the digital forensic laboratories or work places where they were employed, while six (6) of the respondents did not have any standard operating procedures in use in the digital forensic laboratories or work places where they were employed. The majority of the respondents stated that they did not have standard operating procedures. It was also noted that while four (4) respondents stated that they had documented standard operating procedures in the laboratories or work places where they were employed, only three (3) respondents stated that they actually used these documented standard operating procedures as quality assurance practices themselves.

Four (4) of the respondents stated that they had documented standard operating procedures which addresses the acquisition and imaging of digital evidence. Three (3) of the respondents stated that they had documented standard operating procedures which addressed exhibit referencing. Three (3) of the respondents stated that they had documented standard operating procedures which address the examination and analysis methodology used. Two (2) of the respondents stated that they had documented standard operating procedures which addressed the reporting format and standards to be used when documenting the findings of the digital forensic process. Two (2) of the respondents stated that they had documented standard operating procedures which governed access to the laboratory or workplace. Six (6) of the respondents had no documented standard operating procedures. Only two (2) of the respondents had documented standard operating procedures for all of the five categories identified, and another two (2) respondents had documented standard operating procedures for only two of the five categories identified.

The use of documentation is considered an essential component at all stages of handling and processing digital evidence. All of the respondents stated that they used some form of documentation during the digital forensic process. Five (5) of the respondents made use of pro-forma type documentation to document the imaging process. Two (2) of the respondents made use of pro-forma type documentation to document the processing of the evidence. Eight (8) of the respondents made notes during their work. Five (5) of the respondents made use of evidence receipt documentation for receipt and disposal of exhibits and evidence.

The testing and control of the hardware and software environment used in the acquisition, examination, and analysis of digital evidence is considered crucial as this ensures that it is working correctly. All of the respondents stated that they did not test or control their forensic software or hardware in any way.

An aspect of quality assurance, especially in digital forensics is avoiding evidence spoliation. Seven (7) of the respondents stated that they kept all of the evidence in their control under lock and key at all times when they were not processing it to avoid evidence spoliation. Four (4) of the respondents stated that they made multiple copies of their evidence and only worked on one copy to avoid evidence spoliation. Two (2) of the respondents stated that they maintained their evidence hard drives in anti-static bags when not in use to avoid evidence spoliation. Two (2) of the respondents made no effort to avoid evidence spoliation.

Quality review is a crucial component of any digital forensic quality assurance system. Four (4) of the respondents stated that their laboratories or workplaces, along with their work was subject to regular physical inspections or audits, while six (6) of the respondents did not have any physical inspections or audits of their laboratories or workplace, or their work.

Four (4) of the respondents stated that the physical inspections or audits of their laboratories and workplaces included a physical inspection of their laboratory or workplace, as well as a review of all the case documentation. The remaining six (6) respondents were not inspected or audited.

The majority of respondents did not have their digital forensic work inspected or otherwise reviewed, meaning that there was no quality oversight in the work that they had submitted. What is significant is that work inspections or reviews are often instituted by supervisors or managers as part of standard management oversight. Of the three respondents that had supervisory responsibility over other digital forensic practitioners, only one actually conducted inspections or reviews of the work done. The other two respondents stated that they did not do so simply due to time constraints, as not only did they have to supervise other practitioners, but due to staff shortages, they themselves were practitioners with their own case loads, and to review the work of other practitioners would mean that their own work would suffer.

In more mature digital forensic communities, a number of formal quality assurance systems have been applied to the field of digital forensics, such as ISO/IEC 17025 and ASCLD-LAB. Only one (1) of the respondents had any knowledge of formal quality assurance systems that were used in digital forensics practice, namely ASCLD-LAB, while the remaining nine (9) respondents were not aware of any formal quality assurance systems.

The respondent that was aware of the ASCLD-LAB system was a digital forensic laboratory manager in the Private Sector: Internal Service Provider category, and stated that he would like to implement a system like this and personally realized the value thereof, but could not justify the costs of implementing and maintaining a system like this in a commercial environment if it was not a legislated requirement.

F. Training and Certification

In an effort to determine the levels of training that the respondents had received in quality assurance issues as it applied to digital forensics, the training of the respondents in the field of digital forensics was explored.

The respondents had received a combination of training categorized as either vendor specific training, or vendor neutral training.

Vendor specific training is any training provided to teach how to use a specific piece or suite of digital forensic software, or hardware, to perform specific digital forensic tasks, using that hardware and/or software. The courses and the forensic tools that the training focused on, which had been attended by various respondents which were classified as vendor specific training included:

- Accessdata Bootcamp (FTK)
- Forensic Fundamentals (FTK)
- Windows XP Forensics (FTK)
- Internet Forensics (FTK)
- Applied Decryption (FTK)
- Silent Runner (Silent Runner)
- Windows Vista Forensics (FTK)
- Windows Registry Forensics (FTK)
- Bitpim and Cellular Data Artefacts (FTK and Bitpim)
- EnCase Computer Forensics I (EnCase)
- EnCase Computer Forensics II (EnCase)
- EnCase Advanced Internet Examinations (EnCase)
- EnCase Enterprise Examinations (EnCase)

Vender neutral training is any training provided to teach general or specialized digital forensics skills, methods, and techniques, independent of any specific software or hardware digital forensic tool. These training courses are also often referred to as “tool agnostic”. The courses which had been attended by various respondents which were classified as vendor neutral training included:

- FBI Computer Crime Investigation
- French Police Digital Evidence Seizure

None of the respondents had received any general forensic science training.

All of the respondents stated that they felt that the training that they had received from the digital forensics courses that they had attended only dealt with some quality assurance issues in the actual course contents. All of the respondents stated that the courses that they had attended emphasized the importance of cryptographic hashing and hash validation as critical processes to ensure the integrity of the digital evidence. Eight (8) of the respondents stated that the courses that they had attended emphasized the importance of maintaining a chain of custody to ensure the integrity of the digital evidence. Only one (1) of the respondents stated that the training received had stressed the importance of repeatability, so that another practitioner could examine the evidence using the same procedures and processes, and reach the same conclusion.

None of the respondents were guaranteed annual digital forensics training by the laboratories or work places where they were employed.

Three (3) of the respondents had earned their Accessdata Certified Examiner (ACE) certification, and one (1) of the respondents had also earned their EnCase Certified Examiner (EnCE) certification. Seven (7) of the respondents had no digital forensic certifications.

The two certifications certified the holders thereof as proficient in the use of a particular digital forensics software tool set, and neither addressed specific quality assurance issues. While they may not have addressed general digital forensics quality assurance the fact that they provide an independent and tested assessment of a respondent’s proficiency to use a specific digital forensics tool set does have certain implied quality assurance dynamics, namely that the respondent is at least competent in the use of a particular digital forensic tool set.

The fact that none of the respondents had received specific training in either forensic science, or that none of the digital forensic training comprehensively addresses digital forensics quality assurance, could potentially explain a reason for the general poor overall levels of quality assurance practices by digital forensics practitioners that formed the sample.

G. Workload

All of the respondents stated that they felt that their existing digital forensics case load was excessive and that this pressure and workload could lead to poor quality assurance practices taking place, through either taking short cuts or otherwise rushing work simply to get a case done, or to not actually implementing quality assurance measures in the first place.

V. CONCLUSION

The quality of evidence is crucial to ensure that criminal perpetrators are not only brought before court and prosecuted. In the case of digital evidence which is fragile by its very nature, special attention and care needs to be taken to ensure that it will be accepted in court. Digital forensics, which is an identified forensic science, has a symbiotic relationship with digital evidence, with digital evidence often being dependent on digital forensics to be used in court. With the high crime rates in South Africa, and the increasing number of digital devices containing digital evidence, it is crucial that the quality not only of the evidence, but the processes surrounding it be ensured so that the courts can trust the evidence.

The research has identified some of the potential consequences of poor quality assurance in the digital forensic process, and the potential impact these could have not only on individual cases before court, but also on the criminal justice system as a whole. In general, the research has shown that digital forensic practitioners working within the criminal justice system in South Africa have a good understanding of the consequences of poor or non-existent quality assurance practices.

The research identified some quality assurance practices in use by some digital forensic practitioners in South Africa, but there was no consistency or universality in their practice. In general, that state of quality assurance practices in digital forensics by digital forensic practitioners within the criminal justice system in South Africa is poor, which creates a risk that their work could be legitimately undermined during court proceedings, leading to acquittals, or even leading to them making incorrect conclusions which could lead to innocent persons being punished. Possible explanations for the poor state of quality assurance practice identified in the research include lack of training in quality assurance and general forensic science, excessive case loads, and inadequate supervisory and quality oversight.

Based on the findings of this research, it is recommended that additional research be carried out to identify:

- The nature of the case loads experienced and the impact this has on quality assurance
- The significant pressures within the working environment which contribute to a breakdown in quality assurance practices
- Why supervisory oversight is not adequate or effective
- The limitation of current digital forensics training in South Africa with regards to quality assurance practices

REFERENCES

[1] Casey, E. (2004). *Digital Evidence and Computer Crime* (2nd Edition ed.). London: Academic Press.

[2] Swanson, C. R., Chamelin, N. C., Territo, L., & Taylor, R. W. (2006). *Criminal Investigation* (9th Edition ed.). New York: McGraw-Hill.

[3] Peisert, S., Sishop, M., & Marzullo, K. (2008). Computer Forensics in Forensics. *Systematic Approaches to Digital Forensic Engineering* (pp. 102-122). IEEE.

[4] Van Der Merwe, D., Roos, A., Pistorius, T., & Eiselen, S. (2008). *Information and Communications Technology Law.* Durban: LexisNexis.

[5] Hanna, K. E., & Mazza, A.-M. (2006). *Discussion of the Committee on Daubert Standards.* National Research Council. Washington DC: National Academies Press.

[6] Joubert, C. (Ed.). (2001). *Applied Law for Police Officials* (2nd Edition ed.). Lansdowne: Juta.

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

[8] Chen, P. S., Tsai, L. M., Chen, Y.-C., & Yee, G. (2005). Standardizing the Construction of a Digital Forensics Laboratory. *First International Workshop on Systematic Approaches to Digital Forensic Engineering* (pp. 40-47). IEEE.

[9] Association of Chief Police Officers. (2005). *ACPO Advice and Good Practice Guide for Managers of Hi-Tech/Computer Crime Units.* National Hi-Tech Crime Unit, Association of Chief Police Officers. London: Association of Chief Police Officers.

[10] McKemmish, R. (2008). When is Digital Evidence Forensically Sound? In I. Ray, & S. Shenoi (Eds.), *Advances in Digital Forensics IV* (pp. 3-15). Boston: Springer.

[11] Jones, A., & Valli, C. (2009). *Building a Digital Forensic Laboratory*. Burlington: Syngress.

[12] Wiles, J., Alexander, T., Ashlock, S., Ballou, S., Depew, L., Dominguez, G., et al. (2007). *Techno Security's Guide to E-Discovery and Digital Forensics.* Burlington: Syngress.

[13] House of Commons Science and Technology Committee. (2005). *Forensic Science on Trial.* London: The Stationary Office Limited.

[14] Greene, E., & Heilbrun, K. (2011). *Wrightsman's Psychology and the Legal System* (7th Edition ed.). Belmont: Wadsworth.

[15] Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (5th Edition ed.). Harlow: Prentice Hall.

[16] Beckett, J., & Slay, J. (2007). Digital Forensics: Validation and Verification in a Dynamic Work Environment. *40th Annual Hawaii International Conference on System Sciences* (pp. 266-275). IEEE.

[17] Carrier, B. (2005). *File System Forensic Analysis.* Upper Saddle River: Addison-Wesley.

[18] Solomon, M. G., Barrett, D., & Broom, N. (2005). *Computer Forensics Jump Start.* Alameda: Sybex.

[19] Vacca, J. R. (2005). *Computer Forensics: Computer Crime Scene Investigation* (2nd Edition ed.). Boston: Thomson.

[20] Zatyko, K. (2007, February/March). Defining Digital Forensics. (C. Janson, Ed.) *Forensic Magazine , 4* (1), pp. 18-22.

[21] Hankins, R., Uehara, T., & Jigang, L. (2009). A Comparative Study of Forensic Science and Computer Forensics. *Third IEEE International Conference on Secure Software Integration and Reliability Improvement* (pp. 230-239). IEEE.

[22] Pollitt, M. (2008). Applying Traditional Forensic Taxonomy to Digital Forensics. In I. Ray, & S. Shenoi (Eds.), *Advances in Digital Forensics* (pp. 17-26). Boston: Springer.