AN EXAMINATION OF VALIDATION PRACTICES IN RELATION TO THE FORENSIC ACQUISITION OF DIGITAL EVIDENCE IN SOUTH AFRICA

A thesis submitted in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

Of

RHODES UNIVERSITY

by

JASON JORDAAN

January 2014

ABSTRACT

The acquisition of digital evidence is the most crucial part of the entire digital forensics process. During this process, digital evidence is acquired in a forensically sound manner to ensure the legal admissibility and reliability of that evidence in court. In the acquisition process various hardware or software tools are used to acquire the digital evidence. All of the digital forensic standards relating to the acquisition of digital evidence require that the hardware and software tools used in the acquisition process are validated as functioning correctly and reliably, as this lends credibility to the evidence in court. In fact the Electronic Communications and Transactions Act 25 of 2002 in South Africa specifically requires courts to consider issues such as reliability and the manner in which the integrity of digital evidence is ensured when assessing the evidential weight of digital evidence.

Previous research into quality assurance in the practice of digital forensics in South Africa identified that in general, tool validation was not performed, and as such a hypothesis was proposed that digital forensic practitioners in South Africa make use of hardware and/or software tools for the forensic acquisition of digital evidence, whose validity and/or reliability cannot be objectively proven. As such the reliability of any digital evidence preserved using those tools is potentially unreliable. This hypothesis was tested in the research through the use of a survey of digital forensic practitioners in South Africa.

The research established that the majority of digital forensic practitioners do not use tools in the forensic acquisition of digital evidence that can be proven to be validated and/or reliable. While just under a fifth of digital forensic practitioners can provide some proof of validation and/or reliability, the proof of validation does not meet formal international standards. In essence this means that digital evidence, which is preserved through the use of specific hardware and/or software tools for subsequent presentation and reliance upon as evidence in a court of law, is preserved by tools where the objective and scientific validity thereof has not been determined. Since South African courts must consider reliability in terms of Section 15(3) of the Electronic Communications and Transactions Act 25 of 2002 in assessing the weight of digital evidence, this is undermined through the current state of practice in South Africa by digital forensic practitioners.

ACM COMPUTING CLASSIFICATION SYSTEM CLASSIFICATION

- **Applied computing~Evidence collection, storage and analysis**
- *Applied computing~Law*
- *Applied computing~Computer forensics*

ACKNOWLEDGEMENTS

I would like to thank my family and friends for all of their support and for understanding the sacrifices that have to be made to pursue and live one's passions.

I would like to thank Dr. Karen Bradshaw my supervisor and Prof. Barry Irwin from Rhodes University for their support.

Finally I would like to thank all of those digital forensic practitioners who responded to my research survey.

TABLE OF CONTENTS

ABSTRACT i

ACM COMPUTING CLASSIFICATION SYSTEM CLASSIFICATION ii

ACKNOWLEDGEMENTS iii

TABLE OF CONTENTS iv

LIST OF TABLES AND FIGURES vii

1. INTRODUCTION 1

1.1. MOTIVATION FOR THE RESEARCH 1

1.2. HYPOTHESIS 2

1.3. RESEARCH METHODOLOGY 2

1.3.1. Research Objectives 3

1.3.2. Research Questions 3

1.3.3. Limitations of the Research 4

1.4. THESIS STRUCTURE 4

1.5. SUMMARY 5

2. LITERATURE REVIEW 6

2.1. DIGITAL EVIDENCE 6

2.1.1. Digital Evidence in Relation to South African Law 7

2.1.2. Admissibility and Relevance of Digital Evidence 8

2.1.3. Relationship between Digital Evidence and Digital Forensics 9

2.2. DIGITAL FORENSICS 11

2.2.1. Defining Digital Forensics 11

2.2.2. Digital Forensics as a Forensic Science Discipline 12

2.2.3. Importance of Quality Assurance Practices in Digital Forensics 13

2.2.4. General Problems in Relation to Quality Assurance Practices in Digital Forensics 15

2.3. THE DIGITAL FORENSICS PROCESS 17

2.3.1. Digital Forensics Research Workshop (DFRWS) Model 17

2.3.2. The National Institute of Justice (NIJ) Model 17

2.3.3. The Abstract Digital Forensics Model 18

2.3.4. Hierarchical Objectives Based Framework Forensics Model 18

2.3.5. Digital Forensic Investigation Framework 19

2.3.6. Casey Model 19

2.3.7. Harmonised Digital Forensic Investigation Process Model 20
2.4. THE FORENSIC ACQUISITION PROCESS 23
2.4.1. Write Blocking 24
2.4.2. Forensic Imaging 24
2.4.3. Quality Assurance Practices in Digital Forensics Relating to the Forensic Acquisition Process 26
2.4.4. Importance of Validation in the Forensic Acquisition Process 28
2.5. VALIDATION STANDARDS AND PRACTICES RELATING TO THE FORENSIC ACQUISITION PROCESS 29
2.5.1. National Institute of Standards and Technology Computer Forensics Tool Testing Project 31
2.5.2. The Scientific Working Group on Digital Evidence 43
2.5.3. European Network of Forensic Science Institutes 43
2.5.4. Dual Tool Validation 43
2.5.5. Vendor Validation 44
2.6. SUMMARY 44
3. RESEARCH DESIGN 46
3.1. RESEARCH PHILOSOPHY 46
3.2. RESEARCH PURPOSE 47
3.3. RESEARCH APPROACH 47
3.4. RESEARCH STRATEGY 47
3.5. RESEARCH TIME FRAME 48
3.6. RESEARCH METHOD 48
3.7. SAMPLING 48
3.8. DATA COLLECTION 49
3.9. DATA ANALYSIS 49
3.10. ETHICAL ISSUES 50
3.11. SUMMARY 50
4. SURVEY DESIGN AND IMPLEMENTATION 51
4.1. RESEARCH QUESTIONNAIRE 51
4.2. IDENTIFICATION OF PROSPECTIVE RESPONDENTS 51
4.3. DATA COLLECTION AND COLLATION 52
4.4. SUMMARY 52
5. SURVEY ANALYSIS AND DISCUSSION OF FINDINGS 53
5.1. AGE, GENDER, AND LOCATION 53

5.2. EDUCATION 55
5.2.1. Secondary School Education 55
5.2.2. Undergraduate Tertiary Education 58
5.2.3. Postgraduate Education 62
5.3. DIGITAL FORENSIC EXPERIENCE 66
5.4. DIGITAL FORENSICS TRAINING 71
5.5. VALIDATION TRAINING 74
5.6. KNOWLEDGE OF VALIDATION STANDARDS 76
5.7. HARDWARE AND SOFTWARE USED IN THE FORENSIC ACQUISITION PROCESS 77
5.8. THE USE AND VALIDATION OF WRITE BLOCKERS 78
5.8.1. Using Write Blockers That Had Not Been Validated 79
5.8.2. Ensuring That Write Blockers Used Are Validated 80
5.8.3. Validating Write Blockers 84
5.9. THE USE AND VALIDATION OF FORENSIC IMAGING TOOLS 86
5.9.1. Using Forensic Imaging Tools That Had Not Been Validated 88
5.9.2. Ensuring That Forensic Imaging Tools Used Are Validated 89
5.9.3. Validating Forensic Imaging Tools 92
5.10. SUMMARY 95
6. CONCLUSION 96
6.1. THE USE OF VALIDATED FORENSIC ACQUISITION TOOLS 96
6.2. RESEARCH CONTRIBUTION 99
6.3. FURTHER RESEARCH 100
7. REFERENCES 101
8. APPENDIX 107

LIST OF TABLES AND FIGURES

LIST OF FIGURES

Figure 1 - DFRWS Digital Forensics Process 17
Figure 2 - NIJ Digital Forensics Process 18
Figure 3 - Abstract Digital Forensics Process 18
Figure 4 - Hierarchical Objectives Based Framework Digital Forensics Process 19
Figure 5 - Digital Forensic Investigation Framework Forensics Process 19
Figure 6 - The Casey Digital Forensics Process 20
Figure 7 - Harmonised Digital Forensic Investigation Process 21
Figure 8 - Simple Digital Forensics Process 22
Figure 9 - Age Distribution 53
Figure 10 - Gender Distribution 54
Figure 11 - Ethnic Distribution ..... **Error! Bookmark not defined.**
Figure 12 - Gender Distribution by Ethnic Group ..... **Error! Bookmark not defined.**
Figure 13 - HDI vs. Non-HDI by Age Group ..... **Error! Bookmark not defined.**
Figure 14 - HDI vs. Non-HDI Trends by Age Group ..... **Error! Bookmark not defined.**
Figure 15 - Geographic Distribution of Respondents 55
Figure 16 - Matriculation 56
Figure 17 - Grade 12 Mathematics 57
Figure 18 - Grade 12 Physical Science 57
Figure 19 - Grade 12 Information Technology 58
Figure 20 - Undergraduate Qualifications 59
Figure 21 - Undergraduate Qualifications by Category 60
Figure 22 - Undergraduate Qualification Breakdown by Recommended Field 61
Figure 23 - Postgraduate Qualifications 62
Figure 24- Postgraduate Qualifications by Category 63
Figure 25 - Postgraduate Qualification Breakdown by Recommended Field 64
Figure 26 - UCT and UP Digital Forensics Graduates Undergraduate Profile 65
Figure 27 - Digital Forensics Experience 66
Figure 28 - Digital Forensics Experience per Sector 67
Figure 29 - Testified as Digital Forensic Practitioners in Court 67
Figure 30 - Respondent Testifying Experience per Court 68
Figure 31 - Cross Examination about Validity 68
Figure 32 - Validity of Tools Challenged in Court 70
Figure 33 - Formal Digital Forensics Training 71
Figure 34 - Types of Training 72
Figure 35 - Training on Importance of Validation 74
Figure 36- Training on How to Conduct Validation Testing 75
Figure 37 - Knowledge of Validation Standards 76
Figure 38 - Write Blocking Tools Used 77
Figure 39 - Forensic Imaging Tools Used 78
Figure 40 - Only Use Validated Write Blockers 78

Figure 41 - Ensuring Write Blocker Validity 79
Figure 42 - Reasons for Not Using Validated Write Blockers 80
Figure 43 - How Validation Was Done (Write Blockers) 81
Figure 44 - When Write Blockers are Validated 84
Figure 45 - Formal Standards Used for Validating Write Blockers 85
Figure 46 - Validation Test Documentation Retention (Write Blockers) 86
Figure 47 - Only Use Validated Forensic Imaging Hardware or Software 87
Figure 48 - Ensuring Forensic Imager Validation 87
Figure 49 - Reasons for Not Using Validated Forensic Imaging Hardware or Software 88
Figure 50 - How Validation Was Done (Forensic Imagers) 89
Figure 51 - When Forensic Imagers are Validated 92
Figure 52 - Formal Standards Used for Validating Forensic Imagers 93
Figure 53 - Validation Test Documentation Retention (Forensic Imagers) 94
Figure 54 - Proof of Validation 98

LIST OF TABLES

Table 1 - NIST CFTT Hardware Write Blocker Requirements 31
Table 2 - NIST CFTT Hardware Write Blocker Test Assertions 32
Table 3 - NIST CFTT Hardware Write Blocker Test Cases 32
Table 4 - NIST CFTT Software Write Blocker Requirements 34
Table 5 - NIST CFTT Software Write Blocker Test Assertions 34
Table 6 - NIST CFTT Software Write Blocker Test Cases 35
Table 7 - NIST CFTT Forensic Imaging Tool Requirements 40
Table 8 - NIST CFTT Forensic Imaging Tool Test Assertions 40
Table 9 - NIST CFTT Forensic Imaging Tool Test Cases 41
Table 10 - Undergraduate Qualifications 60
Table 11 - Postgraduate Qualifications 63
Table 12 - Vendor Courses Attended 73
Table 13 - Non-Vendor Courses Attended 74
Table 14- Independent Validation Testing (Write Blockers) 82
Table 15- Vendor Validation Testing (Write Blockers) 83
Table 16 - Independent Validation Testing (Forensic Imagers) 90
Table 17- Vendor Validation Testing (Forensic Imagers) 91

1. INTRODUCTION

Digital evidence is a fundamental and integral part of almost all investigations conducted presently; these investigations are not limited to suspected criminal offences, but also include civil investigations and regulatory investigations. In terms of the Electronic Communications and Transactions Act 25 of 2002 (Republic of South Africa, 2002), a key consideration of the courts when looking at digital evidence is reliability of the digital evidence and how the integrity thereof was maintained. Digital forensics is a key discipline used to address this.

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 (Kessler, 2012).

1.1. MOTIVATION FOR THE RESEARCH

A digital forensic practitioner has a responsibility to accurately report on their actions taken to identify, extract, and analyse the data that will be presented as evidence in court. Many digital forensic practitioners rely on hardware and software tools to produce results, often without knowledge of how those results are produced, which risks not only their professional reputations, but also the potential successful outcome of the investigation they have worked on (Marcella & Guillossou, 2012).

One of the crucial elements of the entire digital forensics process is that digital forensic practitioners should have detailed knowledge of the capabilities, limitations, and restrictions of the tools they use (Casey & Rose, 2010). One of the significant challenges faced by digital forensic practitioners is how to assure the reliability of the forensic tools they use, especially as a result of the reliance that is often placed on these tools by digital forensic practitioners (Guo, Slay, & Beckett, 2009).

Very little research has been done on the validation and verification of digital forensic tools and digital evidence (Guo, Slay, & Beckett, 2009).

The acquisition of digital evidence in a forensically sound and valid manner is one of the most critical phases in the digital forensics process; if there are shortcomings in this process, there is a critical risk of the evidence itself being declared inadmissible in court.

The evidence acquisition process requires that the source media containing the digital evidence must be duplicated bit by bit, ensuring that all the data is duplicated, and that the duplication process itself does not alter the data in any way. Various hardware and software tools are used during this process, and it is crucial that all tools and instruments used in any forensic science process actually perform their functions correctly and accurately. Forensic science, therefore, relies on validation, verification, and calibration testing processes to ensure that the tools used are functioning within acceptable standards.

Previous research into quality assurance practices in digital forensics in South Africa (Jordaan, 2012) identified tool validation as a general area of concern. In terms of the forensic acquisition of digital evidence, if the tools used to preserve the evidence were not proven to be valid, then the admissibility and weight of the digital evidence could be significantly affected.

Considering the use of digital evidence in court, it is thus important to identify the current state of practice in this regard to identify any shortcomings or risks in the use of digital evidence as a legitimate form of evidence in South African courts of law.

1.2. HYPOTHESIS

The core hypothesis of the research, based on the observations of the researcher, is that digital forensic practitioners in South Africa make use of hardware and/or software tools for the forensic acquisition of digital evidence, whose validity and/or reliability cannot be objectively proven. As such the reliability of any digital evidence preserved using those tools is potentially unreliable.

1.3. RESEARCH METHODOLOGY

The research makes use of a structured questionnaire to collect both quantitative and qualitative data from South African digital forensic practitioners for analysis, as detailed in the Research Design chapter.

1.3.1. Research Objectives

The literature review guided the formalisation of the research objectives. Research objectives demonstrate a clear sense of purpose and direction, and lead to greater specificity (Saunders, Lewis, & Thornhill, 2009). The research objectives for this research were:

- To determine the current state of practice with regards the validation testing of hardware and/or software tools used in the forensic acquisition process amongst South African digital forensic practitioners.
- To identify shortcomings and deficiencies (if any) in the use of hardware and/or software tools used during the forensic acquisition process, relating to the reliability of the tools used, and the impact this could have on the reliability of digital evidence in court proceedings.
- To identify possible reasons for any shortcomings and deficiencies (if any) in use of hardware and/or software tools used during the forensic acquisition process, relating to the reliability of the tools used.

1.3.2. Research Questions

The clearly defined research objectives, which are critical in the research process (Saunders, Lewis, & Thornhill, 2009), allowed specific and clearly defined research questions to be set out. The following research questions were addressed in this research:

- How do digital forensic practitioners satisfy themselves that the hardware and/or software tools used in the forensic acquisition of digital evidence are reliable?
- To what extent are the hardware and/or software tools used in the forensic acquisition of digital evidence validated as being reliable?
- What are the accepted standards for ensuring that the hardware and/or software tools used in the forensic acquisition of digital evidence are reliable?
- Do South African digital forensic practitioners comply with these standards?

- What training have South African digital forensic practitioners undertaken that has identified the importance of validation and how to conduct validation testing?
- To what extent has potentially unreliable digital evidence been used in court proceedings as a result of potentially unreliable hardware and/or software tools used in the forensic acquisition process?

By answering these questions, the research has identified shortcomings in current practice.

1.3.3. Limitations of the Research

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 respects:

- The curricula of the various training courses and academic programs were not examined in detail to determine either the quality of any material covered relating to the importance of validation testing of tools used in the forensic acquisition process, or the quality of any material addressing how to conduct validation testing of forensic acquisition tools.
- In examining the sample participants' knowledge of formal validation testing standards, their actual knowledge was not specifically tested.
- 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.

1.4. THESIS STRUCTURE

The thesis is organised into six chapters. The first chapter is an introduction to the research topic. The second chapter details the literature review conducted as part of the research. The third and fourth chapters detail the research design and how the research was implemented. The fifth chapter presents the research findings and the sixth chapter the conclusions from the research.

1.5. SUMMARY

Digital evidence is now a crucial element in proving many criminal cases, as well as used in civil trials. Judges and magistrates make their decisions based on the reliable and admissible evidence that is placed before them. The core hypothesis of the research is that digital forensic practitioners in South Africa make use of hardware and/or software tools for the forensic acquisition of digital evidence, whose validity and/or reliability cannot be objectively proven. As such the reliability of any digital evidence preserved using those tools is potentially unreliable. In other words Judges and magistrates are potentially making decisions based on evidence that itself may be fundamentally unreliable.

The research will address a number of issues. It will determine the current state of practice with regards the validation testing of hardware and/or software tools used in the forensic acquisition process amongst South African digital forensic practitioners. It will identify shortcomings and deficiencies (if any) in the use of hardware and/or software tools used during the forensic acquisition process, relating to the reliability of the tools used, and the impact this could have on the reliability of digital evidence in court proceedings. Finally it will identify possible reasons for any shortcomings and deficiencies (if any) in use of hardware and/or software tools used during the forensic acquisition process, relating to the reliability of the tools used.

2. LITERATURE REVIEW

The purpose of the research was to examine the current validation practices in relation to the forensic acquisition phase of the digital forensics process in South Africa, and to determine the possible reasons for these practices. The research also aimed to determine any problem areas that could negatively impact the practice of digital forensics in South Africa, and undermine the value that courts may place on digital evidence in legal proceedings.

This literature review explores a number of topics related to the research. It explores the concept of digital evidence, including its definition, characteristics, and legalities, in so far as it relates to court proceedings. The concept of digital forensics, which is intrinsically linked to digital evidence, is then examined in depth, including the importance of quality assurance in digital forensics and some of the general quality assurance problems typically encountered. The forensic acquisition process is then considered in detail as part of the overall digital forensics process, focusing on write blocking and forensic imaging, the importance of validation practices in these, and the general quality assurance practices that apply in the forensic acquisition process. The literature review finally examines existing validation standards and practices applicable to the forensic acquisition process.

2.1. DIGITAL EVIDENCE

Evidence is the material used by a court of law to reach a legal decision on any case brought before it for adjudication. The entire digital forensics process is interlinked with digital evidence, and as such it is important to examine the nature of digital evidence and the legal issues relating thereto.

Evidence can be defined as anything that proves or disproves a fact at issue in a judicial case (Swanson, Chamelin, Territo, & Taylor, 2006). Digital evidence is considered information stored or transmitted in digital form that has probative legal value (Casey, 2011). In other words, it is stored or transmitted reliable digital objects supporting or refuting a specific hypothesis (Carrier, 2005).

Digital evidence can be used to answer typical investigative questions, proving either who, what, when, where, why, or how, of a matter under investigation (Solomon, Barrett, & Broom, 2005).

It can also answer some very specific questions such as what happened when, who interacted with whom, from where a particular digital object originated, and who was responsible for it (Casey & Rose, 2010).

Digital evidence should be treated no differently than traditional physical evidence and while the methods used to collect and interpret it may appear complicated and expensive, when they are used correctly they produce evidence that is both compelling and cost-effective (Association of Chief Police Officers, 2007). Like any other type of physical evidence, the improper handling or forensic processing of digital evidence, can destroy its court value (Swanson, Chamelin, Territo, & Taylor, 2006).

Digital evidence is a very fragile form of evidence and can easily be altered, damaged, or destroyed by its improper handling or examination (Association of Chief Police Officers, 2007). The nature of digital evidence means that there are a number of inherent challenges to its use in court, the most significant of which is the ease with which it can be manipulated or altered, either intentionally or accidentally, without leaving any obvious signs that the data has been altered (Casey , 2011).

2.1.1. Digital Evidence in Relation to South African Law

The Electronic Communications and Transactions Act 25 of 2002 deals with digital evidence in South African law, and addresses how the courts should deal with digital evidence. Section 15(2) of this Act guides a court in how it should evaluate digital evidence, and one of the key issues that a court must consider is the reliability of the digital evidence itself, and how the integrity of that evidence was maintained (Van Der Merwe, Roos, Pistorius, & Eiselen, 2008).

The Electronic Communications and Transactions Act 25 of 2002 does not define digital evidence per se, but it does define a data message in Section 1: data is an electronic representation of information in any form, and a data message is any data that is generated, sent, received, or stored in electronic means (Republic of South Africa, 2002). In essence a data message is synonymous with digital evidence, and satisfies the definitions of digital evidence given by Casey (2011) and Carrier (2005).

Section 15 of the Electronic Communications and Transactions Act 25 of 2002 deals with the admissibility and weight of data messages. Section 15(1) of the Act states that a data message (and thus digital evidence) cannot be ruled inadmissible simply by virtue of the evidence being in an intangible digital format, while Section 15(2) goes on to

state that information in a digital form must be given due evidential weight (Republic of South Africa, 2002).

Section 15(3) lays down the issues that a court must consider in assessing the evidential weight of the digital evidence, and requires a court to do so (Republic of South Africa, 2002):

- Consider the reliability of the manner in which the data message (digital evidence) was generated, stored, or communicated.
- Consider reliability of the manner in which the integrity of the data message (digital evidence) was maintained.
- Consider the manner in which the originator of the data message (digital evidence) was established.
- Consider any other relevant factors.

A key issue in demonstrating the reliability of the digital evidence is establishing a proper chain of evidence and establishing the reliability of the digital evidence using cryptographic means such as mathematical hashes (Van Der Merwe, Roos, Pistorius, & Eiselen, 2008).

2.1.2. Admissibility and Relevance of Digital Evidence

For evidence to be useable in any court of law, it must be both relevant and admissible. If it does not satisfy both criteria, it cannot be considered by a court as it may unfairly prejudice one side or the other in the case. Even if it involves digital evidence, the traditional requirements of the law of evidence still apply. Relevant evidence is evidence that can prove or disprove any of the facts in the case. If evidence is not considered relevant it will not be considered in the case. Admissible evidence is evidence that meets all regulatory and statutory requirements, and has been correctly obtained and handled (Solomon, Barrett, & Broom, 2005).

A key aspect of establishing the admissibility and persuasive value of digital evidence in legal proceedings, whether they are criminal or civil, is to show to the court that the evidence obtained from the original media is a true and accurate representation of the original data (National Institute of Justice, 2007).

Evidence is either admissible or inadmissible for the purposes of court (Schwikkard & Van Der Merwe, 2002). The two instances that generally cause evidence not be

admissible in court are to collect it in an illegal manner, or to modify the evidence after it has come into the possession of the investigator/examiner (Solomon, Barrett, & Broom, 2005). A typical mistake that leads to digital evidence being ruled inadmissible in court is that it was obtained without the correct legal authorisation (Casey, 2011). Other common mistakes that are made by digital forensic examiners, which can render digital evidence inadmissible, include (Jones & Valli, 2009):

- Failure to create and maintain the proper documentation through all stages of the digital forensic process.
- The inadvertent modification of digital evidence.
- Failure to maintain the chain of custody.
- Failure by a digital forensic examiner to know when s/he has reached the limits of his/her knowledge and ask for advice.

In the United States, use is made of the Daubert criteria when evaluating the admissibility of expert scientific testimony, which would include digital evidence, obtained and presented by a digital forensics practitioner (National Research Council, 2002). These criteria include:

- Whether the theories or techniques used are based on a hypothesis that is testable.
- Whether the theories or techniques used have been subjected to a peer review.
- Whether there is a known or potential error rate of the techniques.
- Whether the methods and techniques are generally accepted in the relevant scientific community.

2.1.3. Relationship between Digital Evidence and Digital Forensics

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 (Van Der Merwe, Roos, Pistorius, & Eiselen, 2008). In assessing the weight of digital evidence in South African courts, digital forensics plays an increasingly important role (Meintjes-Van der Walt, 2012). A significant component of ensuring the admissibility of digital evidence is to show the court that the digital evidence produced in court is exactly the same as that which was initially seized (Association of Chief Police Officers, 2007).

Four basic principles developed in the United Kingdom for computer-based digital evidence (Association of Chief Police Officers, 2007) are commonly used throughout the world. These are:

- No action taken by an investigator or examiner should change data held on a computer or storage media that may subsequently be relied upon in court.
- In circumstances where an investigator or examiner must access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and implications of their actions.
- An audit trail or other record of all processes applied to computer-based digital evidence must be created and preserved, and it must be detailed enough to allow an independent third party to use the processes as documented, and achieve the same results by following those processes.
- The person in charge of an investigation has the overall responsibility for ensuring that these principles are adhered to.

The International Organisation on Digital Evidence also set a number of principles to ensure the integrity of digital evidence, including the following (McKemmish, 2008).

- When dealing with digital evidence, all of the general procedural principles in the field of forensic science should be applied.
- Once digital evidence has been acquired, no actions taken should change that evidence.
- When it is necessary to interact directly with original digital evidence, the person doing so should be specifically trained to do so.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, and this documentation must be preserved and available for review.
- A person in possession of digital evidence is responsible for all actions taken with respect to it when in their possession.
- Any agency responsible for seizing, accessing, storing, or transferring digital evidence, is responsible for complying with these principles.

Physical evidence is collected using very rigorous and established procedures in order to protect it from contamination or destruction, or from claims that it was tampered with

or handled improperly, and to establish and preserve the chain of custody. Digital evidence, just like physical evidence, must be subject to the same rigorous requirements, and by following established forensic science practices, this fragile and easily altered form of evidence can be shown to be authentic. Failure to follow these procedures could result in the digital evidence being excluded from a court of law, or at the very least being given limited evidential value (Jones & Valli, 2009). In many respects, digital evidence is simply another form of latent physical evidence, which must be handed with established forensic science principles (Casey, 2011).

Digital forensic tools play a critical role in preserving and extracting digital evidence during the digital forensics process, and if the tools themselves function incorrectly, or not as intended, then there is a real risk that the resultant digital evidence may be inadmissible in court proceedings. The trustworthiness of digital evidence is thus often interlinked and reliant on the correct functioning of the forensic tools used. To guarantee that digital evidence is sound, digital forensic practitioners must validate and verify their tools (Guo, Slay, & Beckett, 2009).

2.2. DIGITAL FORENSICS

Forensic science is crucial to the successful investigation of crime in the modern age, and is critical to the efficiency and effectiveness of the general criminal justice system (House of Commons Science and Technology Committee, 2005).

Digital forensics is an emerging forensic science (Britz, 2009) that is playing an increasingly significant role in modern criminal and civil court actions.

2.2.1. Defining Digital Forensics

Digital forensics is at its most elementary the preservation, identification, extraction, and documentation of digital evidence stored as data or magnetically encoded information. In essence, digital forensics is about evidence from computers, digital media, or digital devices that can stand up to scrutiny in court. The objective of digital forensics is quite simple: to recover, analyse, and present digital evidence in such a way that it is usable as evidence in a court of law (Vacca, 2005).

One definition of digital forensics is that it is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media (Swanson, Chamelin, Territo, & Taylor, 2006). Digital forensics has also

been defined as computer investigation and analysis techniques that involve the identification, preservation, extraction, documentation, and interpretation of computer data to determine potential legal evidence (Solomon, Barrett, & Broom, 2005). Another definition is that digital forensics is the application of science and engineering to the legal problems associated with digital evidence (Jones & Valli, 2009). In another definition, digital forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events, or helping to anticipate unauthorised actions (McKemmish, 2008).

Ken Zatyko, a former director of the Defence Computer Forensics Laboratory, which is one of the biggest digital forensics laboratories in the United States, defines digital forensic science as "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting, and possible expert presentation" (Zatyko, 2007).

For the purposes of this dissertation, digital forensics is regarded as the forensically and scientifically valid preservation, examination and analysis of digital evidence, and the interpretation thereof to answer specific legal questions in a court of law.

2.2.2. Digital Forensics as a Forensic Science Discipline

Digital forensics did not start as a forensic science in a forensic laboratory; instead it developed as a result of law enforcement investigators who realised that computers may be sources of evidence in the early days of computing (National Research Council, 2009). Digital forensics began as a specific discipline in the mid-1980s as federal law enforcement agencies in the United States saw the increasing involvement of computers in crimes (Jones & Valli, 2009). In the early 1990s, the International Association of Computer Investigative Specialists, which comprised law enforcement digital forensic investigators, created the first documented set of guidelines for digital forensics (Pollitt, 2008).

Digital forensics initially developed in an ad-hoc manner, rather than a scientific one, but this has changed, and many of the current developments in digital forensics are

scientific in nature (Beckett & Slay, 2007). In the decade leading up to the publication of research by the National Research Council in 2009, what had up until then been an investigative methodology practiced by investigators with an interest and aptitude for computers, developed into a separate forensic science discipline subject to the rigors and expectations of the greater field of forensic science (National Research Council, 2009). In 2003 digital forensics became part of mainstream forensic science when the American Society of Crime Laboratory Directors Laboratory Accreditation Board recognised digital forensics as a fully-fledged forensic science discipline, and a discipline in which a forensic science laboratory could be accredited (Carrier, 2005). In 2009, the American Academy of Forensic Science adopted digital forensics as a science (Kessler, 2012).

Initial conceptual approaches to digital forensics were fragmented, which perpetuated the viewpoint that there was no standard approach to digital forensic practice. However, the development of common conceptual approaches was necessary for digital forensics to be considered a valid forensic science discipline (Rogers & Siegfried, 2004). Recent research supports the view of digital forensics as a forensic science, owing to the fundamental aspect of forensic science, which is the application of a scientific discipline to aspects of the law, and this is precisely what is done in digital forensic practice (Irons, Stephens, & Ferguson, 2009).

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 (Irons, Stephens, & Ferguson, 2009). 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 (Hankins, Uehara, & Jigang, 2009).

2.2.3. Importance of Quality Assurance Practices in Digital Forensics

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 (Volonino, Anzaldua, & Godwin, 2007), 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 (Fereday & Kopp, 2003) 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 (House of Commons Science and Technology Committee, 2005).

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 quality of forensic science examinations, including digital forensics, must be beyond reproach.

In digital forensics, as in any forensic science, quality can be defined as a final product free of deficiencies, which means that the evidence can be tested and validated, and the results must be measurable and repeatable. Assurance is the process of validating, testing, or verifying that a specific process functions as intended, or as specified, and this is usually done through testing (Jones & Valli, 2009).

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 (Jones & Valli, 2009). 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.

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, and examiner bias, to confirm the continued validity and reliability of

forensic processes and to improve on processes that need to be improved (National Research Council, 2009).

Two critical properties of digital evidence are the reliability and completeness of the evidence, and if either of these is questionable, the evidentiary value is compromised. Quality assurance can ensure that the evidence presented in court is both reliable and complete. To achieve this, a number of criteria should be established in relation to the digital evidence, namely, that (McKemmish, 2008):

- the meaning and interpretation of the digital evidence has been unaffected by the digital forensic process used,
- all potential errors have been reasonably identified and satisfactorily explained to remove any doubt over the reliability of the evidence,
- the digital forensic process can be independently examined and verified in totality,
- the digital forensic analysis of the evidence has been undertaken by a person with sufficient and relevant experience.

If a digital forensic process is found to be questionable in court, in other words, not forensically sound, this will likely influence the admissibility of the weight of the digital evidence (Casey, 2011). Quality assurance can contribute to establishing the forensic soundness of a process.

2.2.4. General Problems in Relation to Quality Assurance Practices in Digital Forensics

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. The research identified significant problems with quality assurance practices, which were necessary to ensure the accuracy of forensic analysis. As a result of poor or non-existent quality assurance practices, persons had been convicted of crimes that had not been committed (National Research Council, 2009).

Research conducted on forensic science laboratories in California found that several laboratories had no comprehensive quality assurance systems in place. In fact, with respect to digital forensics, of the 32 forensic laboratories in the state of California, only one met the quality assurance standards for digital forensics as prescribed by the American Society of Crime Laboratory Directors Laboratory Accreditation Board (California Crime Laboratory Review Task Force, 2009).

The problems identified most often are attributed to quality assurance practices and issues that impact quality in general, such as time pressures and examiner competency. An additional problem is the current ability of law enforcement, who still comprise the main group of practitioners in the field of digital forensics, to apply scientific principles to digital forensics (Beckett & Slay, 2007).

The increase in requests for digital forensics support in investigations has had a significant impact on the workloads of digital forensic practitioners, who experience significant backlogs. Accuracy is critical in digital forensics, as it is in any branch of forensic science, and as such shortcuts cannot be taken in an effort to save time (Vacca, 2005).

However, significant pressure can be brought to bear on forensic practitioners to get the job done quickly. It is critical that the quality of digital forensic examinations be kept at a high level despite the work pressures, under which many digital forensic practitioners operate. This work pressure has resulted in examiners producing quick results, sometimes at the expense of reliability, accuracy, and even impartiality (Association of Chief Police Officers, 2011).

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 (Swanson, Chamelin, Territo, & Taylor, 2006). 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.

Research conducted in South Africa focusing on quality assurance practices in digital forensics confirmed that these issues are also relevant in South Africa (Jordaan, 2012).

2.3. THE DIGITAL FORENSICS PROCESS

Digital forensics is fundamentally a methodology with a number of distinct stages or phases, which encompass various tasks that are performed by a digital forensics practitioner when dealing with potential digital evidence. The basic digital forensic methodology includes acquiring the data without altering or damaging the source of the data, authenticating that the data acquired is the same as that from the seized source, and analysing the data acquired without altering it (Sansurooah, 2006).

A number of process models have developed, which define the various stages and phases comprising a high-level digital forensics methodology.

2.3.1. Digital Forensics Research Workshop (DFRWS) Model

The first Digital Forensic Research Workshop (DFRWS) held in Utica, New York in August 2001 identified the need for a standard framework for digital forensics, and proposed the following iterative process model consisting of a number of distinct phases: identification, preservation, collection, examination, analysis, presentation, and decision (Palmer, 2001):

Figure 1 - DFRWS Digital Forensics Process

2.3.2. The National Institute of Justice (NIJ) Model

The National Institute of Justice of the United States Department of Justice documented a digital forensics process model consisting of preparation, recognition and

identification, scene documentation, collection and preservation, packaging and transportation, examination, analysis, and reporting (National Institute of Justice, 2001).

Figure 2 - NIJ Digital Forensics Process

2.3.3. The Abstract Digital Forensics Model

The abstract digital forensics model, consisting of identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence phases, built on the NU and DFRWS digital forensics process models (Reith, Carr, & Gunsch, 2002).

Figure 3 - Abstract Digital Forensics Process

2.3.4. Hierarchical Objectives Based Framework Forensics Model

Researchers from the University of Texas in San Antonio proposed a model, which consisted of a preparation phase, a data collection phase, a data analysis phase, a presentation of findings phase, and an incident closure phase (Beebe & Clark, 2005).

Figure 4 - Hierarchical Objectives Based Framework Digital Forensics Process

2.3.5. Digital Forensic Investigation Framework

Researchers in Malaysia consolidated a number of existing digital forensics models into a digital forensic investigation framework, consisting of processes for preparation, collection and preservation, examination and analysis, presentation and reporting, and disseminating the case (Selamat, Yusof, & Sahib, 2008).

Figure 5 - Digital Forensic Investigation Framework Forensics Process

2.3.6. Casey Model

Eoghan Casey, a prominent digital forensic academic and practitioner, proposed a model of the digital forensic process, which includes authorisation and preparation, identification, collection and preservation, examination and analysis, reconstruction, and reporting results (Casey , 2011).

Figure 6 - The Casey Digital Forensics Process

2.3.7. Harmonised Digital Forensic Investigation Process Model

Extensive research has been carried out recently at the University of Pretoria (UP) on a harmonised digital forensic investigation process model, which is an iterative and multi-tiered model that introduces parallel actions to many of the traditional digital forensics processes (Valjarevic & Venter, 2012).

The primary processes include incident detection, first response, planning, preparation, incident scene documentation and potential evidence identification, potential evidence collection, potential evidence transportation, potential evidence analysis, presentation and conclusion (Valjarevic & Venter, 2012).

A number of parallel actions then take place alongside these processes and include obtaining authorisation, documentation, information flow, preserving chain of custody, preserving evidence, and interaction with physical investigation (Valjarevic & Venter, 2012).

This model forms the basis for the ISO 27043 Draft International Standard Information Technology-Security Techniques-Incident Investigation Principles and Processes[1].

[1] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44407

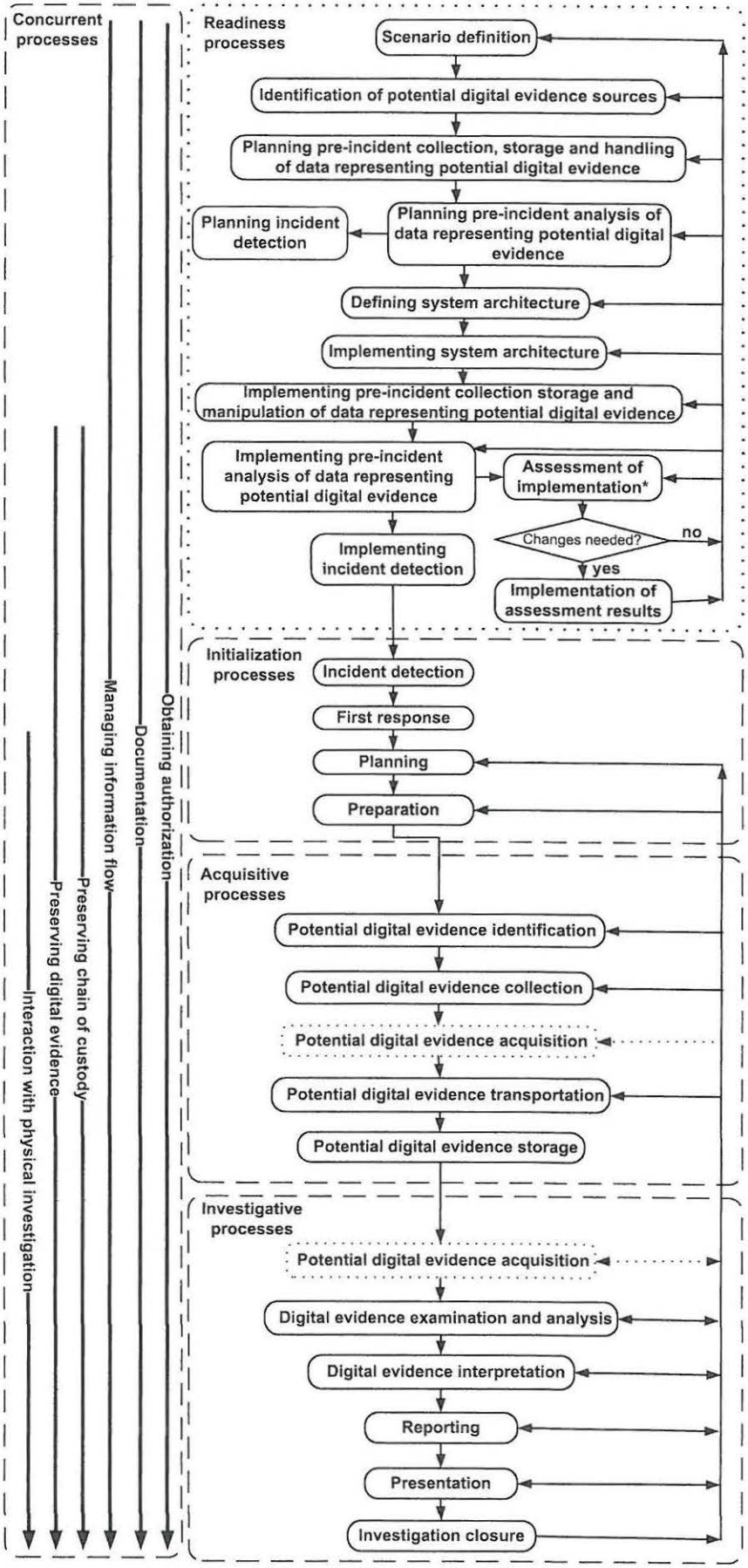


Figure 7 - Harmonised Digital Forensic Investigation Process (Valjarevic & Venter, 2012)

Digital forensics is a process with distinct stages, and as such separate quality assurance practices and processes could not only be applied at each stage of the process, but also collectively across the entire digital forensics process.

An examination of the various digital forensics process models shows that they all contain the following three phases: acquisition of evidence, examination and analysis of the evidence, and reporting on the evidence. These three phases exist in each model, and always follow on from each other (although there may be some additional processes between them in some models, the general flow from one process to the next is in the same direction) and therefore, this can be considered to be a simplified digital forensics process model.

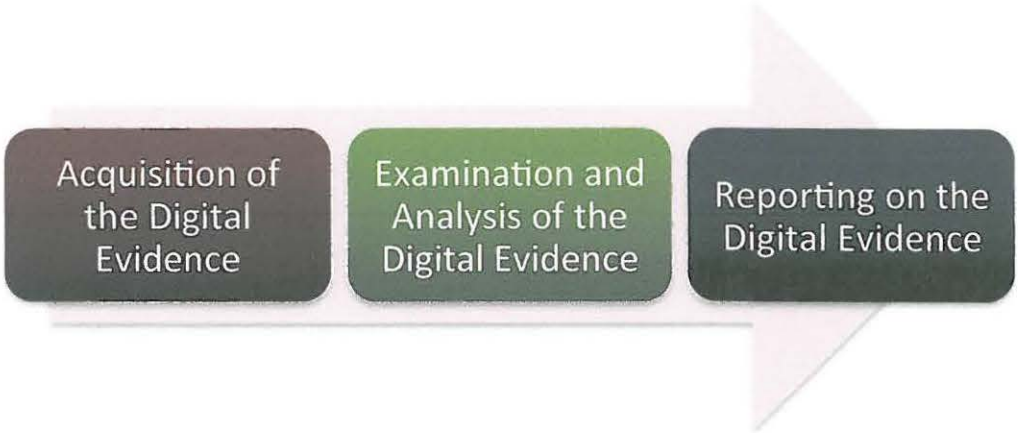


Figure 8 - Simple Digital Forensics Process

This simplification of the various digital forensics process models clearly illustrates that before any digital evidence can be examined and analysed, it must first be acquired. In essence this means that the acquisition of the digital evidence is the most critical part of the digital forensics process as it is the one on which all others depend. In light of the legal issues addressing admissibility and reliability of digital evidence discussed previously, it can be deduced that anything that influences the admissibility or reliability of the digital evidence during the acquisition phase, will taint all the other phases. This could result in the very real possibility that any evidence thus obtained could be challenged in court and potentially excluded from the case at hand.

2.4. THE FORENSIC ACQUISITION PROCESS

The first forensic task in digital forensics is to make a forensic image of the original media, essentially preserving the digital evidence (Nelson, Phillips, Enfinger, & Steuart, 2008). Forensic acquisitions can take place in a "dead" environment where the media to be acquired is removed from the host and is attached to another host with a write blocker to obtain a forensic image, or in a "live" environment where the media is still connected to its host and a forensic image is made of it while it is still connected to the host. A "live" environment is when the host device is still powered on and running when the forensic acquisition process takes place.

Live acquisitions have become common practice due to issues such as encryption; however, because this process will alter the original media, digital forensic practitioners need to be able to document these changes and explain them in court to ensure admissibility as required by the ACPO guidelines (Association of Chief Police Officers, 2007). The forensic acquisition process is the process whereby digital evidence is preserved in a forensically and legally valid manner that is designed to prevent or minimise any alteration or modification of the source data (Sansurooah, 2006). This process is generally referred to as forensic imaging of the evidence (Marcella & Guillossou, 2012).

The forensic acquisition process should change the original evidence as little as possible, and if changes do occur, these changes must be identified and documented, and then assessed in the examination and analysis of the evidence (Casey, 2007).

To illustrate this, consider attaching a USB device containing a forensic imaging software application to a computer running Windows 7 Professional with Bitlocker active. It is necessary to obtain a forensic image of the unencrypted volume, and this can only be done while the computer is running. However, on connecting the USB device to the computer, a number of Registry hives will be written to and data introduced, as well as entries made in the Windows Event Logs located on the media to be imaged. Digital forensic practitioners must be in a position to explain their actions and detail exactly what has been altered on the system through these actions.

The key issue in the forensic acquisition process is that it preserves a complete and accurate representation of the original data, and that the authenticity and integrity of the evidence can be validated (Casey, 2007).

2.4.1. Write Blocking

The simple act of booting a computer, as well as just general interaction with data contained on magnetic and solid state storage media, will normally change data contained on the media connected to the computer, and this contamination can destroy or alter significant data before it can be forensically preserved (Sansurooah, 2006). It is due to this phenomenon that when making a forensic image of original evidence, it is imperative to use a write blocker (Marcella & Guillossou, 2012). A write blocker is a mechanism that intercepts write commands to media before they can be executed on the media, which prevents any alteration to the media. A hardware write blocker is a physical device which media is connected to which intercepts and blocks any write commands, while a software write blocker configures media to be read only, thereby preventing alteration.

The National Institute of Justice strongly recommends that write protection should be used, if available and applicable, when acquiring digital evidence, so as to preserve and protect the original evidence (National Institute of Justice, 2004).

A write blocker allows data to be read from a device or media, but prevents any writes being made to that device or media. Hardware based write blockers are preferred over software write blockers, but there are times when each has specific applications to which it is best suited (Marcella & Guillossou, 2012).

A write blocker, whether implemented in hardware or software, is a crucial part of the forensic acquisition process, and as such it is critical that it functions correctly so as to preserve the original evidence as much as possible.

2.4.2. Forensic Imaging

There are fundamentally two types of forensic imaging methods when dealing with media: making a forensic image of the entire physical media, or only of a logical volume (Nelson, Phillips, Enfinger, & Steuart, 2008). A logical forensic image is usually made of an encrypted volume, while the media is connected to its host and the volume is currently decrypted.

A forensic image is essentially a bit-by-bit copy of the original media that is being imaged (Marcella & Guillossou, 2012). In principle it obtains all the data contained on the media being imaged, including the "live" data, as well as data in unused areas of the media, so that the forensic image itself can be examined as if it were the original media (Sammes & Jenkinson, 2007). The bit-by-bit forensic imaging process involves duplicating all of the data in each and every sector of the original media to a forensic image (Kenneally & Brown, 2005). A forensic image can, depending on the format, also contain metadata relevant to the imaging process itself, such as the image hash values, the date and time of the acquisition, and the details of the examiner making the forensic image.

Certain digital forensic practitioners refer to forensic imaging as mirroring and the resulting forensic image as a mirror image, implying that it is a true mirror of the physical original; however, this is simply not the case. It may be a true bit-by-bit copy of the data, but not of the physical strata of the media, and as such is not a mirror copy of the image. Thus, the use of the term mirror image or mirroring is simply inaccurate (Sammes & Jenkinson, 2007).

Perhaps the most crucial aspect of the forensic imaging process is the process of validating the data acquisition (which is not the same as validating the tools used). During the data validation process, a one-way hash calculation is performed on the original media using the MD5 of one of the SHA hashing algorithms to create a hash value, which functions as a type of digital fingerprint for that particular media. The one-way hash calculation is then performed on the data from the forensic image using the same hashing algorithm to create a hash value. If the hash values of the original data and the image match, then the forensic image is said to be a true "duplicate original" of the original media (Nelson, Phillips, Enfinger, & Steuart, 2008). If they do not match, there has been a problem in the forensic imaging process, and the reliability of the forensic image could be brought into question.

A forensic image is mathematically identical to the original media from which it is made, and is thus legally considered a duplicate original and carries the same weight in court as original evidence would. As a result of this, the reliability of the software or hardware forensic imager that creates the forensic image is crucial to ensure the admissibility of the digital evidence in court.

2.4.3. Quality Assurance Practices in Digital Forensics Relating to the Forensic Acquisition Process

A number of quality assurance practices have been identified in relation to the forensic acquisition of digital evidence.

However, all of these practices are 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 (Swanson, Chamelin, Territo, & Taylor, 2006). 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 (Fereday & Kopp, 2003). 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 (Philipp, Cowen, & Davis, 2010).

The core skills and knowledge of a digital forensics practitioner with regard to the forensic acquisition of digital evidence include (Valli, 2006):

- applying valid forensic processes and principles to acquire digital evidence,
- validating forensic acquisition processes and outcomes using sound scientific principles,
- validating forensic acquisition technology using sound scientific methods and principles.

In relation to the forensic acquisition process, it is thus crucial that digital forensic practitioners are competent to perform all tasks required during the forensic acquisition process, which should include not only the forensic imaging process itself, but also the importance of using validated write blockers and forensic imaging tools, and potentially how to actually validate the tools used in these processes.

Assuring the quality of the acquisition phase of the digital forensic process is the most critical step, as if the acquisition is not carried out correctly, the evidence cannot be used. Quality assurance in the acquisition phase of this process can be achieved through the use of documented proven standard procedures using verified forensic tools to

produce a verified digital evidence image by persons competent to do so, providing that this is checked to ensure that it has been done (Jones & Valli, 2009).

Quality assurance must also be applied to the software tools used in the digital forensic process, including forensic acquisition. Quality assurance can be demonstrated through testing that various critical processes in the digital forensic process are carried out accurately by the application by using appropriate testing such as that used by the National Institute of Standards and Technology's Computer Forensic Tool Testing project (CFTT). The fundamental tests that must be conducted for the software applications used in the forensic acquisition process include (Jones & Valli, 2009):

- that any software that makes a forensic copy of a device or artefacts does so accurately, and
- that any software that produces a checksum, timestamp, or similar device used to verify or validate a digital artefact does so accurately.

The criteria used by the NIST CFTT project is based on standard testing methods and ISO 17025 criteria (Nelson, Phillips, Enfinger, & Steuart, 2008).

Hardware that is used during the forensic acquisition process must also be subjected to quality assurance processes, especially hard drives, write blockers, disk imagers, and computers (Jones & Valli, 2009). As a minimum, this should include:

- Hard drives used to store forensic images must be tested for faults on a regular basis with the appropriate vendor diagnostic tools.
- Before any hard drive is used to store digital evidence, it must be sanitised of any ambient data, and this must be confirmed before it is used.
- Write blockers and disk imagers must be tested on a regular basis to verify that they are working correctly.
- Computers and the hardware therein should be regularly tested using the relevant vendor diagnostic tools.

Due to the nature of the hardware that can be used in the forensic acquisition process, it is crucial that it is tested at regular scheduled intervals to ensure that it works correctly and functions as expected (Jones & Valli, 2009).

When examining the quality assurance practices relating to the hardware and software used in the forensic acquisition process, a common practice is the use of hardware or

software that has been validated as functioning correctly. In the case of write blockers this ensures that they prevent the writing of data to the original media in the forensic acquisition process, while in the case of forensic imaging, it ensures that the forensic image obtained is a true "duplicate original" of the original media.

2.4.4. Importance of Validation in the Forensic Acquisition Process

Digital forensic practitioners make extensive use of forensic software and hardware, and to ensure quality results, they need to satisfactorily answer a number of questions, such as whether the forensic software used has any undocumented "bugs" and whether the forensic hardware was performing correctly (Barbara, 2007). The forensic acquisition process can involve the use of write blockers, which can be either hardware or software, but will always make use of forensic imaging hardware or software, and as such digital forensic tools are a key component of the forensic acquisition process.

Science 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 (Casey, 2011). The power of science in a court of law arises as a result of the supposed objectivity of its methods (Hanna & Mazza, 2006). 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, such as that presented as a result of the digital forensics process, is produced through an objective scientific process using validated methods and tools.

Determining the reliability of forensic tools through validation and verification is a critical quality assurance practice in digital forensics. This is in line with requirements of all forensic sciences, which require that the tools that are used must be trust-worthy. Validation is defined as the confirmation by examination and the provision of objective evidence that a tool functions correctly and as intended. Verification is defined as the confirmation of a validation with laboratory tools (Guo, Slay, & Beckett, 2009).

Hardware and software tools can have defects, and the digital forensics community have a responsibility to identify these defects owing to the nature of forensic work undertaken by them, which must satisfy the most stringent standards to have value in a court of law (Wilsdon & Slay, 2006). It has been observed through interactions with many digital forensic practitioners that some forensic tool vendors promote the strengths of their tools while underplaying their weaknesses, which have included

incomplete forensic acquisitions, amongst others (Casey, 2005). It is crucial that digital forensic practitioners apply due diligence to ensure that the tools used in the forensic acquisition process work correctly. This is best done through validation either by themselves or through a trusted testing process; simply relying on vendor assurances is a significant risk.

Digital forensic examiners should be rigorously questioned when testifying to ensure their credibility and that of their findings. Some of the questions that they should be asked in court include whether they have documentation demonstrating that the forensic software or hardware used were validated prior to their use (Barbara, 2007).

Fundamentally, the importance of validation testing of the tools used in the forensic acquisition process, whether a write blocker of forensic imager, is that it establishes the reliability of the tools used to obtain the digital evidence that will be used in a court of law. If the reliability cannot be established, then the reliability of the evidence itself would potentially be brought into question.

In a South African context, the courts must consider Section 15(3) of the Electronic Communications and Transactions Act 25 of 2002 (Republic of South Africa, 2002), to determine evidential weight of digital evidence, and reliability is an aspect that must be satisfied. If the reliability of a tool used to acquire the digital evidence is challenged, and it cannot be countered through an objective means that it is valid and reliable, the court must take this into consideration.

2.5. VALIDATION STANDARDS AND PRACTICES RELATING TO THE FORENSIC ACQUISITION PROCESS

A number of validation and verification standards and practices exist that are applicable to the various forensic tools that can be used in the forensic acquisition process. These include hardware or software write blockers, and forensic imaging software or hardware. Some are formally documented standards, while others are practices that have developed in an ad-hoc manner by the digital forensics community of practitioners. It is critical to be able to verify the results of any digital forensics tool used, so that the accuracy of the tool can be assured (Carrier, 2003).

In the United States, the Daubert standards, which must be taken into account by a trial judge to assess the credibility of scientific evidence, require that the known or potential

error rate for a particular technique be identified. This has led to some researchers stating that the decision by the trial judge in the Daubert case itself has motivated the necessity to establish error rates for digital forensic tools (Lyle, 2010).

Although the nature of the errors that can occur in complex systems such as those used in a normal computing environment means that the individual errors per test case can be quantified one by one, there does not seem to be a reasonable method to aggregate all of these individual errors into an error rate (Lyle, 2010), as some researchers have stated is a requirement to satisfy the Daubert requirements. This is simply due to the number of variables that exist in any computing system, where multiple software applications are interacting with multiple hardware components, as well as each other. That simply makes it impractical to establish generic error rates.

It is felt that a general error rate for digital forensic tools is not meaningful, and it is more meaningful to identify the specific errors that can occur and account for these, due to the systematic nature of the errors that can occur in a computing environment. To satisfy the spirit of the Daubert requirements (if not the letter thereof), the types of errors and failures for each digital forensic tool, and what conditions trigger a particular error or failure should be identified and documented (Lyle, 2010).

A digital forensic tool validation process should involve the following (Wilsdon & Slay, 2006):

- acquisition of the forensic tool to be evaluated,
- identification of the specific functions of the forensic tool,
- development of test cases and reference sets to be used in the evaluation process,
- development of an acceptable desired standard for the results,
- execution of the tests and evaluation of the results, and
- release of the results of the evaluation.

It must be borne in mind that the development of extensive and exhaustive tests to validate and verify digital forensics tools is a lengthy and complex process (Guo, Slay, & Beckett, 2009). In addition to this, the ability to test digital forensic tools is often limited due to both time and financial constraints for many digital forensic practitioners (Wilsdon & Slay, 2006). In general, digital forensic practitioners have heavy workloads and variations in resources and skill levels, providing conditions that are conducive to

errors occurring in digital forensic tool testing. As a result, the tests themselves may not be accurate (Pan & Batten, 2009).

2.5.1. National Institute of Standards and Technology Computer Forensics Tool Testing Project

The National Institute of Standards and Technology (NIST) has been one of the pioneering organisations trying to address validation and verification of digital forensics tools through their Computer Forensics Tool Testing (CFTT) project. They have developed specific testing methodologies for write blockers and forensic imaging (Guo, Slay, & Beckett, 2009).

The NIST CFTT standards are very comprehensive, but the technical comprehensiveness of the testing criteria also means that testing is time consuming, and requires a high level of technical proficiency.

2.5.1.1. Hardware Write Blockers

The NIST CFTT project defined a fundamental principle when evaluating hardware write blockers that they should block all modifying commands sent to a hard drive. This was subsequently used to define specific requirements for hardware write blockers as detailed in Table 1 (Lyle, 2006).

Table 1 - NIST CFTT Hardware Write Blocker Requirements

Requirement	Description
HWB-RM-01	A hardware write blocker shall not, after receiving an operation of any category from the host, nor any time during its operation, transmit any modifying category operation to a protected storage device.
HWB-RM-02	A hardware write blocker, after receiving a read category operation from the host, shall return the data requested by the read operation.
HWB-RM-03	A hardware write blocker, after receiving and information category operation from the host shall return a response to the host that shall not modify and access significant information contained in the response.
HWB-RM-04	Any error condition reported by the storage device to the hardware write blocker shall be reported to the host.

The requirements for hardware write blockers were then used to develop test assertions, which are testable statements as detailed in Table 2 (Lyle, 2006).

Table 2 - NIST CFTT Hardware Write Blocker Test Assertions

Assertion	Description
HWB-AM-01	The hardware write blocker shall not transmit any modifying category operation to the protected storage device.
HWB-AM-02	If the host sends a read category operation to the hardware write blocker and no error is returned from the protected device to the hardware write blocker, then the data addressed by the original read operation are returned to the host.
HWB-AM-03	If the host sends an information category operation to the hardware write blocker and if there is no error on the protected storage device, then any returned access significant information is returned to the host without modification.
HWB-AM-04	If the host sends an operation to the hardware write blocker and if the operation results in an unresolved error on the protected storage device, then the hardware write blocker shall return an error status code to the host.
HWB-AM-05	The action that a hardware write blocker device takes for any commands not assigned to the modifying, read or information categories is defined by the vendor.

These assertions can be measured to ensure conformity using operational, observational, indirect, and detailed methods. To facilitate this process, a number of defined test cases are used as detailed in Table 3 (Lyle, 2006).

Table 3 - NIST CFTT Hardware Write Blocker Test Cases

Test	Description

HWB-01	Identify commands blocked by the hardware write blocker. This case uses a protocol analyser and a general command generator.
HWB-02	Identify modifying commands blocked by the hardware write blocker. This case uses a write command generator to try to write a unique message to a unique location for each defined write command.
HWB-03	Identify commands blocked by the hardware write blocker while attempting to modify a protected drive with forensic tools. This case uses a protocol analyser to record the commands generated and blocked by attempting to write to a drive with either a forensic tool or an operating system command.
HWB-04	Attempt to modify a protected drive with forensic tools. This case attempts to write to a drive with either a forensic tool or an operating system command. Any modifications to the protected drive are detected by comparing a pre-test hash to a post-test hash.
HWB-05	Identify read commands allowed by the hardware write blocker. A read command generator is used to try to read known data from a drive using each defined read command.
HWB-06	Identify read and information commands use by forensic tools and allowed by the hardware write blocker. Use a forensic tool to read an entire drive with a protocol analyser recording the actual commands used by the forensic tool.
HWB-07	Read a protected drive with forensic tools. Use a forensic tool to read an entire drive.
HWB-08	Identify access significant information unmodified by the hardware write blocker. Use a tool to generate a request for drive size and verify that the correct size is reported.
HWB-09	Determine if an error on the protected drive is returned to the host. Generate an error at the drive by attempting to read a sector beyond the end of the drive.

2.5.1.2. Software Write Blockers

The NIST CFTT project defined a fundamental principle when evaluating software write blockers that they should not allow a protected drive to be changed, they should not prevent obtaining any information from or about any drive, and they should not prevent any operations to a drive that is not protected. These were then used to define specific requirements for software write blockers as detailed in Table 4 (National Institute of Standards and Technology, 2003).

Table 4 - NIST CFTT Software Write Blocker Requirements

Requirement	Description
SWB-RM-01	The tool shall block any commands to a protected drive in the write, configuration, or miscellaneous categories.
SWB-RM-02	The tool shall not block any commands to a protected drive in thread, control or information categories.
SWB-RM-03	The tool shall give an indication to the user that the tool is active.
SWB-RM-04	The tool shall report all drives accessible by the covered interfaces.
SWB-RM-05	The tool shall report the protection status of all drives.
SWB-RM-06	The tool shall, if so configured, adjust the return value of any blocked commands to indicate that the operation was carried out successfully even though the operation was blocked.
SWB-RM-07	The tool shall, if so configured, adjust the return value of any blocked commands to indicate that the operation failed.
SWB-RM-08	The tool shall not block any commands to an unprotected drive.

The requirements for software write blockers were subsequently used to develop test assertions as detailed in Table 5 (National Institute of Standards and Technology, 2003).

Table 5 - NIST CFTT Software Write Blocker Test Assertions

Assertion	Description
SWB-AM-01	If a drive is protected and a command from the write category is issued for the protected drive then the tool shall block the command.
SWB-AM-02	If a drive is protected and a command from the configuration category is issued for the protected drive then the tool shall block the

	command.
SWB-AM-03	If a drive is protected and a command from the miscellaneous category is issued for the protected drive then the tool shall block the command.
SWB-AM-04	If a drive is protected and a command from the read category is issued for the protected drive then the tool shall not block the command.
SWB-AM-05	If a drive is protected and a command from the control category is issued for the protected drive then the tool shall not block the command.
SWB-AM-06	If a drive is protected and a command from the information category is issued for the protected drive then the tool shall not block the command.
SWB-AM-07	If the tool is executed then the tool shall issue a message indicating that the tool is active.
SWB-AM-08	If the tool is executed then the tool shall issue a message indicating all drives accessible by the covered interfaces.
SWB-AM-09	If the tool is executed then the tool shall issue a message indicating the protection status of each drive attached to a covered interface.
SWB-AM-10	If the tool is configured to return *success* on blocked commands and the tool blocks a command then the return code shall indicate successful command execution.
SWB-AM-11	If the tool is configured to return *fail* on blocked commands and the tool blocks a command then the return code shall indicate unsuccessful command execution.

These assertions can then be measured to ensure conformity. To facilitate this process, a number of defined test cases are used, a sample of which are given in Table 6 (National Institute of Standards and Technology, 2003).

Table 6 - NIST CFTT Software Write Blocker Test Cases

Test	Description
SWB-01	Install all drives, configure return code to fail, protect all drives, and

	execute write commands.
SWB-02	Install two drives, configure return code to success, protect all drives, and execute write commands.
SWB-03	Install one drive, configure return code to fail, protect all drives, and execute configuration commands.
SWB-04	Install all drives, configure return code to success, protect all drives, and execute configuration commands.
SWB-05	Install two drives, configure return code to fail, protect all drives, and execute miscellaneous commands.
SWB-06	Install one drive, configure return code to success, protect all drives, and execute miscellaneous commands.
SWB-07	Install all drives, configure return code to fail, protect all drives, and execute read commands.
SWB-08	Install two drives, configure return code to success, protect all drives, and execute read commands.
SWB-09	Install one drive, configure return code to fail, protect all drives, and execute information commands.
SWB-10	Install all drives, configure return code to success, protect all drives, and execute information commands.
SWB-11	Install two drives, configure return code to fail, protect all drives, and execute control commands.
SWB-12	Install one drive, configure return code to success, protect all drives, and execute control commands.
SWB-13	Install all drives, configure return code to fail, protect with pattern odd (Pattern odd protects each odd numbered drive: 0x81, 0x83, 0x85, etc.), and execute write commands.
SWB-14	Install all drives, configure return code to success, protect with pattern low (Pattern low protects the low numbered drives: 0x80, 0x81, etc. Given *n* drives, the first unprotected drive is 0x80 + *n*/2, using integer division discarding any fraction), and execute write

	commands.
SWB-15	Install all drives, configure return code to fail, protect with pattern first (Pattern first protects drive 0x80), execute configuration commands.
SWB-16	Install all drives, configure return code to success, protect with pattern mid (Pattern mid protects, given *n* drives, drive 0x80 + *n*/2. Discarding any fraction), and execute configuration commands.
SWB-17	Install all drives, configure return code to fail, protect with pattern random_p (Pattern random protected, selects at random one drive that has not been used as a single protected drive. If there are no unused drives, selected any drive at random), and execute miscellaneous commands.
SWB-18	Install all drives, configure return code to success, protect with pattern not_last (Given *n* drives, protect all drives except for drive 0x80 + *n* – 1), and execute miscellaneous commands.
SWB-19	Install all drives, configure return code to fail, protect with pattern last (Given *n* drives protect drive 0x80 + *n* - 1.), execute read commands.
SWB-20	Install all drives, configure return code to success, protect with pattern not_mid (Given *n* drives, protect all drives except for 0x80 + *n*/2, discarding any fraction), and execute read commands.
SWB-21	Install all drives, configure return code to fail, protect with pattern high (Protect the high numbered drives. Given *n* drives, the first protected drive is 0x80 + *n*/2), and execute information commands.
SWB-22	Install all drives, configure return code to success, protect with pattern not_first (Protect all drives except for 0x80, and execute information commands.
SWB-23	Install all drives, configure return code to fail, protect with pattern random_u (Select at random one drive that has not been used as a single unprotected drive. If there are no unused drives, select any drive at random), and execute control commands.

SWB-24	Install all drives, configure return code to success, protect with pattern even (Protect the even numbered drives: 0x0, 0x82, 0x4, etc.), and execute control commands.
SWB-25	Install three drives, configure return code to fail, protect with pattern PUU (The first drive is protected and the second and third drives are not protected), and execute write commands.
SWB-26	Install three drives, configure return code to success, protect with pattern UPU (The second drive is protected and the first and third drives are not protected), and execute write commands.
SWB-27	Install three drives, configure return code to fail, protect with pattern UUP (The third drive is protected and the first and second drives are not protected), and execute write commands.
SWB-28	Install three drives, configure return code to success, protect with pattern UPP, and execute write commands.
SWB-29	Install three drives, configure return code to fail, protect with pattern PUP, and execute write commands.
SWB-30	Install three drives, configure return code to success, protect with pattern PPU, and execute write commands.
SWB-31	Install three drives, configure return code to fail, protect with pattern PUU, and execute read commands.
SWB-32	Install three drives, configure return code to success, protect with pattern UPU, and execute read commands.
SWB-33	Install three drives, configure return code to fail, protect with pattern UUP, and execute read commands.
SWB-34	Install three drives, configure return code to success, protect with pattern UPP, and execute read commands.
SWB-35	Install three drives, configure return code to fail, protect with pattern PUP, and execute read commands.

SWB-36	Install three drives, configure return code to success, protect with pattern PPU, and execute read commands.
SWB-37	Install all drives, configure to be active at boot and shutdown, configure return code to fail, protect with pattern odd, and execute write commands.
SWB-38	Install all drives, configure to be active at boot and shutdown, configure return code to success, protect with pattern even, and execute write commands.
SWB-39	Install all drives, configure return code to fail, protect with pattern high, execute write commands, uninstall, and execute all commands.
SWB-40	Install all drives, configure return code to success, protect with pattern low, execute write commands, uninstall, and execute all commands.

2.5.1.3. Forensic Imaging Tools

The forensic imaging specification developed by the NIST CFTT requires that a forensic imaging application must make a bit-stream duplicate or forensic image of an original disk or partition, it must not alter the original disk, it must be able to verify the integrity of an image file, and it must log I/O errors (Lyle, 2003).

When making a forensic image of a hard drive, all sectors of the media should be completely and accurately acquired and saved to an image file. However, some hard drives will occasionally contain faulty sectors that cannot be acquired using traditional forensic imaging tools. Forensic imaging tools should meet the following requirements (which are requirements of the National Institute of Standards and Technology in the United States), for handling faulty sectors (Lyle & Wozar, 2007):

- The tool must acquire all sectors that are not faulty.
- The tool must identify all faulty sectors.
- In instances where there are faulty sectors, the forensic image file must replace the faulty sector content with benign fill that will have no influence on the results of an examination.

These were subsequently used to define specific requirements for forensic imaging tools as detailed in Table 7 (National Institute of Standards and Technology, 2004).

Table 7 - NIST CFTT Forensic Imaging Tool Requirements

Requirement	Description
DI-RM-01	The tool shall be able to acquire a digital source using each access interface visible to the tool.
DI-RM-02	The tool shall be able to create either a clone of a digital source, or an image of a digital source, or provide the capability for the user to select and then create either a clone or an image of a digital source.
DI-RM-03	The tool shall operate in at least one execution environment and shall be able to acquire digital sources in each execution environment.
DI-RM-04	The tool shall completely acquire all visible data sectors from the digital source.
DI-RM-05	The tool shall completely acquire all hidden data sectors from the digital source.
DI-RM-06	All data sectors acquired by the tool from the digital source shall be accurately acquired.
DI-RM-07	If there are unresolved errors reading from a digital source then the tool shall notify the user of the error type and the error location.
DI-RM-08	If there are unresolved errors reading from a digital source then the tool shall use a benign fill in the destination object in place of the inaccessible data.

The requirements for forensic imaging tools were then used to develop test assertions as detailed in Table 8 (National Institute of Standards and Technology, 2005).

Table 8 - NIST CFTT Forensic Imaging Tool Test Assertions

Assertion	Description
DA-AM-01	The tool uses access interface SRC-AI to access the digital source.
DA-AM-02	The tool acquires digital source DS.
DA-AM-03	The tool executes in execution environment XE.

DA-AM-04	If clone creation is specified, the tool creates a clone of the digital source.
DA-AM-05	If image file creation is specified, the tool creates an image file on file system type FS.
DA-AM-06	All visible sectors are acquired from the digital source.
DA-AM-07	All hidden sectors are acquired from the digital source.
DA-AM-08	All sectors acquired from the digital source are acquired accurately.
DA-AM-09	If unresolved errors occur while reading from the selected digital source, the tool notifies the user of the error type and location within the digital source.
DA-AM-10	If unresolved errors occur while reading from the selected digital source, the tool uses a benign fill in the destination object in place of the inaccessible data.

These assertions can be measured to ensure conformity. To facilitate this process, a number of defined test cases are used as detailed in Table 9 (National Institute of Standards and Technology, 2005); however, not all test cases would be required for all assertions.

Table 9 - NIST CFTT Forensic Imaging Tool Test Cases

Test	Description
DA-01	Acquire a physical device using access interface AI to an unaligned clone.
DA-02	Acquire a digital source of type DS to an unaligned clone.
DA-03	Acquire a physical device to a cylinder aligned clone.
DA-04	Acquire a physical device to a truncated clone.
DA-05	Respond to a write error on the clone device during an acquisition to a clone.
DA-06	Acquire a physical device using access interface AI to an image file.
DA-07	Acquire a digital source of type DS to an image file.

DA-08	Acquire a physical drive with hidden sectors to an image file.
DA-09	Acquire a digital source that has at least one faulty data sector.
DA-10	Acquire a digital source to an image file in an alternate format.
DA-11	Respond to a disk error writing an image file.
DA-12	Attempt to create an image file where there is insufficient space.
DA-13	Create an image file where there is insufficient space on a single volume, and use destination device switching to continue on another volume.
DA-14	Create an unaligned clone from an image file.
DA-15	Create a cylinder aligned clone from an image file.
DA-16	Create a clone from a subset of an image file.
DA-17	Create a truncated clone from an image file.
DA-18	Respond to a write error on the clone device while creating a clone from an image.
DA-19	Acquire a physical device to an unaligned clone, filling excess sectors.
DA-20	Acquire a logical device to an unaligned clone, filling excess sectors.
DA-21	Acquire a physical device to a cylinder aligned clone, filling excess sectors.
DA-22	Create an unaligned clone from an image file, filling excess sectors.
DA-23	Create a cylinder aligned clone from an image file, filling excess sectors.
DA-24	Verify a valid image.
DA-25	Detect a corrupted image.
DA-26	Convert an image to an alternate image file format.

2.5.2. The Scientific Working Group on Digital Evidence

The Scientific Working Group on Digital Evidence (SWGDE) has also been working on issues pertaining to the validation and verification of digital forensics tools, and rather than develop specific testing methodologies as the NIST CFTT project has done, they have recommended general guidelines for validation testing. The SWGDE validation guidelines for digital forensic tools include defining the purpose and scope of the validation test, defining the requirements to be tested, determining the methodology to be used, selecting appropriate test scenarios, conducting the tests, and documenting the process (Guo, Slay, & Beckett, 2009).

It is recommended that validation testing should be performed whenever a new, revised or reconfigured tool is introduced into the forensic process (Scientific Working Group on Digital Evidence, 2009).

The recommendation for when tools should be tested however, does not take into account hardware based tools, which being electronic devices, can fail over time and as such, should be tested on a regular basis to ensure that they remain functional.

2.5.3. European Network of Forensic Science Institutes

The European Network of Forensic Science Institutes has published broad validation testing guidelines for forensic imaging, which recommend that the imaging tools be checked to ensure that they make no changes to the original media, that the imaging verification process is reliable, and that the audit or log functions of the tool are accurate and detailed. With regard to write blocking tools, all that they require is that they need to be tested to ensure that they do not change any data on the original media (European Network of Forensic Science Institutes, 2009).

2.5.4. Dual Tool Validation

Dual tool verification is a process whereby two different digital forensics tools are used to confirm whether both tools produce the same result (Association of Chief Police Officers, 2011).

After one tool has been used to obtain a particular outcome, the results should be verified by performing the same tasks with another similar forensic tool (Nelson, Phillips, Enfinger, & Steuart, 2008). Cross-validation is an important element of quality assurance in digital forensics, and requires the findings of a particular digital forensic

tool to be verified by another digital forensic tool (Philipp, Cowen, & Davis, 2010). Making use of only one forensic tool (and therefore trusting it blindly) creates an opportunity for the opposing party to target the tool instead of the process.

There is, however, a logical flaw in the concept of dual tool validation. What if both tools that are used in a dual tool validation do not work correctly? Unless the tool used to compare against is known to be functioning correctly and reliably, one cannot say with certainty that the tool it is being compared to is functioning correctly either. If one does make use of the dual tool validation method, then the tool being used for comparison purposes should at least have been independently validated to ensure a measure of reliability.

2.5.5. Vendor Validation

There is a heavy reliance on digital forensic tools in the practice of digital forensics, and this reliance often hinges on blind faith that the specific tool works. This has actually lead to industry myths that certain of these tools have been accepted by the courts and are thus court validated. Vendors, who are often protective of their commercial market share, have not officially published error rates for their digital forensic tools, or the exact reasons for minor and major version changes (Meyers & Rogers, 2005).

A problem with vendor validation is that it is generally undocumented and not proven publically, except through comments, which are mostly hearsay on the bulletin boards of the vendors themselves (Guo, Slay, & Beckett, 2009).

Unless the vendor validation has been documented and made publically available, little reliance can actually be placed on the idea of vendor validation.

2.6. SUMMARY

Digital evidence is clearly defined both from a scientific and legal perspective, and both definitions are aligned to each other. The nature of digital evidence, however, does raise certain legal challenges, which need to be addressed to ensure the reliability and admissibility of the evidence. Digital forensics is the process that fundamentally addresses the reliability and admissibility of the digital evidence in a court of law.

Digital forensics is a science, and as such is considered to be governed by many of the requirements of traditional forensic science. Thus, issues such as quality assurance are

crucial to ensuring that the evidence produced through a forensic science process is considered valid. A number of models have been developed describing the digital forensics process, all of which include three specific stages: acquisition, examination and analysis, and report and testifying.

A key aspect of the digital forensics process is that the digital evidence must first be preserved for examination and analysis during the forensic acquisition phase, and as such this phase is considered the most critically important of the entire digital forensics process. It is thus crucial that quality assurance is ensured in this phase as all other phases of the digital forensics process are dependent on it.

The forensic acquisition phase consists of one mandatory process, forensic imaging, and another recommended process, write blocking. These processes play a significant role in the preservation of the digital evidence, which is used for later examination and analysis, and which will ultimately be presented in court. As such it is crucial that the evidence preserved through this is reliable. These processes are, however, dependent on software and/or hardware tools and it is crucial that these tools function reliably and correctly, so that the evidence preserved though them can be considered reliable as well. There is a real risk in court that if the tools used are not reliable, then the reliability of the digital evidence court will be brought into question and the evidence ruled inadmissible.

Tool validation is the process by which the various forensic tools are tested and evaluated for reliability. Specific validation practices and standards are considered within the digital forensics community.

There are formally documented testing standards such as those developed by the National Institute of Standards and Technology, which are very comprehensive and technically valid. There are recommended testing guidelines such as those issued by the Scientific Working Group on Digital Evidence and the European Network of Forensic Science Institutes. There are also practitioner standards that have evolved through practice, such as dual tool validation. Finally, there is the belief that vendors themselves validate the tools.

3. RESEARCH DESIGN

The purpose of the research was to examine the current state of validation testing practices with regards the hardware and/or software tools used by digital forensic practitioners in South Africa for the purposes of preserving and acquiring digital evidence, so as to determine areas of concern that could negatively impact on the use of digital evidence in a court of law. As discussed in Chapter 1, our main objectives were the following:

- To determine the current state of practice with regards the validation testing of hardware and/or software tools used in the forensic acquisition process amongst South African digital forensic practitioners.
- To identify shortcomings and deficiencies (if any) in the use of hardware and/or software tools used during the forensic acquisition process, relating to the reliability of the tools used, and the impact this could have on the reliability of digital evidence in court proceedings.
- To identify possible reasons for any shortcomings and deficiencies (if any) in use of hardware and/or software tools used during the forensic acquisition process, relating to the reliability of the tools used.

To achieve the purpose of this research, a specific research methodology was utilised as detailed below.

3.1. RESEARCH PHILOSOPHY

The research philosophy selected provides the overall assumptions made by the research in terms of the way in which the research views the particular field, and underpins the research strategy followed as well as the methods chosen as part of that strategy (Saunders, Lewis, & Thornhill, 2009).

The research philosophy embraced by the researcher was pragmatism. The nature of digital forensic practice is, by the nature of the field, multidisciplinary and as such, the research questions asked and the relevance of different subject areas may require specific epistemologies, ontologies, and axiologies, each to answer a specific research question (Saunders, Lewis, & Thornhill, 2009). This research philosophy is thus appropriate in a multidisciplinary field such as digital forensics.

3.2. RESEARCH PURPOSE

The purpose of the research was an exploratory study. Exploratory studies are suitable for establishing what is happening, asking questions, and assessing practices (Saunders, Lewis, & Thornhill, 2009), which is the fundamental objective of this research.

An advantage of an exploratory study is that it is particularly useful in determining the nature of a problem and to clarify the understanding thereof (Saunders, Lewis, & Thornhill, 2009). Previous research, which had a limited scope, identified some concerns with regard to the general validation of tools used in digital forensics in South Africa; however, this was not examined in depth. This research builds on this initial research and explores validation practices in relation to the forensic acquisition of digital evidence in depth. As such an exploratory study is highly relevant.

3.3. RESEARCH APPROACH

The research approach selected is a combination of deduction and induction. The multidisciplinary nature of digital forensics requires an in-depth understanding of disciplines ranging from computer science to law to criminology and how these interrelate, as there is not always a simple cause and effect answer (Saunders, Lewis, & Thornhill, 2009). The inductive research approach allowed the researcher to gain a better understanding of the issues and contexts, which add value to the practical application of the research, while the deductive approach was used to test the hypothesis.

3.4. RESEARCH STRATEGY

The research strategy selected for the research was a survey based approach. The basis for selecting the survey approach is that it allows for the collection of structured quantitative data suitable for an exploratory study. The use of a survey approach using questionnaires allows for standardisation of the data and easy comparison thereof (Saunders, Lewis, & Thornhill, 2009).

The survey strategy is particularly adept at generating answers to questions such as "who", "what", "where", "how many", and "how much" (Saunders, Lewis, & Thornhill, 2009), which are the fundamental question types utilised as research questions in this research.

3.5. RESEARCH TIME FRAME

The research time frame was a cross-sectional one, as it sought to explore the state of validation practices in relation to hardware and/or software forensic tools used in the forensic acquisition of digital evidence, at a particular point in time. The results are in effect a "snapshot" of the current situation in time (Saunders, Lewis, & Thornhill, 2009).

3.6. RESEARCH METHOD

The research method used in the research was a mixture of quantitative and qualitative methods, providing a holistic approach to the research problem.

Quantitative research is appropriate when trying to identify trends and generalisations that can be applied to a whole population (Saunders, Lewis, & Thornhill, 2009). Qualitative research is an approach best suited to attempts to better understand complex and interactive phenomena, particularly since these phenomena are often unique (Schloss & Smith, 1999). There is no doubt that the interplay between the legal system and digital forensic procedures and processes by digital forensic practitioners, is complex. The use of a qualitative approach is important, especially when examining exactly how digital forensic practitioners conduct validation testing and how these practices compare to acceptable standards. Taking these factors into account, a qualitative research approach was deemed appropriate.

3.7. SAMPLING

The population represents the full set of cases from which a sample can be obtained (Saunders, Lewis, & Thornhill, 2009). In the context of this research, the population can be defined as digital forensic practitioners practising digital forensics as their primary profession. The researcher is the head of a digital forensics laboratory in a national law enforcement agency. By virtue of his position he is well known to the digital forensic practitioner community in South Africa. He also has access to many members of this community across multiple agencies and organisations.

Owing to practical issues such as the availability and willingness of members of the population, and the time frame available for conducting the research, it was not practical to use the entire population as a source of data for this research. As such it was necessary to make use of sampling. A sample is no more than a sub-group of the entire population (Saunders, Lewis, & Thornhill, 2009).

To determine the sample, the random sampling method was used (Saunders, Lewis, & Thornhill, 2009). The survey instrument used was an online survey, and invitations to complete the survey were sent to all known digital forensic practitioners in South Africa; those who responded represented a random sample, as the researcher was not in a position to determine who would actually respond to the survey.

3.8. DATA COLLECTION

The data collection was conducted by means of an Internet based structured questionnaire, which is an appropriate method to collect quantitative data and limited qualitative data. This allowed for standardisation and ease of comparison. It is also shown to be an appropriate data collection method in exploratory studies, such as is the case with this research (Saunders, Lewis, & Thornhill, 2009).

Careful consideration was given to the design of the questionnaire to be used to ensure that there was internal validity in the questionnaire itself, so that the data would be considered valid, while attention was also paid to content validity (Saunders, Lewis, & Thornhill, 2009). The questions asked in the questionnaire were specifically selected to answer the research questions stated for this research, thereby addressing content validity of the questionnaire.

Reliability of the questionnaire was addressed by designing the questionnaire itself for internal consistency by correlating the responses to each question in the questionnaire with others in the questionnaire (Saunders, Lewis, & Thornhill, 2009).

The questionnaire is detailed in the Appendix.

3.9. DATA ANALYSIS

The data received from the respondents to the Internet based survey questionnaire formed the basis of the data to be analysed.

The first stage of the analysis involved collating the data from the questionnaires, which was downloaded from the Internet survey system as a spreadsheet and then converted into a relational database to allow queries to be run against the data more efficiently.

The data itself was analysed using an exploratory data analysis approach using diagrams and tables to aid in the exploration of the data to identify specific data and values of

interest, to identify and compare trends and proportions, and to illustrate distributions within the data sets (Saunders, Lewis, & Thornhill, 2009).

3.10. ETHICAL ISSUES

All participants in this research consented to the research by way of informed consent (Saunders, Lewis, & Thornhill, 2009), which was provided by means of the Internet based survey questionnaire. Participation in the research was voluntary, and no participant was compelled in any way to participate.

While the respondents could potentially be identified by their email addresses which were recorded in the survey questionnaire, this has not been included in the data analysed, and has remained privileged and not released by the researcher. In addition, care was taken to ensure that no specific agency affiliations were identified so as not to prejudice individual participants or affiliated agencies, which could compromise their effectiveness in presenting evidence in court. The confidentiality of the data has been maintained at all times.

In addition to complying with any prescribed research codes of ethics prescribed by Rhodes University, the researcher was bound by the code of ethics governing him as a computing professional (Code of Ethics of the Institute of Information Technology Professionals of South Africa, Code of Ethics of the Association of Computing Machinery, and Code of Ethics of the Institute for Electrical and Electronics Engineers), as well as those governing him as a professional digital forensic practitioner and fraud examiner (Code of Ethics of the International Association of Computer Investigative Specialists, Code of Ethics of the SANS Institute, and Code of Ethics of the Association of Certified Fraud Examiners).

3.11. SUMMARY

The research design selected allows the collection and analysis of relevant data directly from primary sources, namely South Africa practitioners who make use of the forensic tools to acquire digital evidence. This ensures the relevance of the research to the research objectives.

4. SURVEY DESIGN AND IMPLEMENTATION

Implementing the research design required the design and hosting of the questionnaire, the invitation to potential respondents to complete the questionnaire, and finally the extraction of the data from the questionnaire for analysis.

4.1. RESEARCH QUESTIONNAIRE

The research questionnaire was designed using skip logic so that respondents would only have to answer questions that were relevant to them, and as such, an ICT based survey platform was considered to allow for the implementation of this.

The research questionnaire was hosted using SurveyMonkey[2], an Internet based survey service, which was selected owing to its ease of use and security. This tool also allowed the use of skip logic in the design of the questionnaire itself, which resulted in a more dynamic, yet structured user experience for respondents.

Before the survey questionnaire went live, it was extensively tested by the researcher to ensure that the skip logic functionality functioned correctly, and that the questionnaire functioned as intended. Once the testing was finalised the questionnaire went live and was available to respondents to complete.

4.2. IDENTIFICATION OF PROSPECTIVE RESPONDENTS

The researcher made use of two methods to identify potential respondents, to whom emails were sent requesting their participation in the research.

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.

The researcher then conducted a search using LinkedIn[3], to identify all individuals in South Africa who were employed as digital forensic practitioners. A total of 57 individuals were identified that met this criterion and invitations were sent to them requesting their participation in the survey.

[2] http://www.surveymonkey.net
[3] http://www.linkedin.com

Since a number of these individuals were employed by organisations to which invitations had previously been sent, the questionnaire required respondents to provide their e-mail address to validate that duplicate responses were not received.

The survey was opened for participation for a period of six months to ensure a maximum possible participation rate.

4.3. DATA COLLECTION AND COLLATION

At the time the survey was closed, a total of 56 unique responses had been received, and the data were downloaded from SurveyMonkey in a Microsoft Excel spreadsheet format, which was then imported into Microsoft Access to be analysed.

4.4. SUMMARY

The research implementation was in line with the research design, and the survey was deployed using a well-established internet based survey based service. Prospective participants were identified, all of which were digital forensic practitioners. In total 56 digital forensic practitioners responded to the survey and their responses form the core of the data that was analysed.

5. SURVEY ANALYSIS AND DISCUSSION OF FINDINGS

The research results and findings are based on the data provided by the respondents. All of the respondents were current digital forensic practitioners, and as such their responses to the survey represent data from the relevant population.

There were a total of 56 respondents. The population of digital forensic practitioners in South Africa is generally considered small, but to date there is no quantifiable data indicating the exact number of digital forensic practitioners in South Africa; however, estimates place the number at no more than 150 practitioners. 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.

5.1. AGE, GENDER, AND LOCATION

Twenty-three respondents were aged between 30 and 39 years of age (41% of the sample), 17 were aged between 40 and 49 (30% of the sample), 14 were aged between 21 and 29 (25% of the sample), and two were aged between 50 and 59 (4% of the sample). The percentages are illustrated in Figure 9.

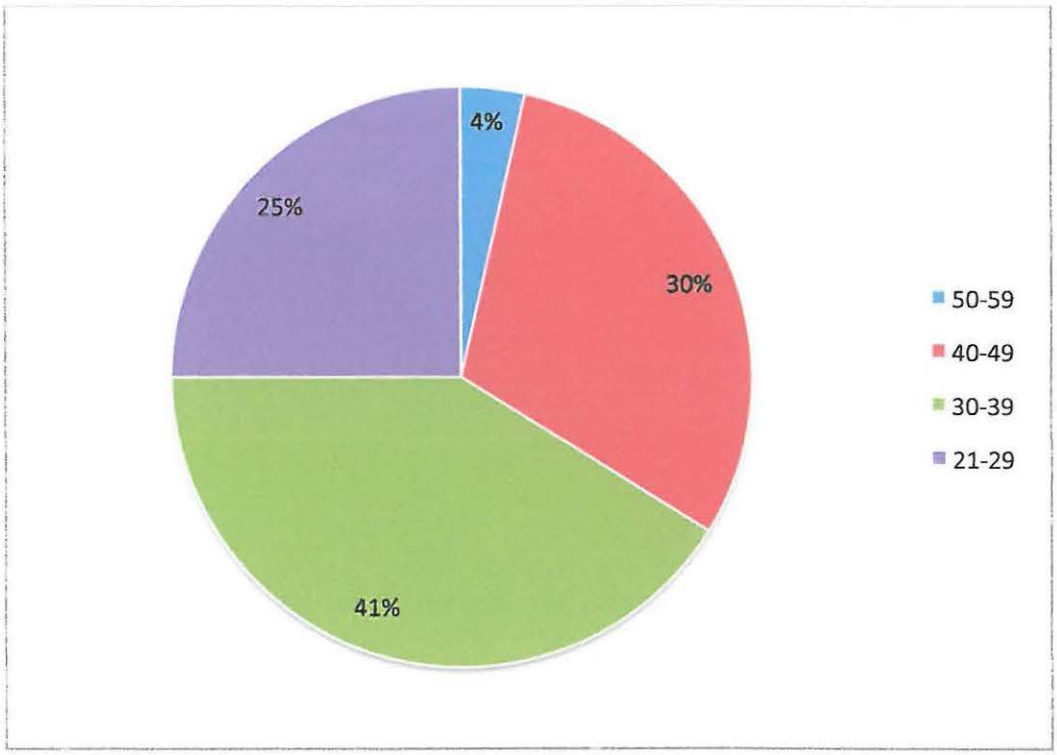


Figure 9-Age Distribution

Forty-eight respondents were male (86% of the sample), and eight were female (14% of the sample). The gender distribution expressed as a percentage is illustrated in Figure 10, which clearly demonstrates that the majority of digital forensic practitioners in South Africa are male.

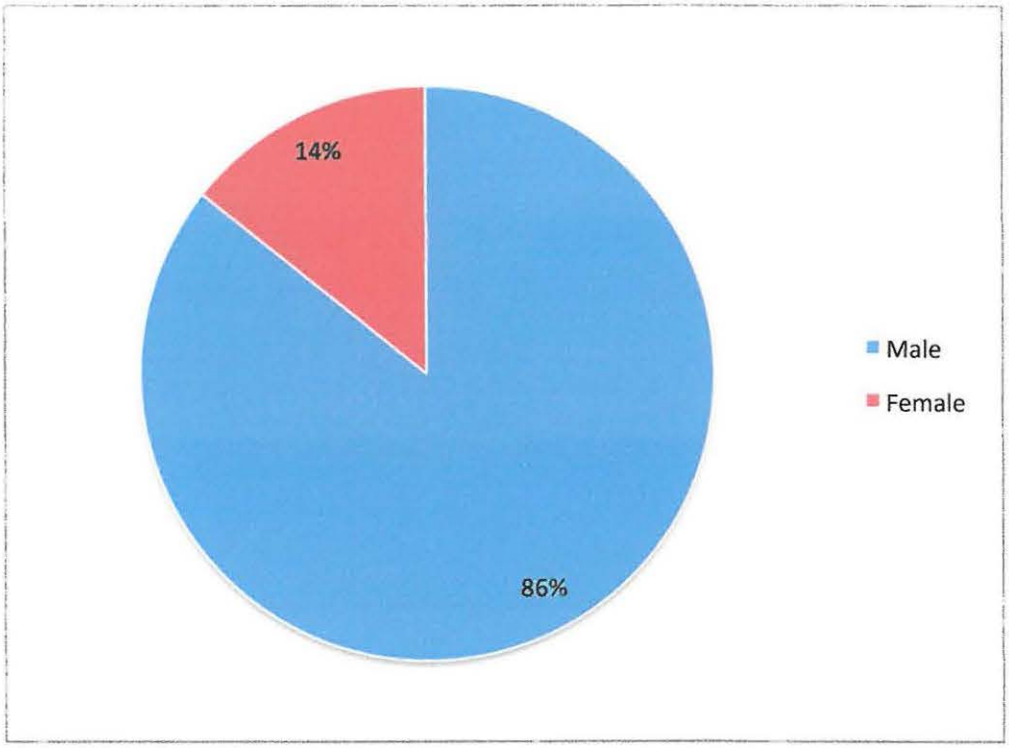


Figure 10-Gender Distribution

Thirty-eight respondents were living in Gauteng (68% of the sample), 11 in the Western Cape (20% of the sample), four in the Eastern Cape (11% of the sample), two in the Free State (3% of the sample), and one in KwaZulu Natal (2% of the sample). There were no respondents from the Northern Cape, North West, Limpopo, or Mpumalanga. The researcher is of the opinion that the reasons for this is that these provinces are not major commercial centres, and that due to their proximity to Gauteng they are most often serviced by digital forensic practitioners from Gauteng. The provincial distribution expressed as a percentage is illustrated in Figure 11.

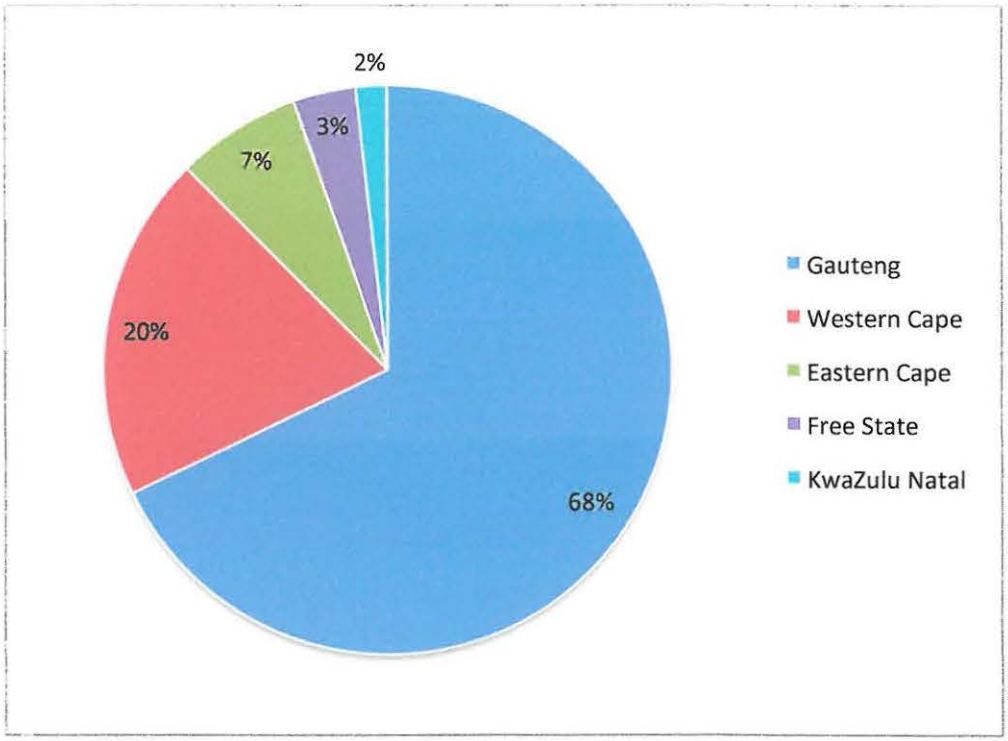


Figure 11 - Geographic Distribution of Respondents

5.2. 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 (Valli, 2006). 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.

5.2.1. Secondary School Education

All of the respondents had completed Grade 12. Thirty-seven had completed Grade 12 with a University exemption, and 19 had completed Grade 12 without a University exemption. The percentages are illustrated in Figure 12.

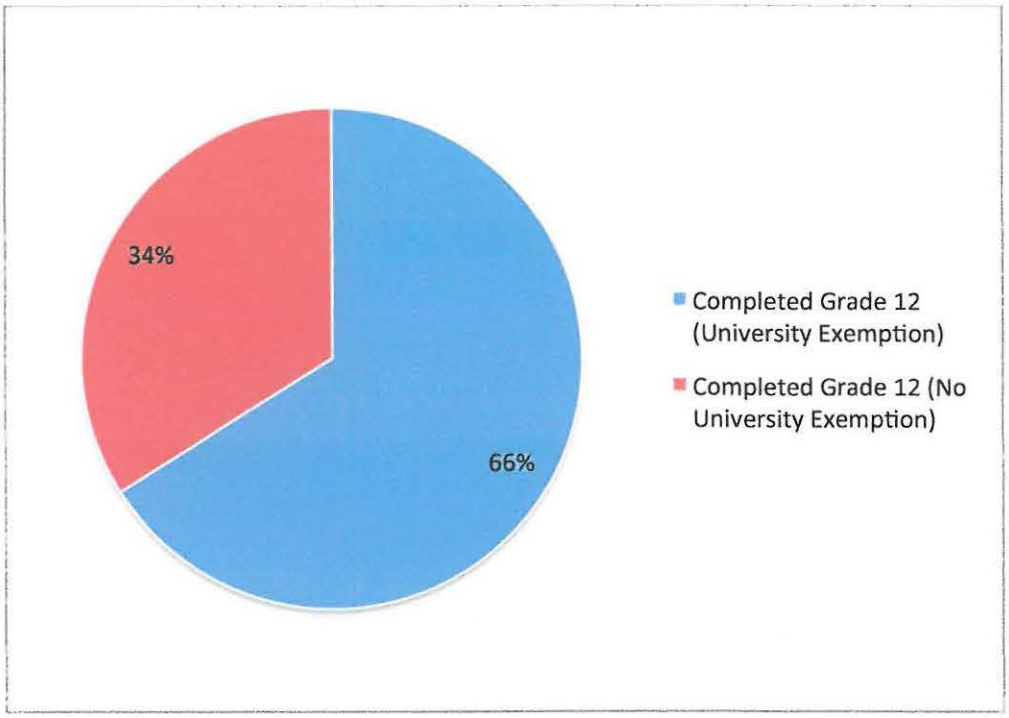


Figure 12 - Matriculation

Figure 12 clearly illustrates that 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% of the sample), two respondents had failed mathematics in Grade 12 (3% of the sample), and six respondents did not have mathematics as a subject in Grade 12 (11% of the sample). The percentages are illustrated in Figure 13.

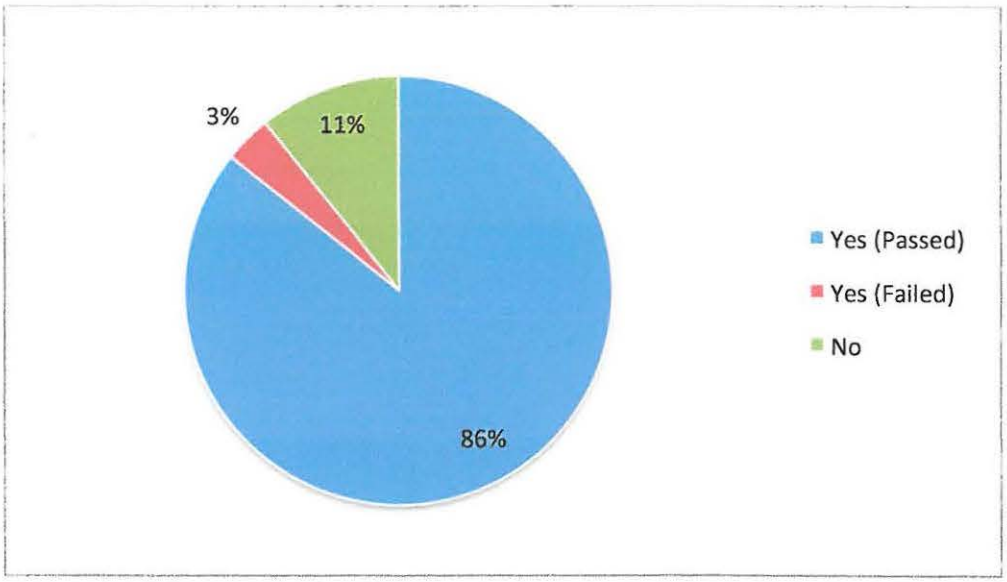


Figure 13 - Grade 12 Mathematics

Thirty-six respondents had passed physical science in Grade 12 (64% of the sample), while 20 respondents did not have physical science as a subject in Grade 12 (36% of the sample). The percentages are illustrated in Figure 14.

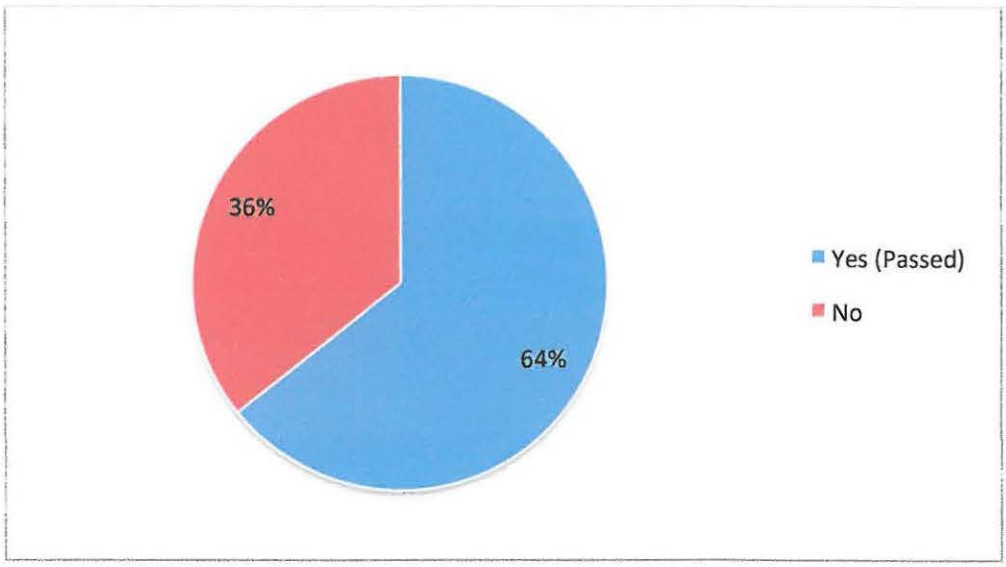


Figure 14 - Grade 12 Physical Science

Fifteen respondents had passed information technology in Grade 12 (27% of the sample), while 41 respondents did not have information technology as a subject in Grade 12 (73% of the sample). The percentages are illustrated in Figure 15.

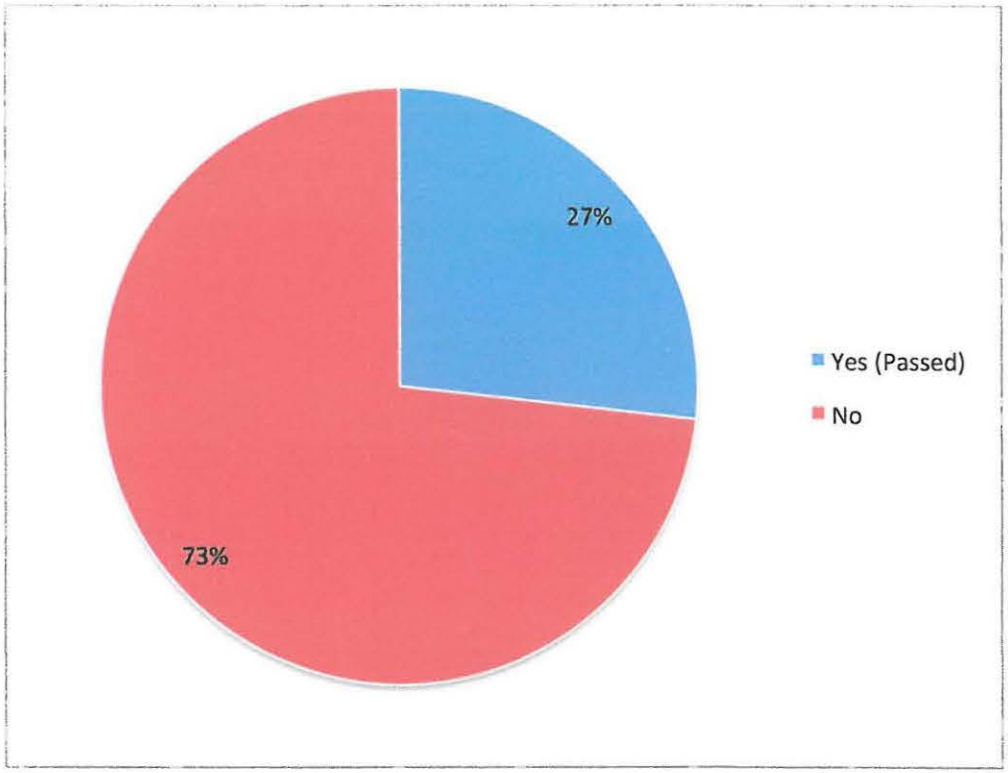


Figure 15 - Grade 12 Information Technology

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.

5.2.2. 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 (National Research Council, 2009). The European Network of Forensic Science Institutes recommends that digital forensic practitioners have a minimum of a degree in computer science or computer engineering (European Network of Forensic Science Institutes, 2009). 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 (United Nations Office on Drugs and Crime, 2011).

Thirty-three respondents had completed an undergraduate degree or diploma (59% of the sample), while 23 of the respondents had not completed an undergraduate degree or diploma (41% of the sample). The percentages are illustrated in Figure 16.

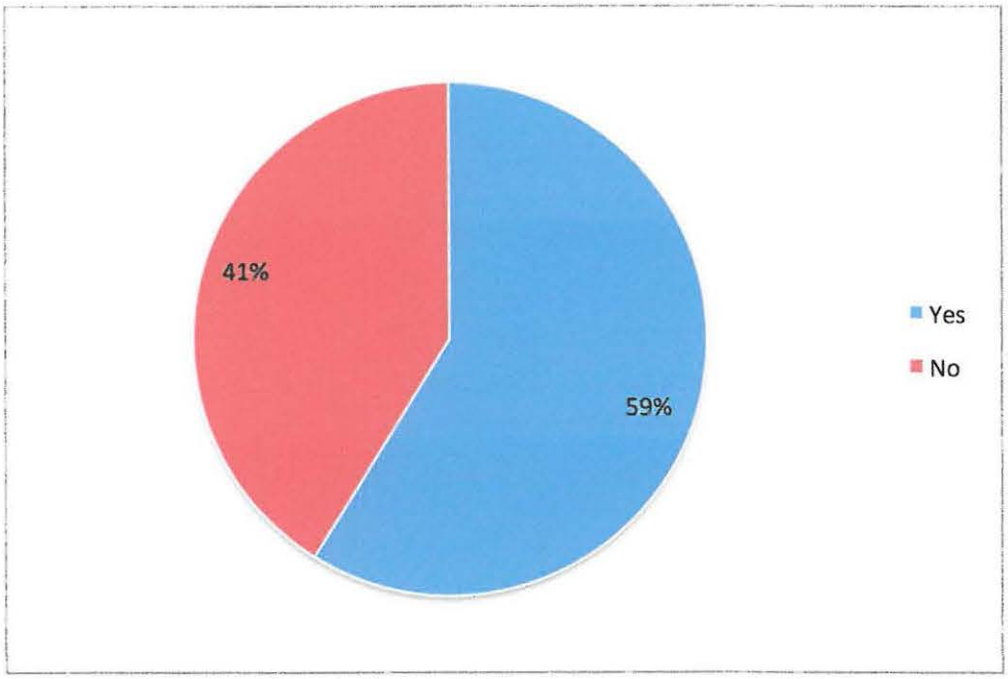


Figure 16 - Undergraduate Qualifications

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 10.

Table 10 - 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 17.

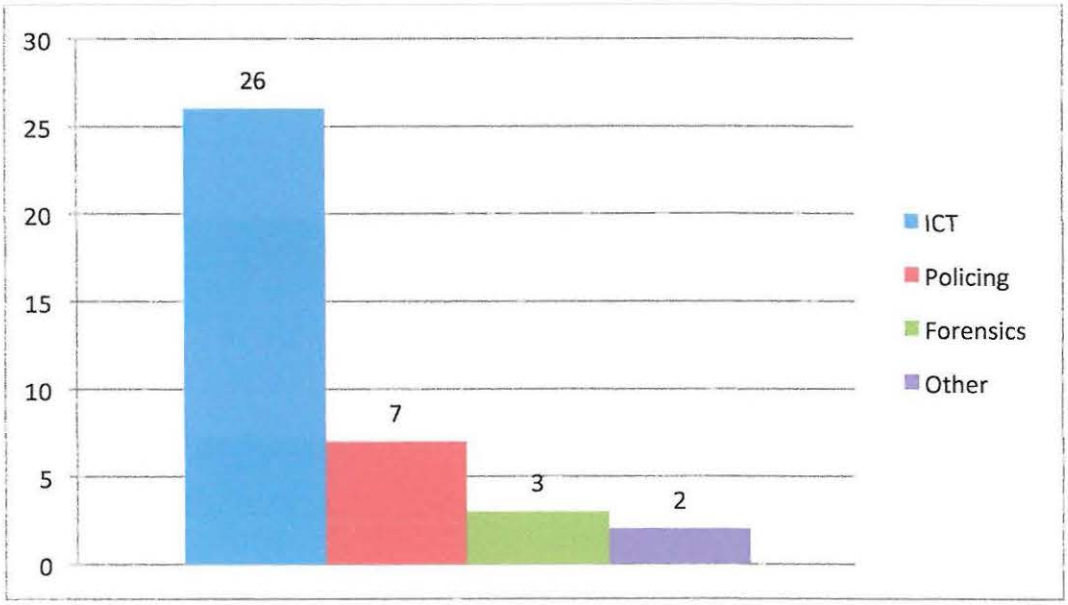


Figure 17 - Undergraduate Qualifications by Category

It should be noted that a few respondents had more than one undergraduate qualification and these are shown separately in Figure 17. 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. As shown in Figure 18, 23 respondents (41% of the sample) had no undergraduate qualifications, nine respondents (16% of the sample) had an undergraduate qualification not recommended for digital forensics, and 24 respondents (43% of the sample) 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.

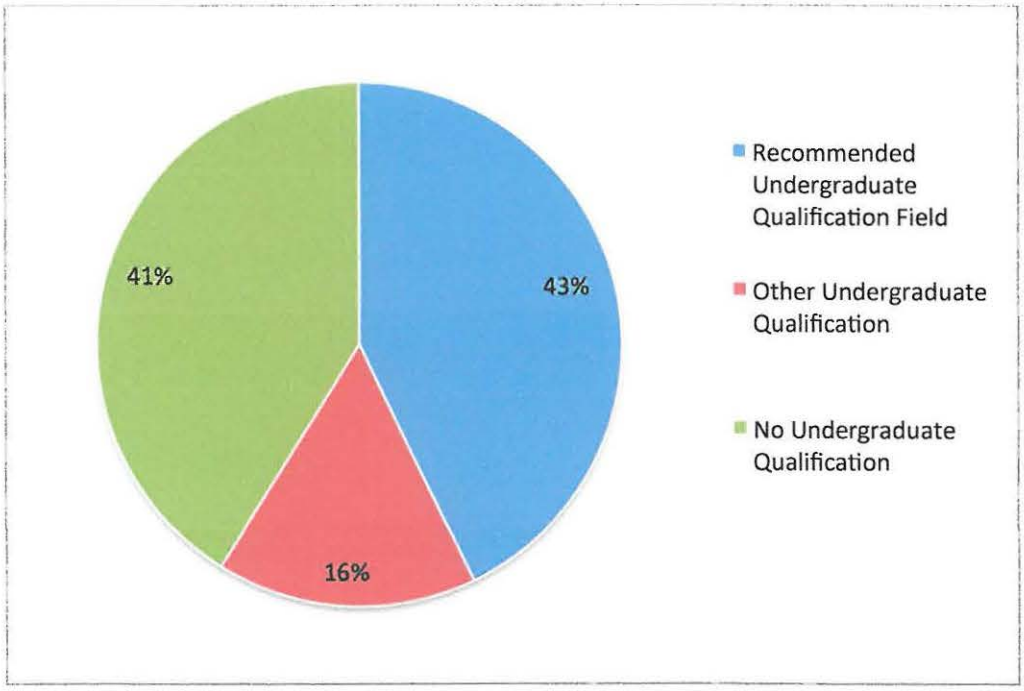


Figure 18 - Undergraduate Qualification Breakdown by Recommended Field

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 (Brennan, 2013).

5.2.3. Postgraduate Education

Sixteen respondents had completed a postgraduate degree or diploma (29% of the sample), while 40 respondents had not completed a postgraduate degree or diploma (71% of the sample). The percentages are illustrated in Figure 19.

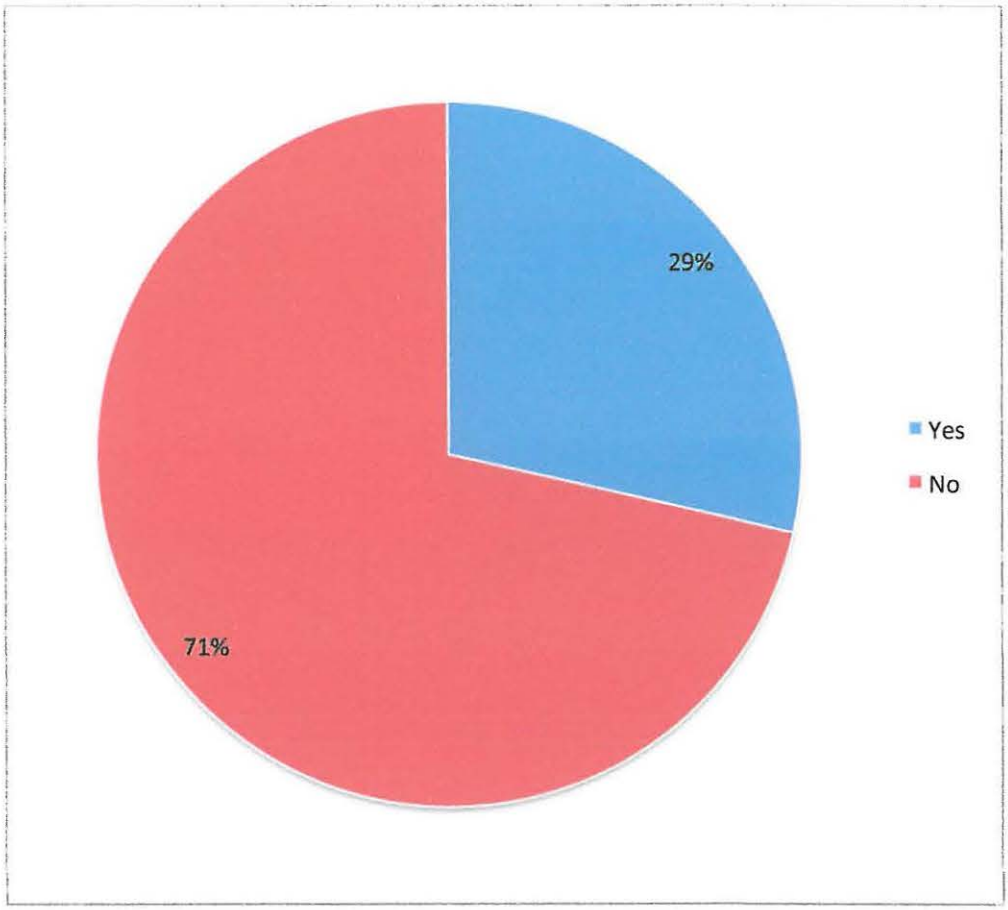


Figure 19 - Postgraduate Qualifications

A breakdown of the postgraduate qualifications is given in Table 11.

Table 11 - 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 20.

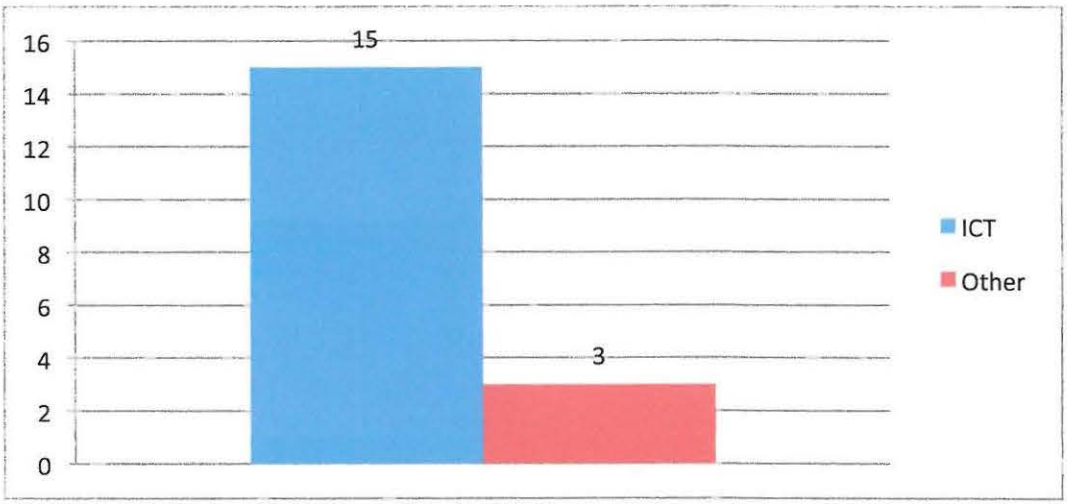


Figure 20- Postgraduate Qualifications by Category

Note that one respondent had more than one postgraduate qualification. Next we grouped the respondents 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 21, 40 respondents (72% of the sample) have no postgraduate qualifications, three respondents (5% of the sample) has a postgraduate qualification that is not recommended for digital forensics, and 13 respondents (23% of the sample) have a postgraduate degree that is at least in the subject areas recommended for the practice of digital forensics.

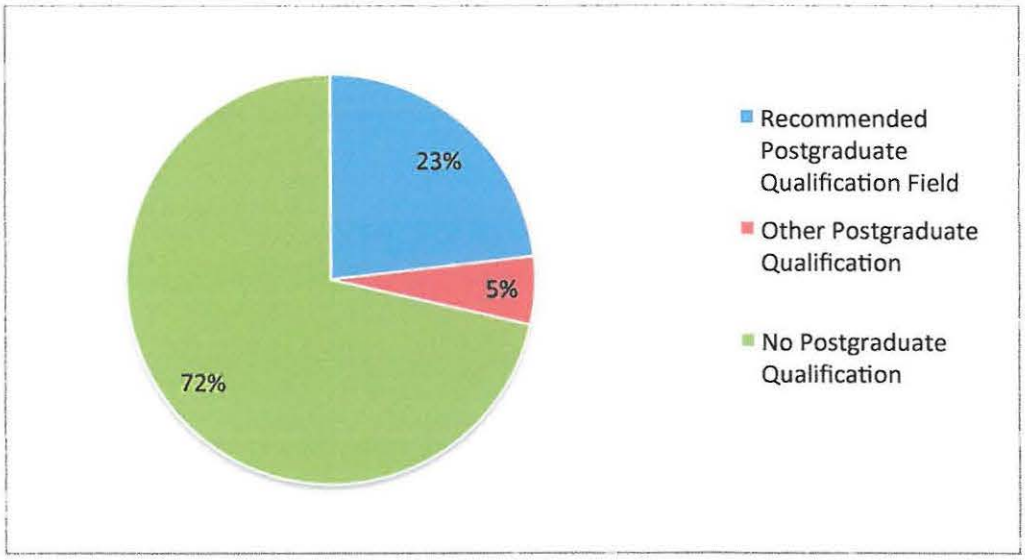


Figure 21 - Postgraduate Qualification Breakdown by Recommended Field

In South Africa, three tertiary academic institutions currently offer postgraduate taught modules in digital forensics. UP offers an Honours level module in Digital Forensics and Investigations as part of the BScHons Computer Science program (University of Pretoria, 2013), the University of Johannesburg offers and Honours level module in Computer Forensics as part of the BScHons Computer Science Program (University of Johannesburg 2013), 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 (University of Cape Town, 2013).

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 UCT, and one had completed the Digital Forensics and Investigations module at UP.

The prerequisites for registration for UCT 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[4] 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 (University of Cape Town, 2013).

[4] 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.

The prerequisites for registration for the UP course are a BSc degree in Computer Science (or equivalent) with an average of 60% in all of the third-year computer science modules (University of Pretoria, 2013).

Figure 22 shows the previous academic qualifications of those respondents who had completed the respective postgraduate degrees from either UCT or UP.

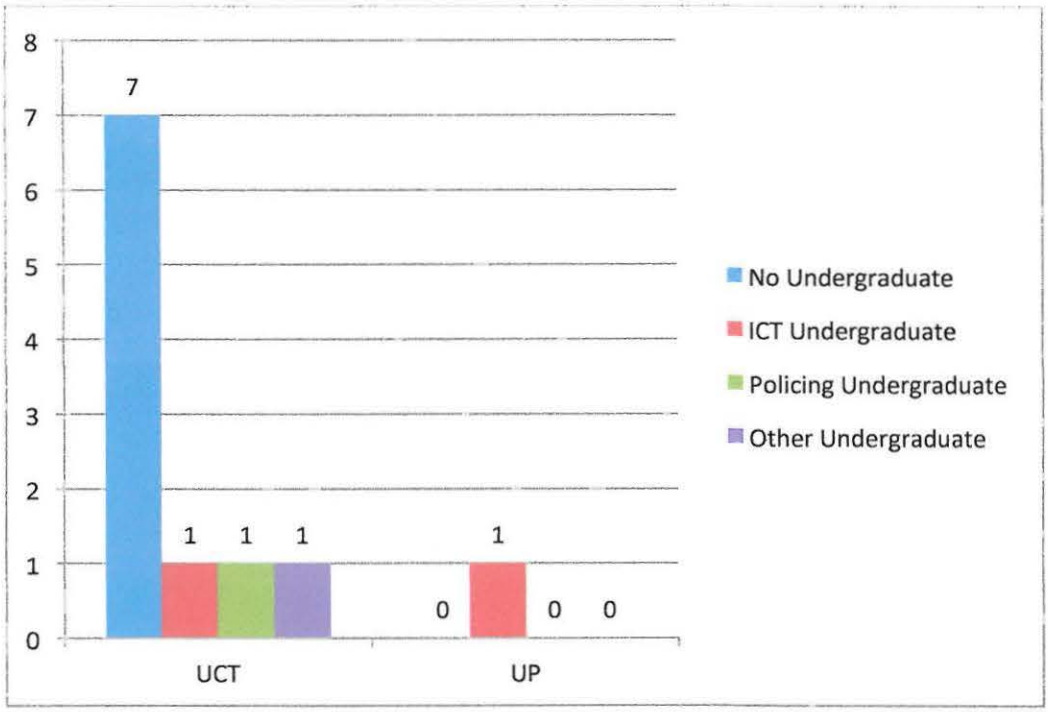


Figure 22 - UCT and UP Digital Forensics Graduates Undergraduate Profile

Nine of the respondents who obtained the UCT 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. 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.

5.3. DIGITAL FORENSIC EXPERIENCE

Four respondents had less than one year's experience as a digital forensic practitioner (7% of the sample), one respondent had between one and two years' experience as a digital forensic practitioner (2% of the sample), 17 respondents had between three and five years' experience as a digital forensic practitioner (30% of the sample), 17 respondents had between six and ten years' experience (30% of the sample), 15 respondents had between eleven and fifteen years' experience (27% of the sample), and two respondents had more than fifteen years' experience (4% of the sample). These percentages are illustrated in Figure 23.

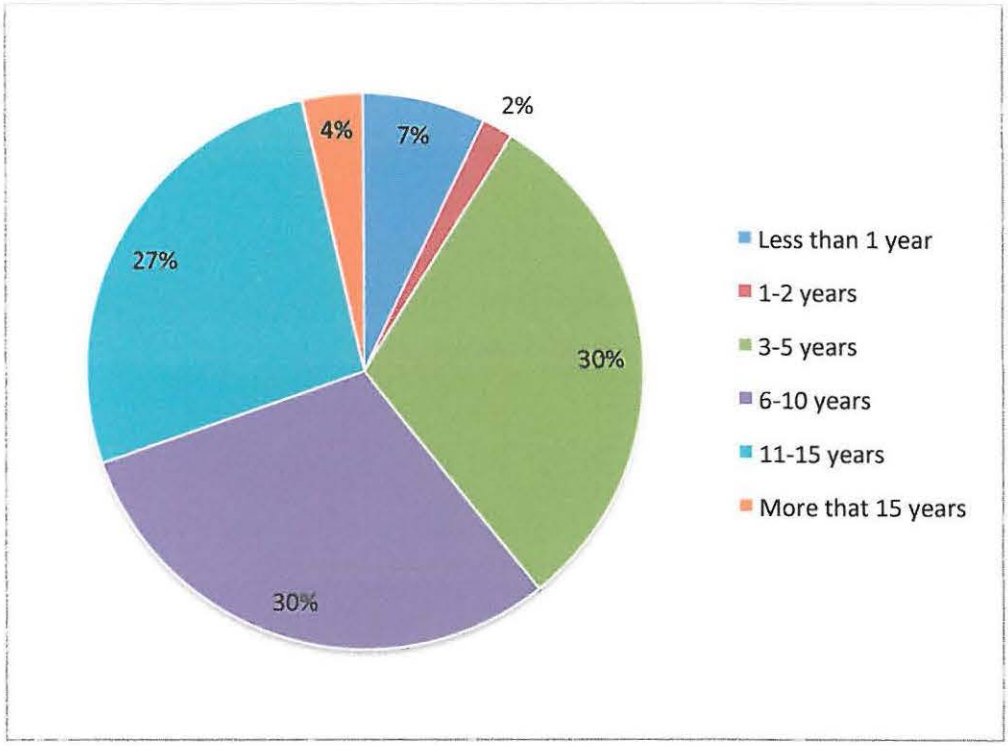


Figure 23 - Digital Forensics Experience

Twenty-three respondents had worked as digital forensic practitioners in a government law enforcement, intelligence, or military agency (41% of the sample); four respondents had worked in other government agencies (7% of the sample); 40 respondents had worked for private organisations that provided digital forensic services to other organisations (71% of the sample); and 13 respondents had worked for private organisations providing digital forensic services within their own organisations only (23% of the sample). This experience is illustrated in Figure 24.

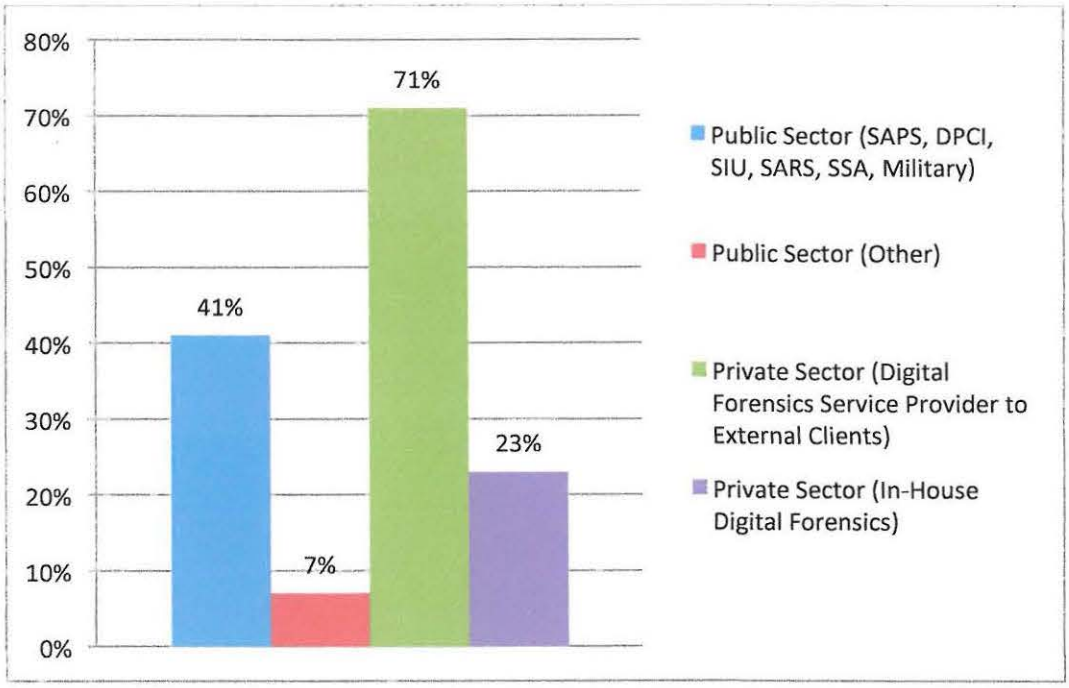


Figure 24 - Digital Forensics Experience per Sector

Twenty-five respondents had testified in a court of law in their capacity as digital forensic practitioners (45% of the sample), while 31 respondents had not testified in court (55% of the sample). The percentages are illustrated in Figure 25.

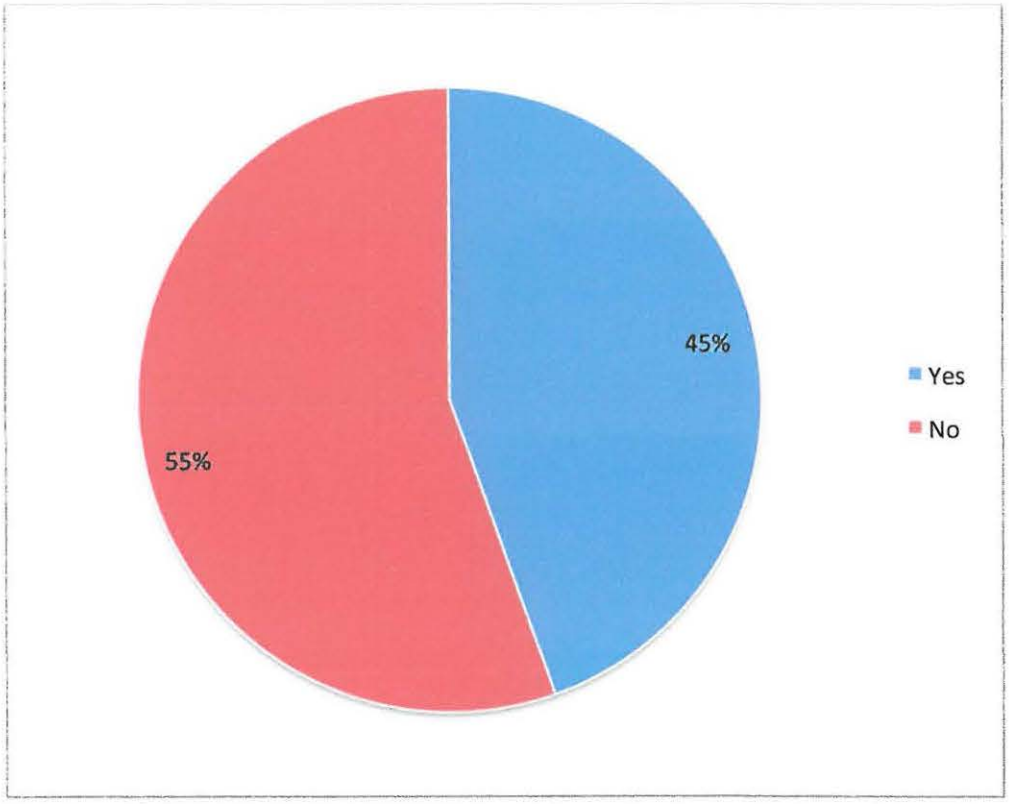


Figure 25 - Testified as Digital Forensic Practitioners in Court

The respondents that had stated that they had testified in court in their capacity as a digital forensic practitioner had testified in a variety of courts as illustrated in Figure 26.

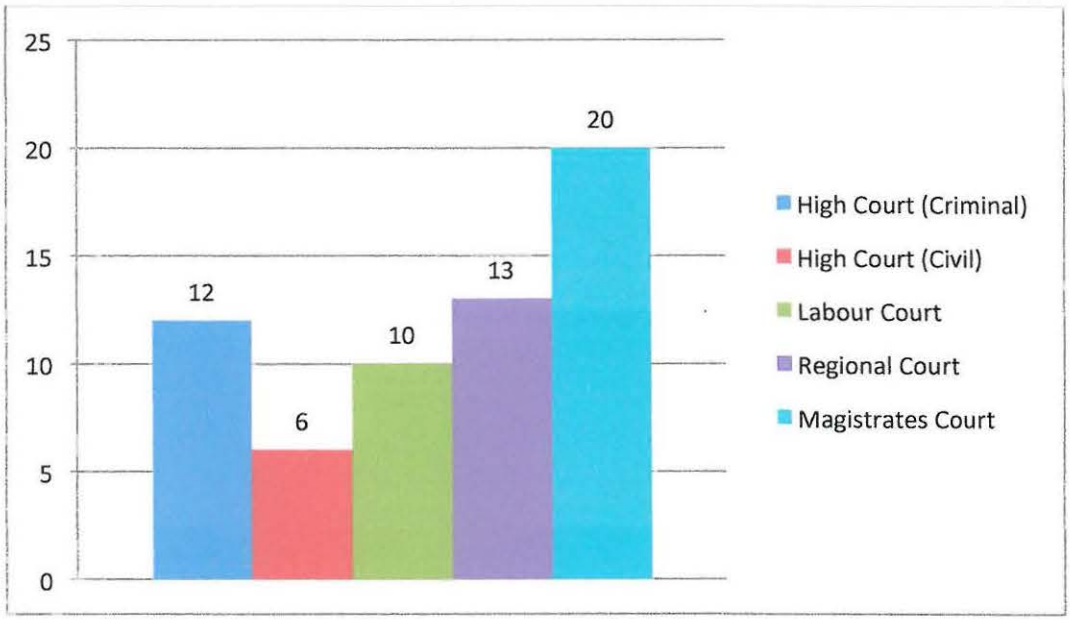


Figure 26 - Respondent Testifying Experience per Court

Only four of the respondents had been questioned during cross examination in court as to whether the forensic imaging software or hardware, or hardware or software write blockers had been tested or validated, whereas 21respondents had never been asked this during cross examination (see Figure 27).

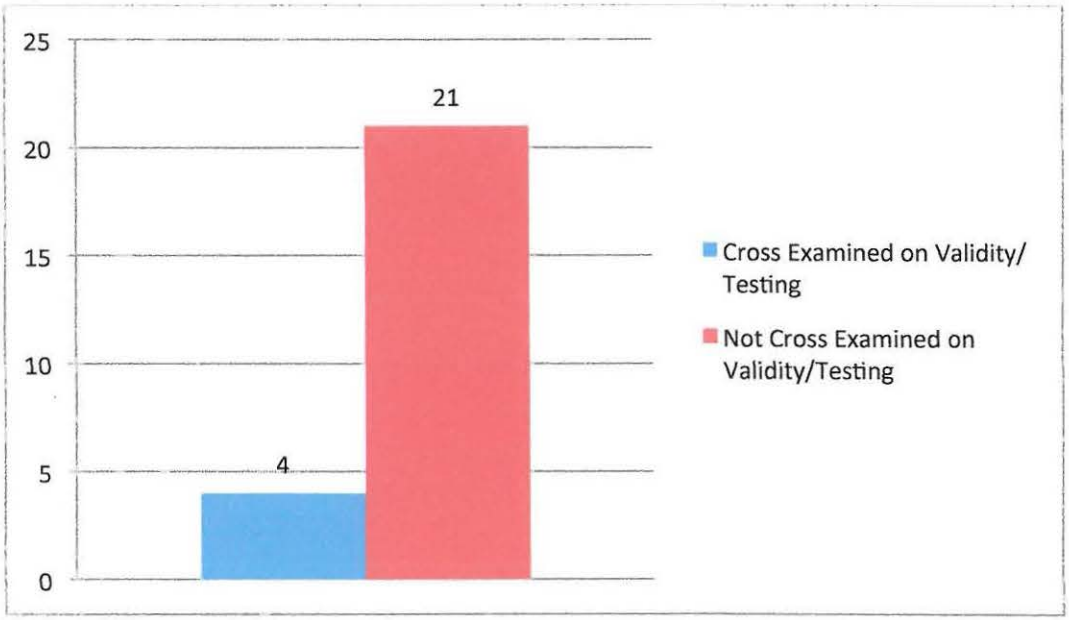


Figure 27 - Cross Examination about Validity

All of the four respondents who had been questioned as to whether the hardware or software they had used in the forensic acquisition process had been tested and validated as functioning correctly, stated that the hardware or software used had been tested.

All of these respondents had stated in the survey that they only make use of write blockers and forensic imaging tools that have been validated. Three respondents stated that they tested their own write blockers and forensic imaging tools, while one stated that the write blockers and forensic imaging tools were tested by others.

Only one of the respondents that tested their own write blockers made use of a method that was a valid write blocking testing method. All three of the respondents that tested their own forensic imaging tools made use of a valid testing method for forensic imaging. All three (3) of the respondents stated that they documented their write blocker and forensic imaging tool test.

The one respondent that stated that reliance was placed on write blockers and forensic imaging tools tested by others, confirmed that this was established as a result of validation documents prepared by an independent testing body and those prepared by the respective vendors.

None of these respondents had been asked to prove or verify their assertions in court that their tools had been validated, and no test documents or reports were submitted as evidence to verify their statements.

It can be argued that digital forensic science has its own intrinsic quality metric, namely, the evidence admitted into court and which stands up to vigorous cross examination (Jones & Valli, 2009). Quality assurance can, however, increase the likelihood that the evidence and the processes applied to it can successfully stand up to this vigorous cross examination. This is all good and well, but the key for this to be valid is that the digital forensic practitioners must in fact testify, and be subjected to vigorous cross examination in court.

Thirty-one respondents had not testified in court in their capacity as digital forensic practitioners and this is cause for concern as their findings and work were not subjected to the cross-examination process in court testing the credibility and reliability of their findings.

Considering that 21 respondents had testified, but never been cross examined about the validity of their write blocker or forensic imaging tools, the validity of write blockers and forensic imaging tools of 52 respondents (93% of the sample) had never been challenged in court, as illustrated in Figure 28.

This in itself is of significant concern, as these tools are a crucial component of preserving the digital evidence that is used in court. If the reliability of these tools is not challenged, there is a risk that digital evidence that should not be considered legally reliable may be relied upon in court, which could unfairly prejudice one side in the legal proceedings. In the experience of the researcher, in cases such as exceeding the speed limit when driving, or driving under the influence of alcohol, it is routine in court for the validity of the tools used to collect the evidence to be tested through cross-examination. Thus, it is concerning that the same principle is not being followed with regard to the forensic acquisition of digital evidence.

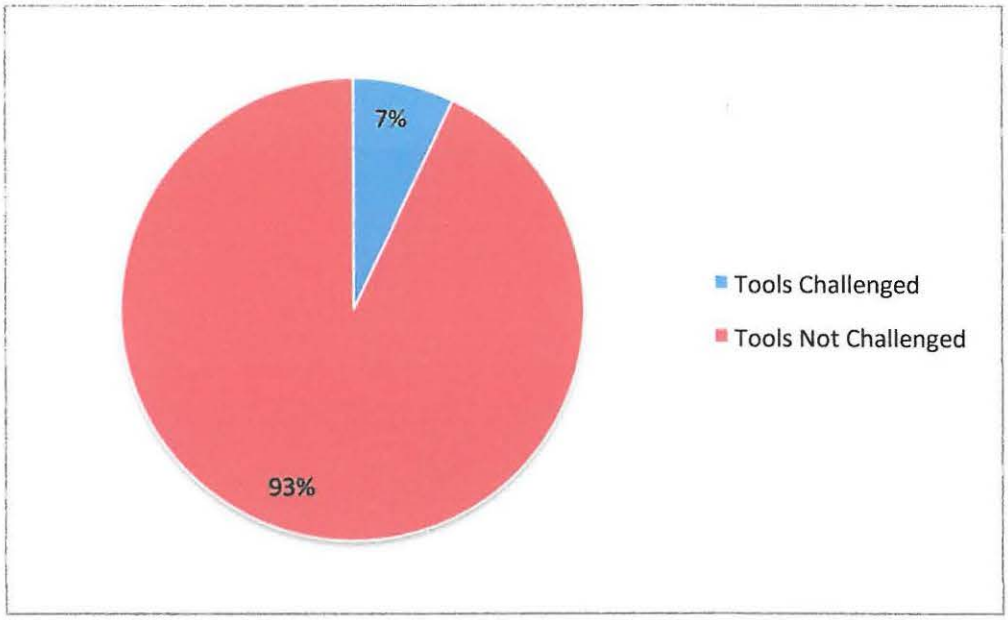


Figure 28 - Validity of Tools Challenged in Court

It is, however, also concerning that while seven percent of the sample was questioned about the validity of their tools in court, none was actually asked to provide proof of this. In the experience of the researcher where speed cameras and breathalysers are used to obtain evidence for use in court, it is routine for the calibration certificates or other validation documents to be submitted to the court to prove that the results obtained were in fact valid due to the tools working correctly. It is concerning that the same is not done for digital evidence.

Based on an examination of the data, it is suggested that testifying in court is not currently an effective method for determining whether write blockers or forensic imaging tools have been validated. However, further research is needed to determine why legal practitioners are not challenging or testing the validity of the tools used in digital forensics, while they routinely do so in more common forensic disciplines.

5.4. 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 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 (National Research Council, 2009).

Forty respondents had received some form of formal digital forensics training (71% of the sample), while 16 respondents had not received any formal digital forensics training (29% of the sample). The percentages are illustrated in Figure 29.

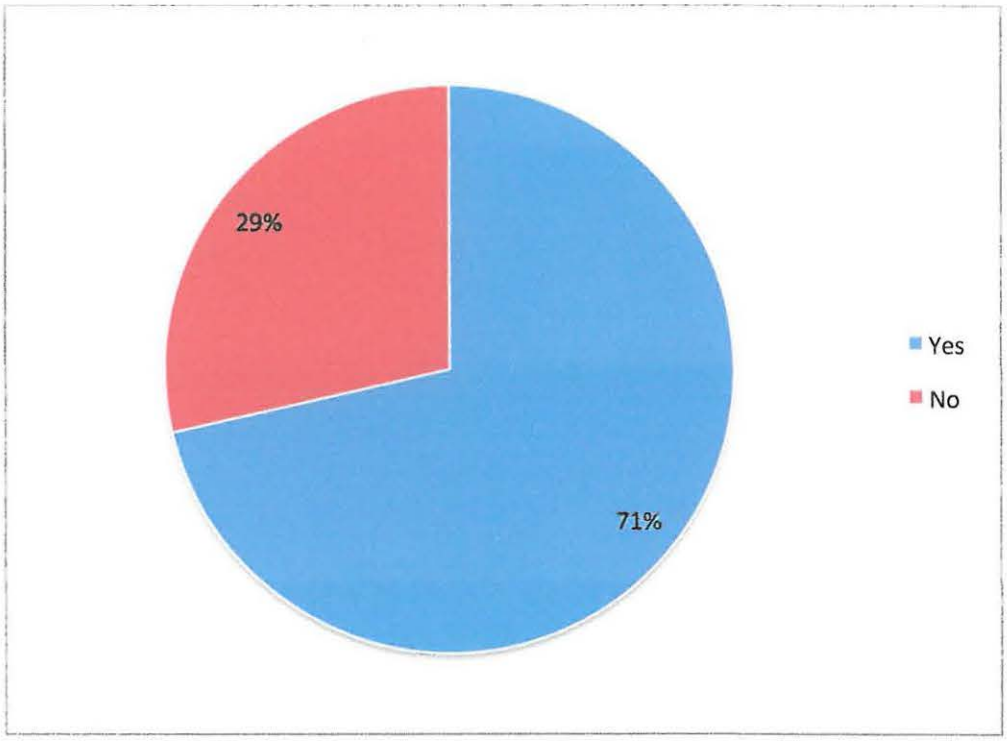


Figure 29 - Formal Digital Forensics Training

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 30, which clearly shows the dominance of vendor training in the sample.

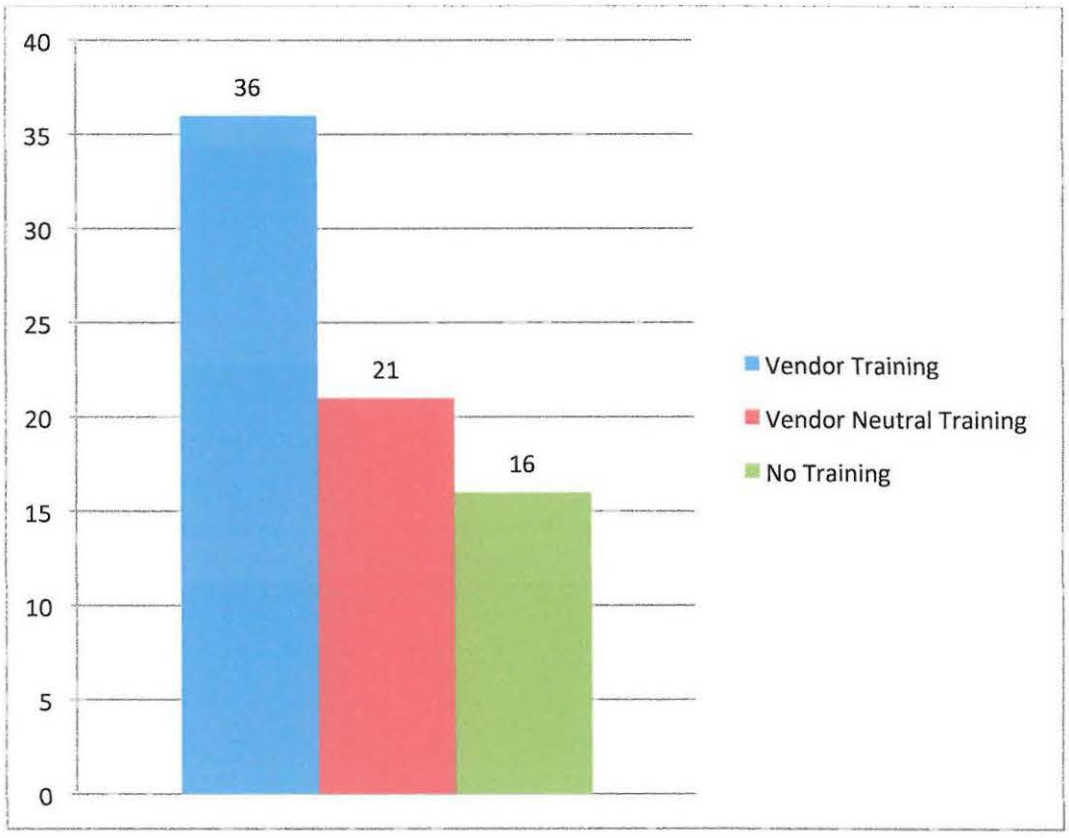


Figure 30 - Types of Training

The specific vendor courses that members of the sample had attended, and how many had attended each course are reflected in Table 12.

Table 12 - 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 (Philipp, Cowen, & Davis, 2010). 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 (Valli, 2006).

The specific vendor neutral courses that members of the sample had attended, and how many had attended each course are reflected in Table 13.

Table 13 - 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

5.5. VALIDATION TRAINING

Five respondents stated that they had received training on the importance of validation testing of the hardware and software used in the digital forensics process (9% of the sample), while 51 respondents had not (91% of the sample). The percentages are illustrated in Figure 31.

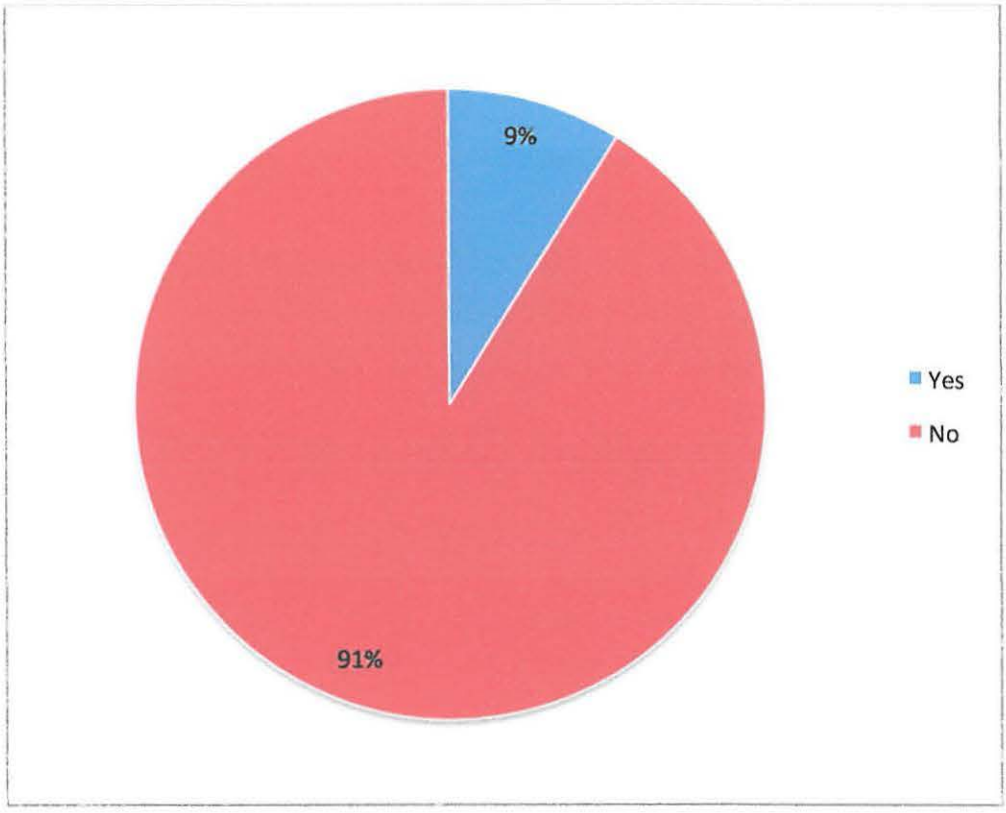


Figure 31 - Training on Importance of Validation

One respondent stated that the importance of validation testing was covered in the EnCase Computer Forensics I course, and that this covered the necessity for validation and various validation processes. Three respondents stated that the importance of validation testing was covered in the SANS408 Windows Forensics In-Depth course, and that this covered the importance of validating the tools used in digital forensics. One respondent stated that the importance of validation testing was covered in the FLETC Seized Computer Evidence Recovery Specialist course, and that this covered the necessity for validation and various validation processes, and how the results should be documented.

One respondent stated that he had received training in how to conduct validation testing of the hardware and software used in the digital forensic process (2% of the sample), while 55 respondents had not (98% of the sample). The percentages are illustrated in Figure 32.

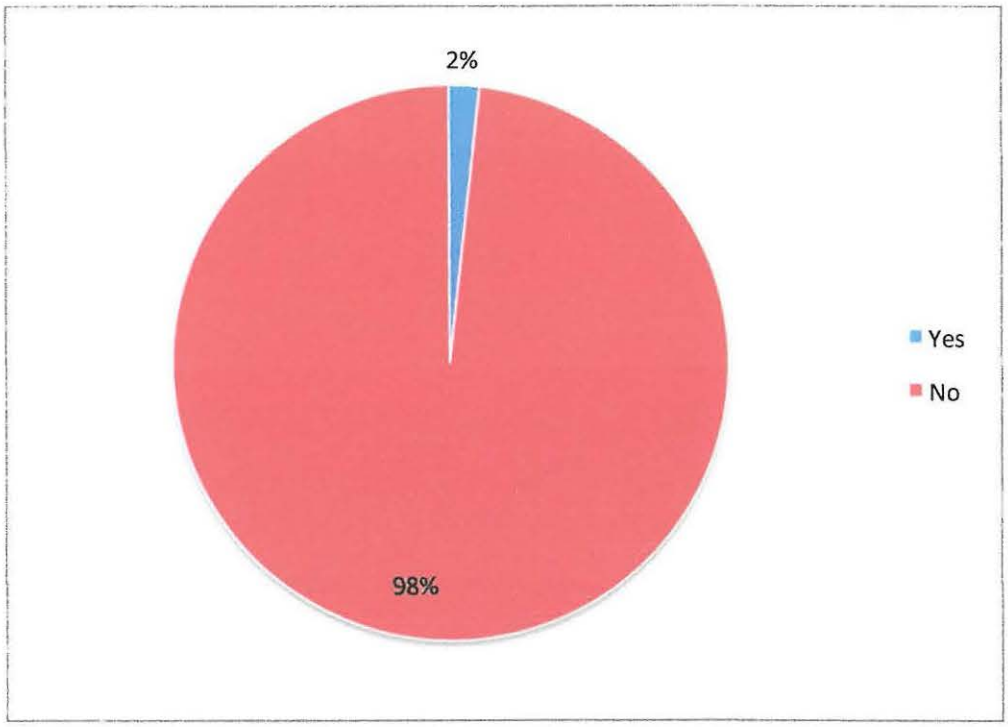


Figure 32 - Training on How to Conduct Validation Testing

The respondent who had received training in how to conduct validation testing had been taught this on the FLETC Seized Computer Evidence Recovery Specialist course, which taught validation methods that complied with the SWGDE standards.

The EnCase Computer Forensics I course syllabus does not specifically mention that it addresses the importance of validation testing[5], while the SANS408 Windows Forensics In-Depth course syllabus does address the importance of validation testing[6]. The FLETC Seized Computer Evidence Recovery Specialist course syllabus specifically addresses the importance of validation testing[7], as well as how to conduct this type of testing.

While three respondents stated correctly that they had received training in the importance of validation testing as part of the SANS408 Windows Forensics In-Depth course, 15 respondents stated that they had attended this course, meaning that 12 did not recall that the course covered the importance of validation testing.

What is of significant concern is that only one respondent had actually been formally trained to conduct validation testing, and that this respondent received the training in the United States of America.

5.6. KNOWLEDGE OF VALIDATION STANDARDS

The literature review identified three specific formal validation standards used in the field of digital forensics. The respondents were questioned to determine how they rated their knowledge of these standards. The responses are illustrated in Figure 33.

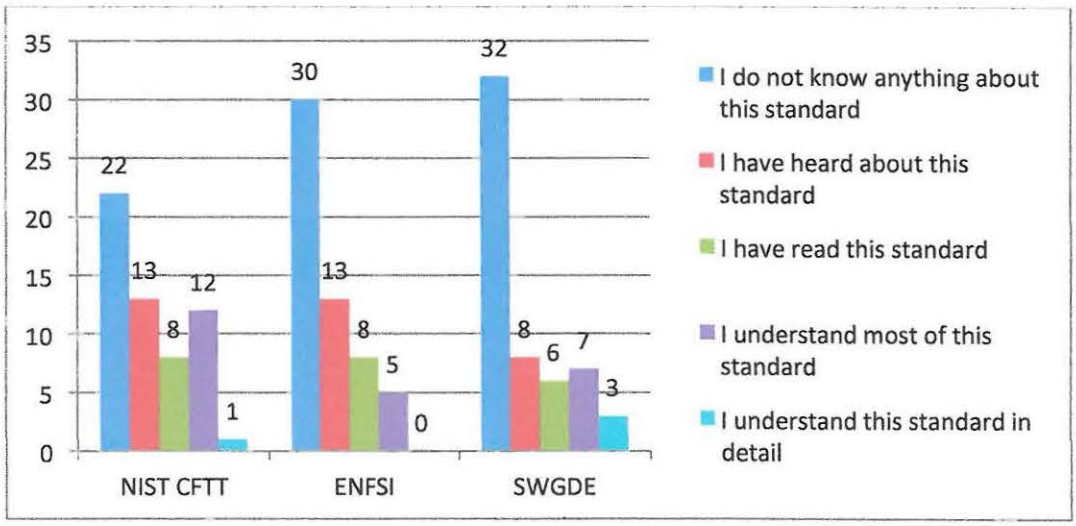


Figure 33 - Knowledge of Validation Standards

[5] http://www.guidancesoftware.com/resources/Documents/Doc-Library-PDFs/EnCase_CF1_v7_Syllabus.pdf
[6] http://digital-forensics.sans.org/training/course/computer-forensic-investigations-windows-in-depth
[7] http://www.fletc.gov/training/programs/technical-operations-division/seized-computer-evidence-recovery-specialist-scers/

The graph suggests that the majority of the respondents are not in a position to apply these formal validation standards used in the field of digital forensics, as very few understand the various standards, either generally or in detail.

5.7. HARDWARE AND SOFTWARE USED IN THE FORENSIC ACQUISITION PROCESS

The respondents made use of various write blocker and forensic imaging tools, and in most instances made use of more than one type of tool.

The write blocking tools used by the respondents are indicated in Figure 34, which suggests that the most common write blockers are the Tableau Hardware Write Blockers[8], followed by the use of Linux based software write blocker environments such as Helix[9] and Raptor[10].

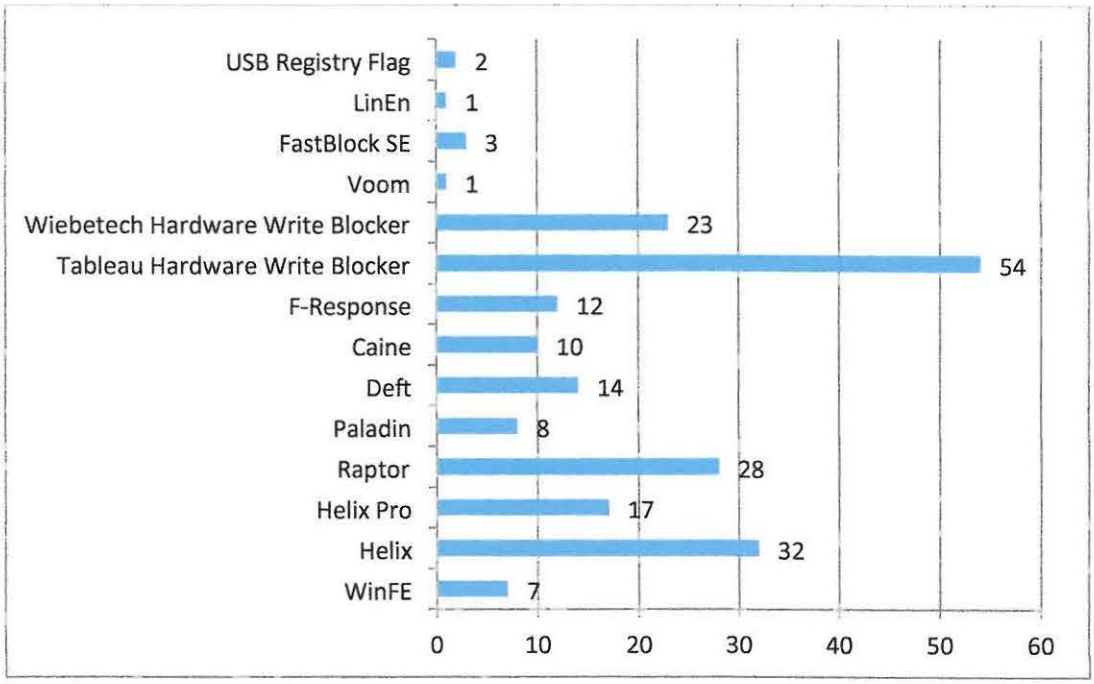


Figure 34 - Write Blocking Tools Used

The imaging tools used by the respondents are indicated in Figure 35, which suggests that the most common forensic imaging tools are FTK Imager[11], followed by EnCase Imager[12], and then various hardware imaging tools.

[8] https://www.guidancesoftware.com/products/Pages/tableau/overview.aspx
[9] http://www.e-fense.com/products.php
[10] https://www.forensicsandediscovery.com/Pages/Raptor.aspx
[11] http://accessdata.com/product-download
[12] https://www.guidancesoftware.com/products/Pages/Product-Forms/Forensic-Imager-download.aspx

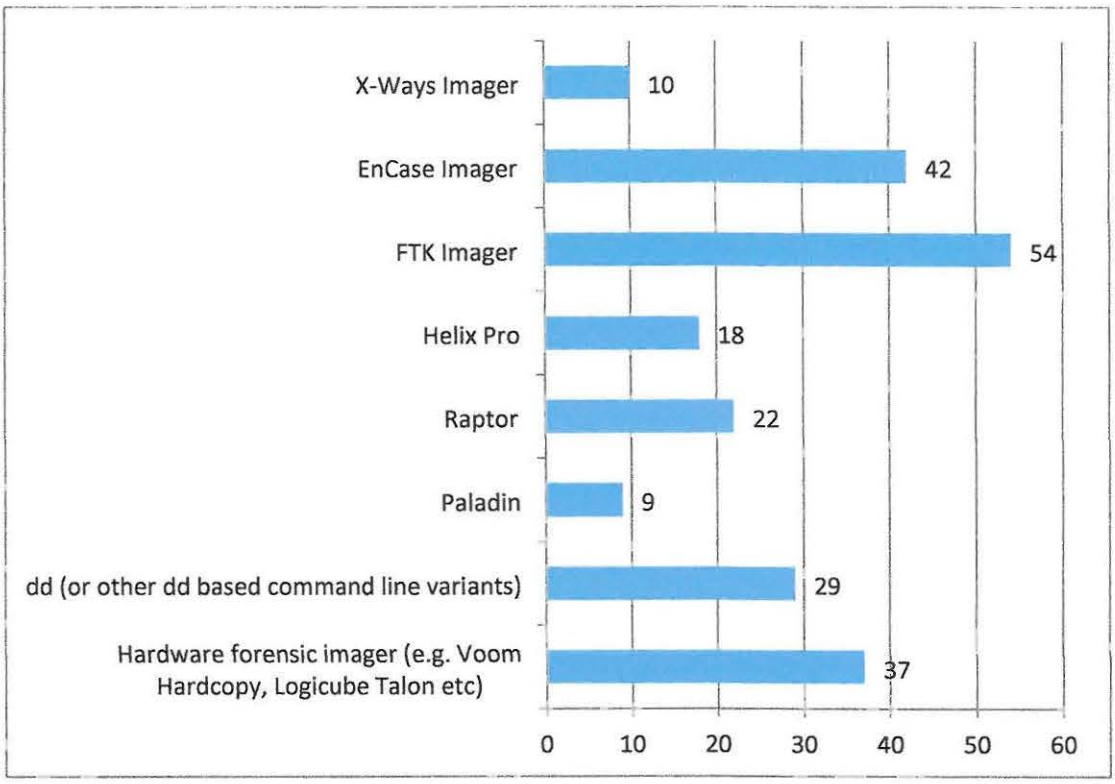


Figure 35 - Forensic Imaging Tools Used

5.8. THE USE AND VALIDATION OF WRITE BLOCKERS

Forty-two respondents stated that they only made use of write blockers that had been validated as working correctly (75% of the sample), while 14 did not always use write blockers that had been validated as working correctly (25% of the sample). The percentages are illustrated in Figure 36.

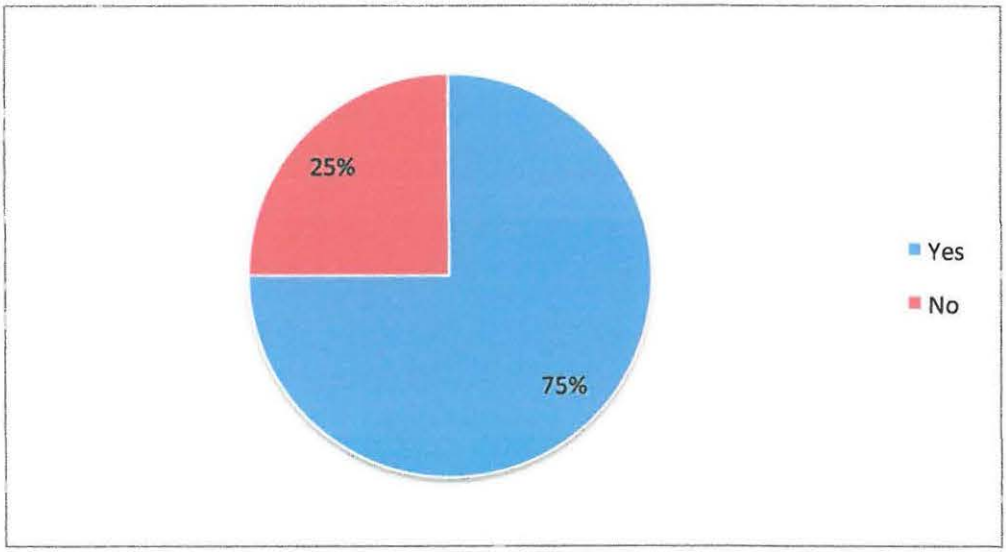


Figure 36 - Use of Validated Write Blockers only

Eighteen respondents stated that they conducted validation tests of the write blockers they used. Twenty-four respondents did not conduct the validation tests themselves, but relied on other methods to establish that the write blockers they used were validated. These figures, as well as the number of respondents that did not make use of validated write blockers are illustrated in Figure 37.

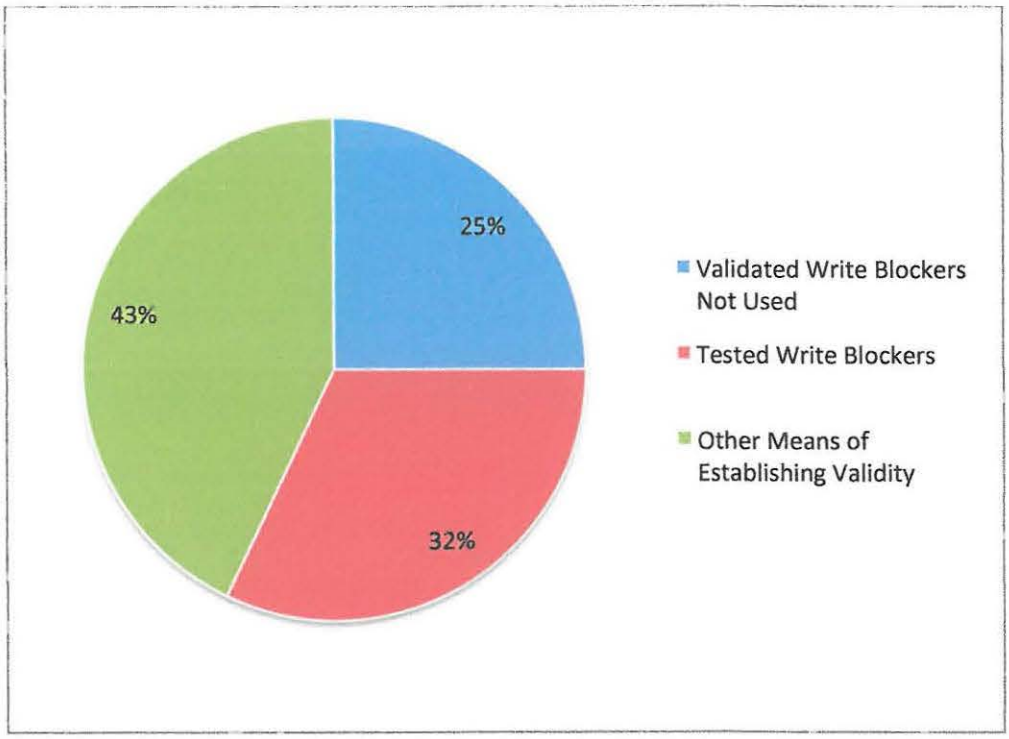


Figure 37 - Ensuring Write Blocker Validity

5.8.1. Using Write Blockers That Had Not Been Validated

The 14 respondents who did not always make use of validated write blockers gave a variety of reasons for not doing so:

- There was no compelling case law or legislation that required them to only use validated write blockers.
- They had never been challenged in court on this matter, and that until they had been, they would not worry about it.
- They did not have the time to validate write blockers.
- There was no protocol in place in their work environment compelling them to use validated write blockers.
- They were not trained in how to validate write blockers.
- They were not aware of the necessity of using validated write blockers.

The reasons provided by the respondents are quantified in Figure 38.

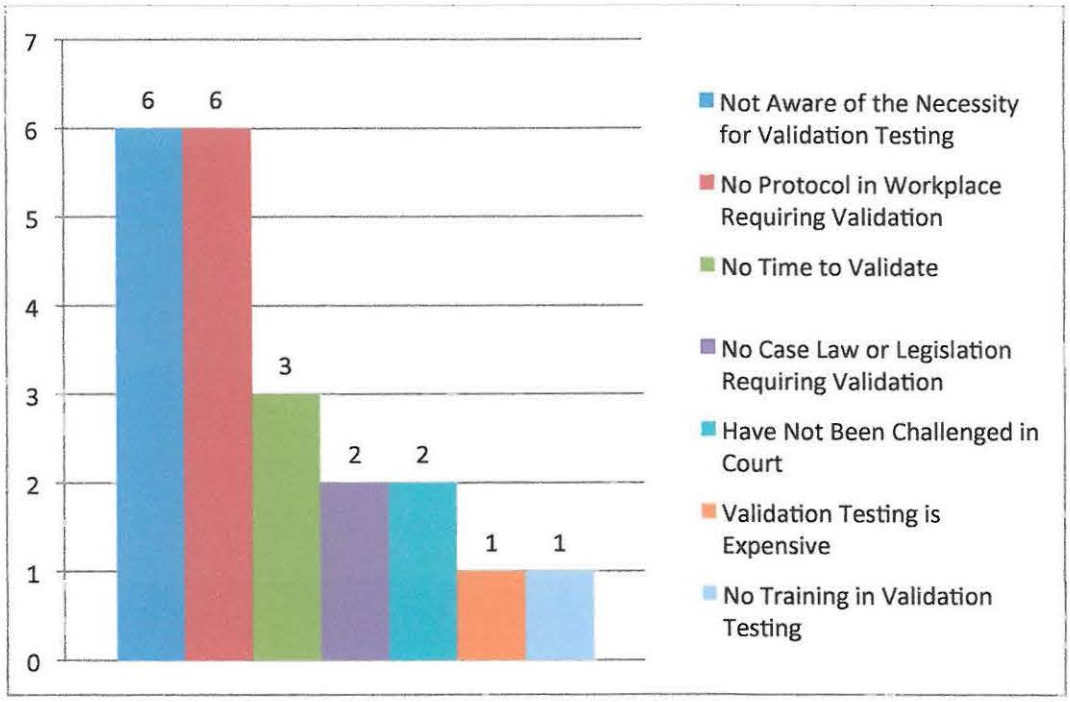


Figure 38 - Reasons for Not Using Validated Write Blockers

One of these respondents who stated that he did not always use validated write blockers had received training in the importance of using validated tools on the SANS408 Windows Forensics In-Depth course. His specific reasons for not using validated write blockers was simply that he did not have time to test his write blockers as well as that he had never yet been challenged on this in court.

Seven of the respondents had attended vendor training courses, and three of these had also completed the course in computer forensics at UCT. Seven of the respondents had received no formal digital forensics training, but one had completed the course in computer forensics at UCT.

Five of these respondents had experience testifying in court as digital forensic practitioners, but none had ever been cross examined about the use of validated tools.

5.8.2. Ensuring That Write Blockers Used Are Validated

The 24 respondents who only used validated write blockers, although they did not test them themselves, gave the following reasons why they were satisfied that the write blockers they used were in fact validated:

- There was a validation document for the write blocker that had been prepared by another member of the laboratory who had validated the write blocker.
- There was a validation document for the write blocker that had been prepared by an independent testing body.
- There was a validation document for the write blocker that had been prepared by a university or other research institution.
- There was a validation document for the write blocker from the vendor of the write blocker.

The reasons provided by the respondents are quantified in Figure 39.

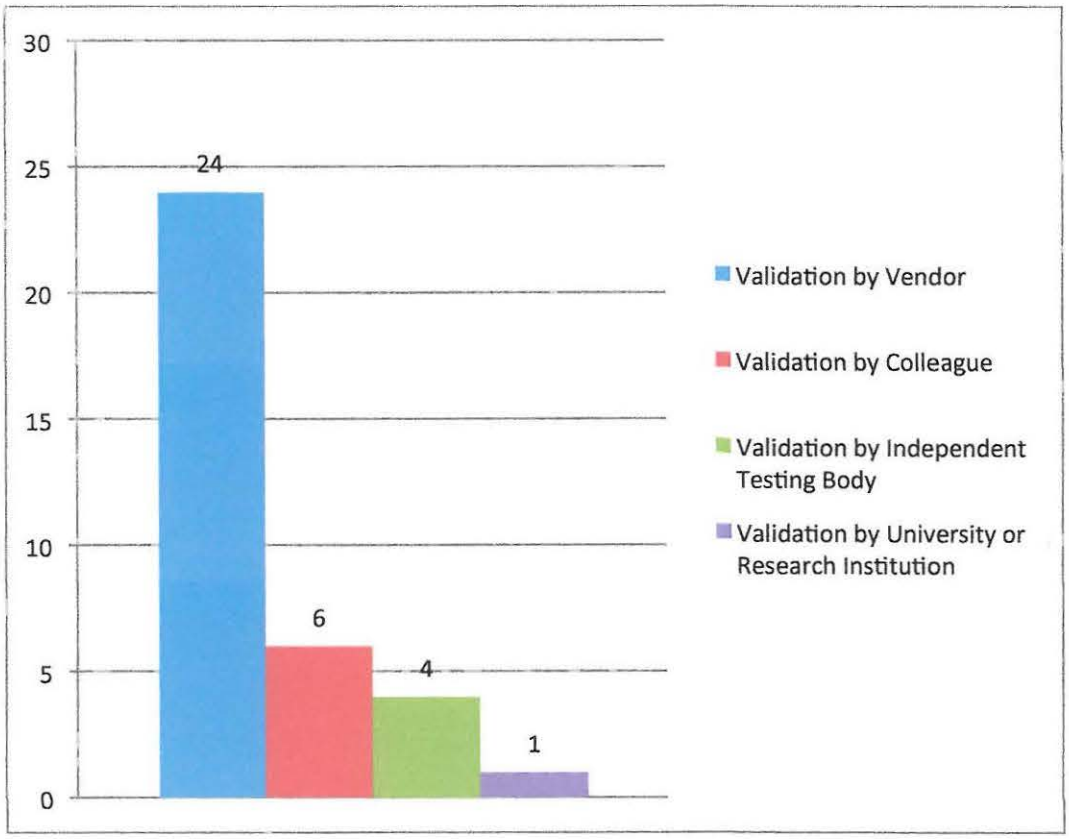


Figure 39 - How Validation Was Done (Write Blockers)

Twenty-four respondents relied on the belief that the various write blockers that they stated they used had in fact been validated by the vendors themselves, although one of these twenty-four also relied on a colleague, and two of these twenty-four also relied on validations conducted by an independent testing body. Fifteen of these respondents only relied on the belief that the vendors of the various write blockers that they stated they used had in fact been validated by the vendors themselves.

Six respondents stated that they used write blocker tools that had been validated by an independent testing body. All of the write blocking tools that were used by these respondents were identified, and a comprehensive search was conducted on the Internet to attempt to identify if any of these tools had in fact been independently validated as stated by the respondents. The results of this are illustrated in Table 14.

Table 14- Independent Validation Testing (Write Blockers)

Write Blocking Tool	Type	Independent Validation Testing
Tableau Hardware Write Blocker	Proprietary, Commercial	Yes[13]
Helix	Open source	No
Raptor	Proprietary, Freeware (Based on open source)	No
Wiebetech Hardware Write Blocker	Proprietary, Commercial	Yes[14]
Helix Pro	Proprietary, Commercial (Based on open source)	No
Deft	Open source	No
Caine	Open source	No
FastBlock SE	Proprietary, Commercial	No

Only two of the write blocker tools that were used could be confirmed to have been independently validated, and as such the belief by the respondents that the tools they used were validated by an independent testing body is inaccurate.

Twenty-six of the respondents relied on the belief that the vendors of the various write blockers had validated the tools. All of the write blocking tools used by these respondents were identified, and a comprehensive search was conducted on the Internet to attempt to identify if any of these tools had in fact been vendor validated as stated by the respondents. The results of this investigation are illustrated in Table 15.

[13] http://www.nij.gov/pubs-sum/216981.htm
[14] http://www.nij.gov/pubs-sum/214063.htm

Table 15- Vendor Validation Testing (Write Blockers)

Write Blocking Tool	Type	Vendor Validation Testing
Tableau Hardware Write Blocker	Proprietary, Commercial	No[15]
Helix	Open source	No
Raptor	Proprietary, Freeware (Based on open source)	No
Wiebetech Hardware Write Blocker	Proprietary, Commercial	No
Helix Pro	Proprietary, Commercial (Based on open source)	No
Deft	Open source	No
Caine	Open source	No
FastBlock SE	Proprietary, Commercial	No
F-Response	Proprietary, Commercial	Yes[16]
Voom	Proprietary, Commercial	No
WinFE	Proprietary, Freeware	No
Paladin	Proprietary, Freeware (Based on open source)	No
LinEn	Proprietary, Commercial	No
USB Registry Flag	Proprietary, Commercial	No

Eleven of the respondents had attended vendor neutral training courses, 14 had attended vendor training courses, and four of these had also completed the course in computer forensics at UCT. Seven of the respondents had received no formal digital forensics training, but one had completed the course in computer forensics at UCT.

Nine of these respondents had experience testifying in court as digital forensic practitioners, but only two of the respondents had been cross examined about the use of validated tools.

[15] While the vendor does not report their own test results, they have posted a link to the NIST CFTT validation test reports on their website.

[16] https://www.f-response.com/assets/pdfs/F-ResponseValidationTestingReportApril2009-Final2.0.pdf

5.8.3. Validating Write Blockers

Eighteen of the respondents stated that they conducted validation tests of the write blockers they used. These respondents were then asked when they conducted their validation tests; their responses are quantified in Figure 40.

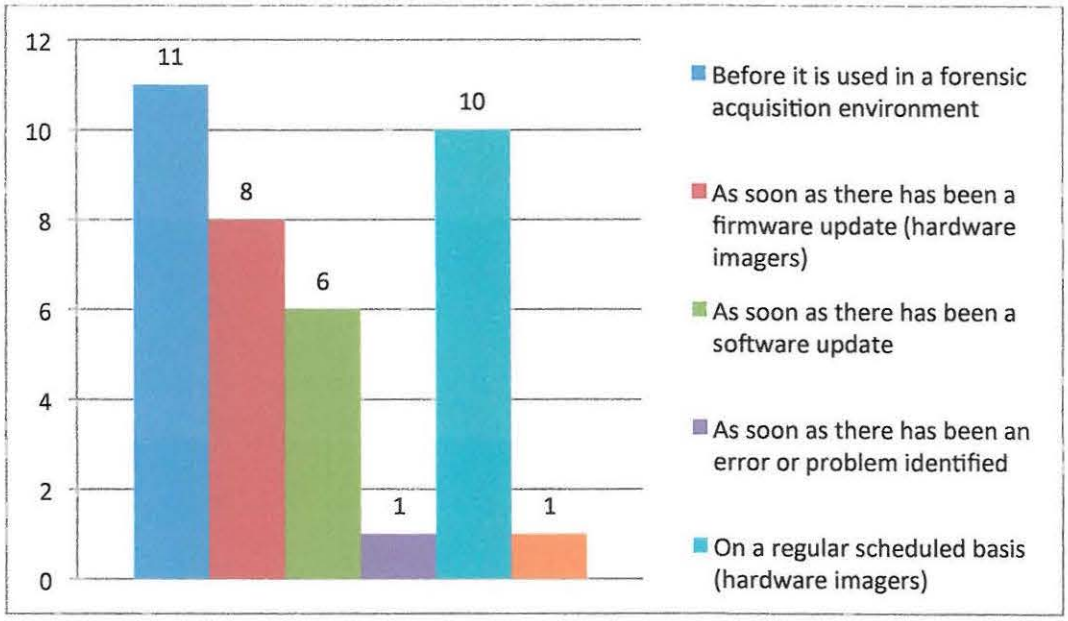


Figure 40 - When Write Blockers are Validated

Only 11 of these respondents stated that they conducted validation testing before a particular write blocker was used to acquire digital evidence for the first time by them. All 18 of these respondents stated that they used software based write blockers, however only six of them stated that they conducted validation tests after a software update had been made. Three of the respondents stated that they tested only hardware based write blockers, despite the fact that they stated that they also used software based write blockers.

Thirteen of these respondents stated that they did not conduct their validation tests in terms of any established validation standard, while five stated that they did. The standards that they stated they complied with are illustrated in Figure 41.

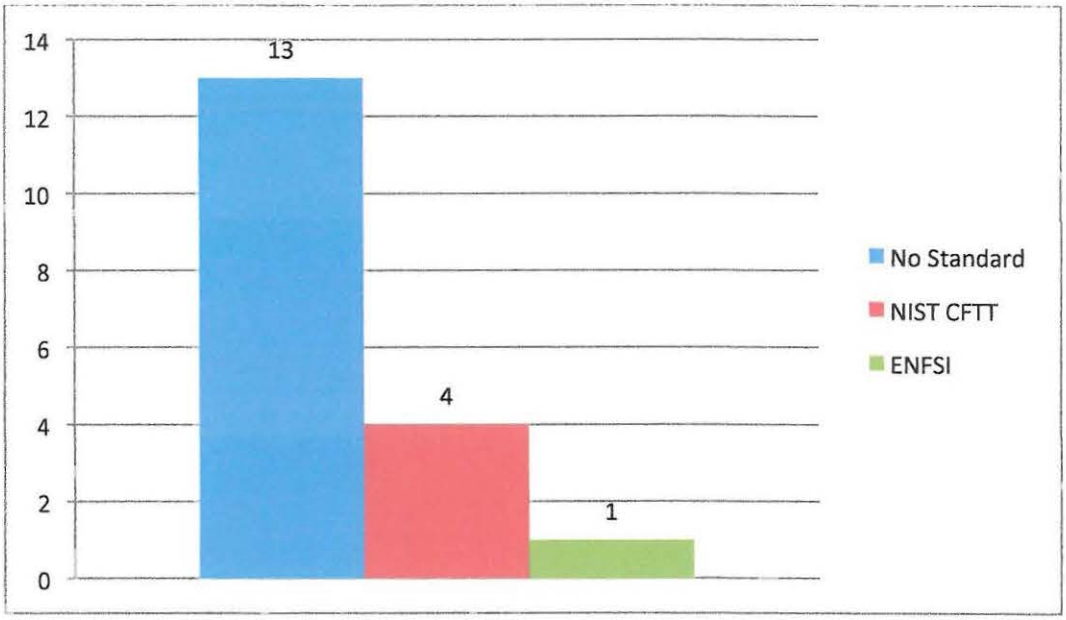


Figure 41 - Formal Standards Used for Validating Write Blockers

The four respondents who stated that they conducted their validation testing in terms of the NIST CFTT standard described their testing methodology. Three of them stated that they tried to deliberately write data to a drive connected a write blocker, which is partially compliant with the NIST CFTT standard, but one simply stated that he just hashed the drive before and after using a write blocker to determine whether any data was altered on the drive, which is not compliant with the NIST CFTT standard. The one respondent who stated that he conducted his validation testing in terms of the ENFSI standard described his testing methodology as simply trying to deliberately write data to a drive connected a write blocker, which is only partially compliant with the ENFSI standard.

The 13 respondents that stated that they did not use an existing validation standard were also asked to describe their methodologies used. Two specific methodologies were identified. Eight of these respondents simply tried to write data to the media while it was connected to a write blocker. The remaining five respondents simply calculated the hash value of the media before it was connected to a write blocker, imaged the media, and then recalculated the hash of the media to determine whether it had changed. Both these methods, while not necessarily scientifically robust, do at least provide a certain level of assurance in the tool functionality.

Eleven of the respondents who stated that they validated their write blockers stated that they documented their validation tests, while seven stated that they did not, as illustrated in Figure 42. It is however concerning that seven respondents did not document their tests, meaning that there was no evidence that they could produce in court if asked to do so, to prove that they had actually conducted validation tests.

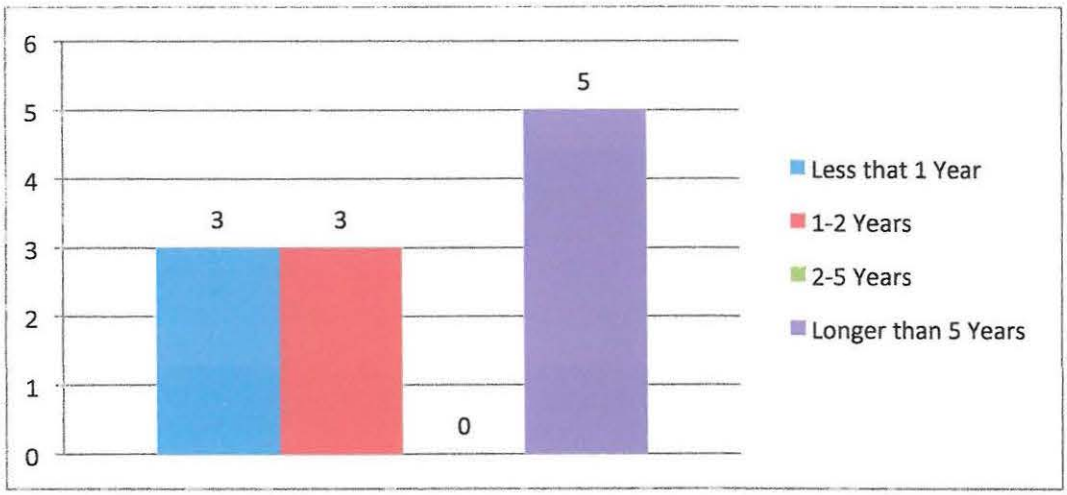


Figure 42 - Validation Test Documentation Retention (Write Blockers)

Only one respondent stated that he had been trained in how to conduct a validation test, and this was training received in the United States on the Seized Computer Evidence Recovery Specialist course.

Nine of these respondents had attended vendor neutral training courses, 15 had attended vendor training courses, while three had also completed the course in computer forensics at UCT and one had completed the computer forensics course at UP. Two of the respondents had received no formal digital forensics training.

Eleven of these respondents had experience testifying in court as digital forensic practitioners, but only three of the respondents had been cross examined about the use of validated tools.

5.9. THE USE AND VALIDATION OF FORENSIC IMAGING TOOLS

Forensic imaging tools, whether or not they are hardware based tools, software based tools, or a combination of both, are crucial tools for making a forensically sound image of evidential data, and preserving it for examination and analysis, and finally presentation in court.

Forty-seven respondents stated that they only made use of forensic imaging hardware or software that had been validated as working correctly (84% of the sample), while nine respondents did not always use forensic imaging hardware or software that had been validated as working correctly (16% of the sample). The percentages are illustrated in the Figure 43.

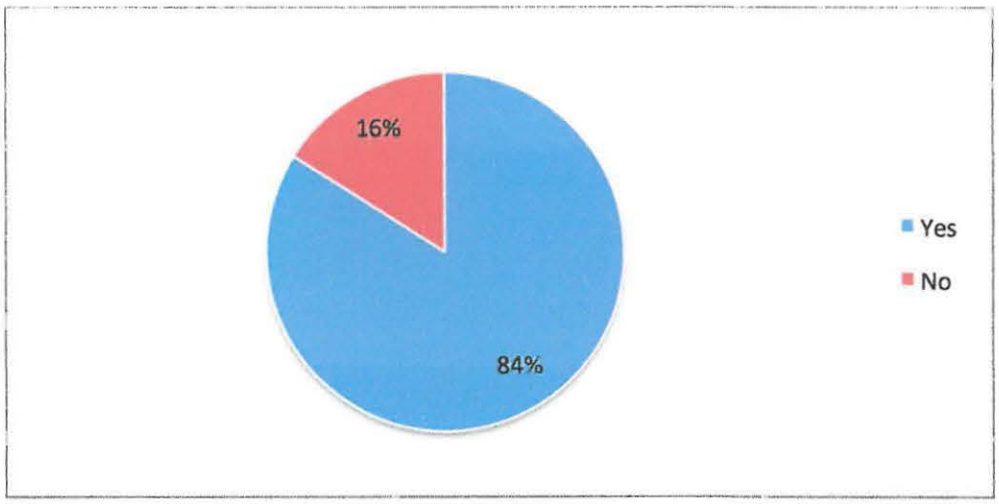


Figure 43 - Only Use Validated Forensic Imaging Hardware or Software

Sixteen respondents stated that they conducted validation tests of the forensic imaging software or hardware they used, while (31 respondents did not conduct the validation tests themselves, but relied on other methods to establish that the forensic imaging software or hardware they used was validated. These figures as well as the number of respondents that did not make use of validated forensic imaging hardware or software are illustrated in Figure 44.

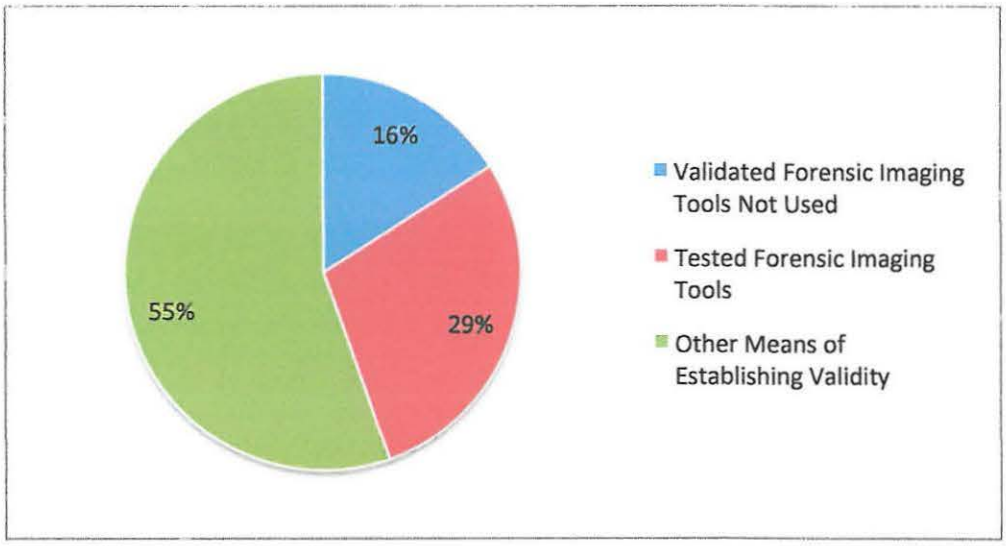


Figure 44 - Ensuring Forensic Imager Validation

5.9.1. Using Forensic Imaging Tools That Had Not Been Validated

The nine respondents who did not always make use of validated forensic imaging tools gave various reasons for this:

- They had never been challenged in court on this matter, and that until they had been, they would not worry about it.
- They did not have the time to validate forensic imaging tools.
- There was no protocol in place in their work environment compelling them to use validated forensic imaging tools.
- They were not aware of the necessity of using validated forensic imaging tools.

The reasons provided by the respondents are quantified in Figure 45.

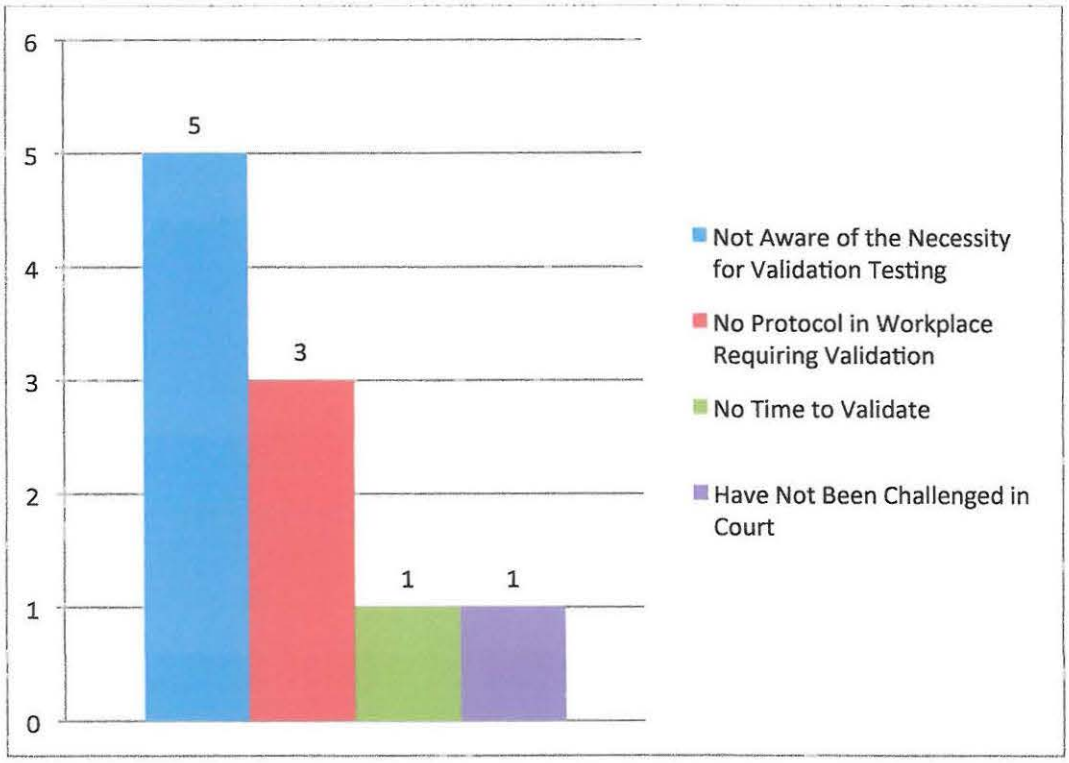


Figure 45 - Reasons for Not Using Validated Forensic Imaging Hardware or Software

One of the respondents who stated that he did not always use validated forensic imaging tools, had received training in the importance of using validated tools on the SANS408 Windows Forensics In-Depth course. His specific reasons for not using validated forensic imaging tools were simply that he did not have time to test his forensic imaging tools, as well as that he had never yet been challenged on this in court.

Three of these respondents had attended vendor training courses, and one of these had also completed the course in computer forensics at UCT. Six of these respondents had received no formal digital forensics training, but one had completed the course in computer forensics at UCT.

One of these respondents had experience testifying in court as a digital forensic practitioner, but had not been cross examined about the use of validated tools.

5.9.2. Ensuring That Forensic Imaging Tools Used Are Validated

The 31 respondents who only used validated forensic imaging tools, but did not test them themselves, gave the following reasons why they were satisfied that the forensic imaging tools they used where in fact validated:

- There was a validation document for the forensic imaging tool that had been prepared by another member of the laboratory who had validated the forensic imaging tool.
- There was a validation document for the forensic imaging tool that had been prepared by an independent testing body.
- There was a validation document for the forensic imaging tool that had been prepared by a university or other research institution.
- There was a validation document for the forensic imaging tool from the vendor of the forensic imaging tool.

The reasons provided by the respondents are quantified in Figure 46.

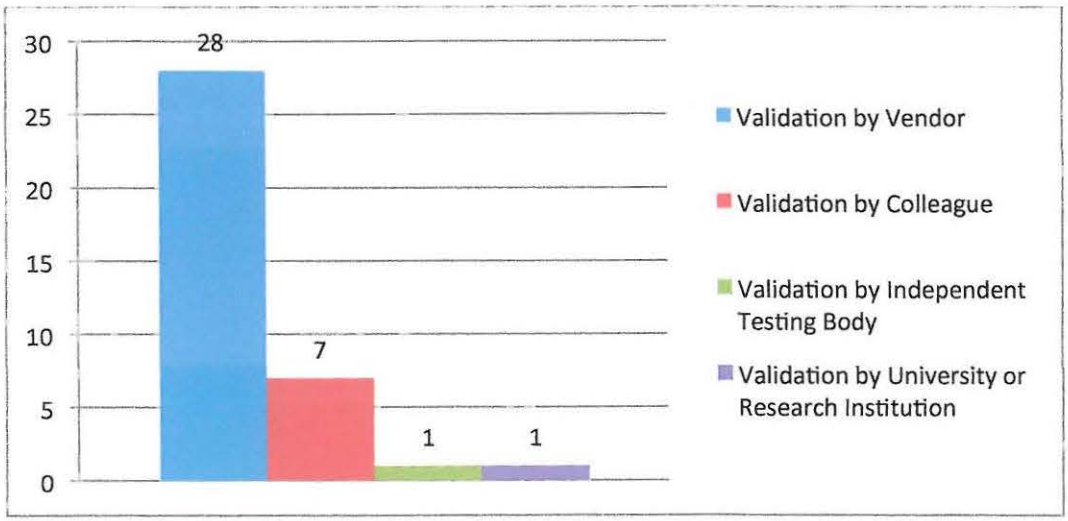


Figure 46 - How Validation Was Done (Forensic Imagers)

Twenty-eight of the respondents relied on the belief that the vendors of the various forensic imaging tools that they stated they used had in fact validated these tools, although five also relied on colleagues, one also relied on validations conducted by an independent testing body, and one also relied on validation conducted by a university or other research institution. Thus, in total 23 of these respondents relied solely on the belief that the vendors themselves had validated the various forensic imaging tools that they stated they used.

Four respondents stated that the tools they used had been validated by an independent testing body. One respondent who stated that he used forensic imaging tools validated by an independent testing body, also stated that these tools were in fact, validated by the independent testing body. All the forensic imaging tools used by these respondents were identified, and a comprehensive search was conducted on the Internet to attempt to identify if any of these tools had in fact been independently validated as stated by the respondents. The results of this survey are listed in Table 16.

Table 16 - Independent Validation Testing (Forensic Imagers)

Forensic Imaging Tool	Type	Independent Validation Testing
EnCase Imager	Proprietary, Freeware	Yes[17]
FTK Imager	Proprietary, Freeware	Yes[18]
Helix Pro	Proprietary, Commercial (based on open source)	Yes
Helix	Proprietary, Freeware (based on open source)	No
dd (or other dd based command line variants)	Open source	Yes[19]
Hardware forensic imager (e.g. Voom Hardcopy, Logicube Talon, etc.)	Proprietary, Commercial	Yes[20]

[17] https://cyberfetch.org/groups/test-results-digital-data-acquisition-tool-encase-65
[18] https://www.cyberfetch.org/groups/reporttest-results-digital-data-acquisition-toolftk-imager-cli-290debian
[19] https://cyberfetch.org/groups/test-results-disk-imaging-tools-dd-gnu-fileutils-4036-provided-red-hat-linux-71
[20] https://cyberfetch.org/groups/test-results-digital-data-acquisition-tool-voom-hardcopy-3p—-firmware-version-2-04

The Auckland University of Technology Digital Forensics Research Laboratories tested a number of forensic imaging tools that were used by the respondents, in particular FTK Imager (version 2.9.0) and Helix Pro, using the NIST CFTT criteria and assertions (Cusack, 2011). FTK Imager 2.9.0 had a pass rate of 89% while Helix Pro had a pass rate of 74% (Cusack, 2011), meaning that FTK Imager 2.9.0 met 89% of the NIST CFTT criteria, and Helix Pro 74% of the NIST CFTT criteria

Twenty-six of the respondents relied on the belief that the vendors of the various forensic imagers had validated the tools, and for 23 of these respondents, this was their sole means of establishing validation. All the forensic imaging tools used by these respondents were identified, and a comprehensive search was conducted on the Internet to attempt to identify if any of these tools had in fact been vendor validated as stated by the respondents. The results of this survey are listed in Table 17.

Table 17- Vendor Validation Testing (Forensic Imagers)

Forensic Imaging Tool	Type	Vendor Validation Testing
X-Ways Imager	Proprietary, Commercial	No
EnCase Imager	Proprietary, Freeware	No
FTK Imager	Proprietary, Freeware	No
Helix	Proprietary, Freeware (based on open source)	No
Helix Pro	Proprietary, Commercial (based on open source)	No
Raptor	Proprietary, Freeware (based on open source)	No
Paladin	Proprietary, Freeware (based on Open Source)	No
dd (or other dd based command line variants)	Open source	No
Hardware forensic imager (e.g. Voom Hardcopy, Logicube Talon, etc.)	Proprietary, Commercial	No

Given the results of our survey, this means that all these 23 respondents believed incorrectly that the forensic imaging tools they used had been validated by the vendors of those tools.

Twelve of the respondents had attended vendor neutral training courses and 20 had attended vendor training courses, while seven and one of these, respectively, had also completed the course in computer forensics at UCT and UP. Eight of these respondents had received no formal training in digital forensics, while two of these eight had completed the computer forensics course at UCT.

Thirteen respondents had experience testifying in court as digital forensic practitioners, but only two of these had been cross examined about the use of validated tools.

5.9.3. Validating Forensic Imaging Tools

Sixteen respondents stated that they conducted validation tests of the forensic imaging tools they used. These respondents were asked when their validation tests were conducted with their responses quantified in Figure 47.

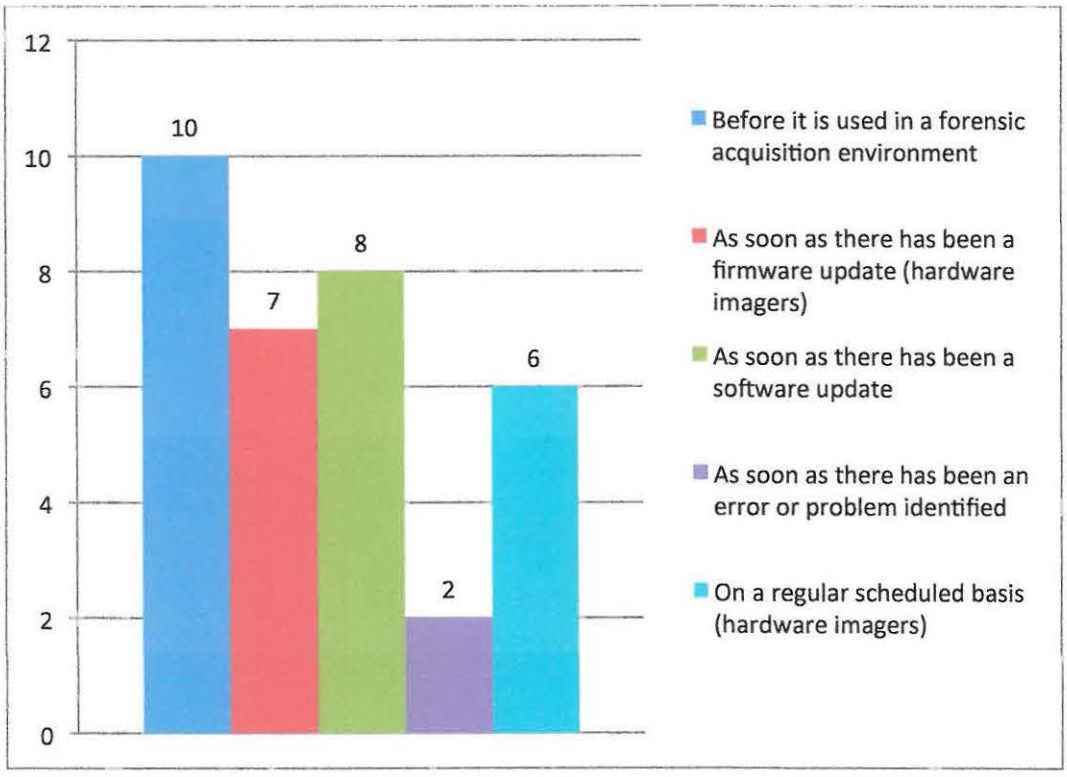


Figure 47 - When Forensic Imagers are Validated

Only ten of these respondents stated that they conducted validation testing before a particular forensic imaging tool was used to acquire digital evidence for the first time by them.

All 16 of these respondents stated that they used software based forensic imaging tools, however, only eight of them stated that they conducted validation tests after a

software update had been made. Two of the respondents stated that they tested hardware based imaging tools, despite the fact that both of them stated that they also used software based forensic imaging tools.

Eleven of these respondents stated that they did not conduct their validation test in terms of any established validation standard, while five stated that they did, as illustrated in Figure 48.

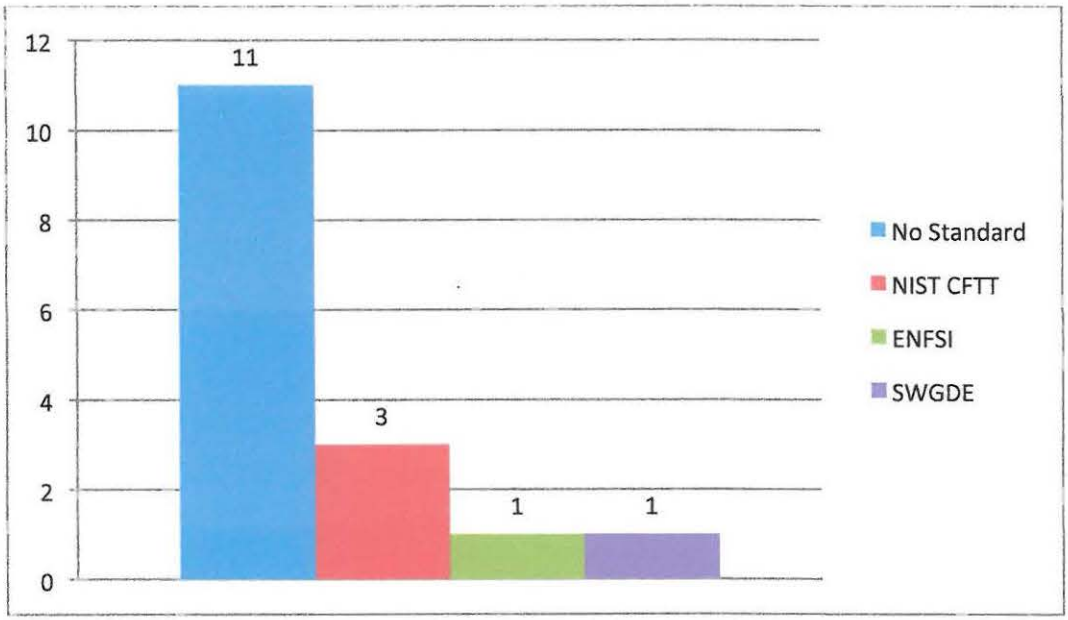


Figure 48 - Formal Standards Used for Validating Forensic Imagers

The three respondents who stated that they conducted their validation testing in terms of the NIST CFTT standard described their testing methodology. All of them stated that they used a dual tool validation method, which is not compliant with the NIST CFTT standard. The one respondent who stated that he conducted his validation testing in terms of the ENFSI standard described his testing methodology as simply imaging a known test drive and confirming that the hash of the image matched that of the drive, which is only partially compliant with the ENFSI standard. The one respondent who stated that he conducted his validation testing in terms of the SWGDE standard described his testing methodology as simply imaging known test drives and confirming that the hash of the image matched that of the drives, which is only partially compliant with the SWGDE standard.

The 11 respondents who stated that they did not use an existing validation standard were also asked to describe their methodologies used. Two specific methodologies were identified. Six of these respondents simply imaged the same media using two

different forensic imaging tools to determine if the images obtained matched each other. The remaining five respondents simply made use of the hashing functionality of the forensic imaging tools to test the hash values of the media being imaged before acquisition, and then compared the hash values of the image to see whether they matched. Both of these methods, while not necessarily scientifically robust, do at least provide a certain level of assurance of a tool's functionality.

Ten of these respondents stated that they documented their validation tests, while six stated that they did not, as illustrated in Figure 49. It is however, concerning that six respondents did not document their tests, meaning that there was no evidence that they could produce in court if asked to do so to prove that they had actually conducted validation tests.

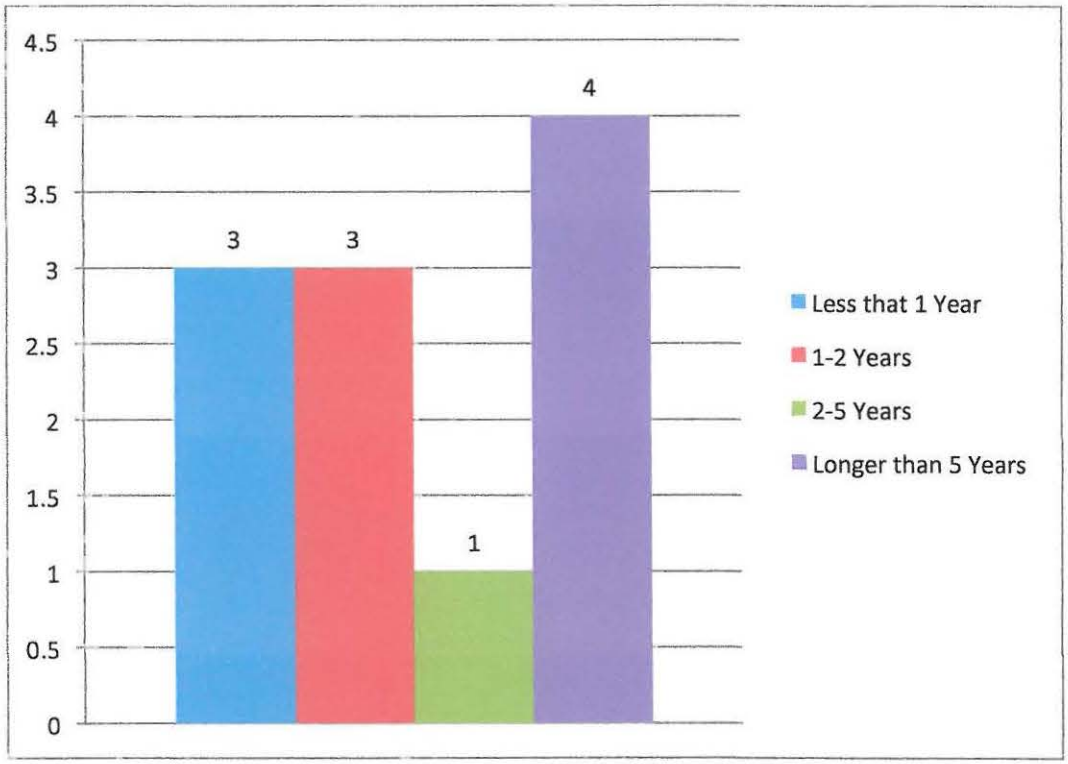


Figure 49 - Validation Test Documentation Retention (Forensic Imagers)

Only one respondent stated that he had been trained in how to conduct a validation test while attending the Seized Computer Evidence Recovery Specialist course in the United States.

Eight of the respondents had attended vendor neutral training courses, 13 had attended vendor training courses, and one had also completed the course in computer forensics at UCT. Two of the respondents had received no formal digital forensics training.

Ten of these respondents had experience testifying in court as digital forensic practitioners, but only three had been cross examined about the use of validated tools.

5.10. SUMMARY

The analysis of the data from the respondents identified significant concerns with regards hardware and/or software using the forensic acquisition of digital evidence. In general the validity of both write-blockers and imagers could not be objectively proven. A number of potential contributing factors were identified which included a lack of training, lack of experience, lack of knowledge or standards (including validation practices), and the manner in which legal practitioners introduce and challenge digital evidence in court.

6. CONCLUSION

Having completed our research we are able to draw specific inferences supported by the research data. Using these inferences, recommendations are made for further research.

6.1. THE USE OF VALIDATED FORENSIC ACQUISITION TOOLS

The core hypothesis of this study was that digital forensic practitioners in South Africa make use of hardware and/or software tools for the forensic acquisition of digital evidence, whose validity and/or reliability cannot be objectively proven; and as such the reliability of any digital evidence preserved using those tools is potentially unreliable.

There were three specific categories of data regarding the use of validated tools.

- **Category One**
  Digital forensic practitioners that did not make use of validated tools.
- **Category Two**
  Digital forensic practitioners that were of the opinion that the tools they used were validated by another party.
- **Category Three**
  Digital forensic practitioners that tested the tools they used themselves.

With regard to Category One, 14 respondents did not make use of validated write blockers, while nine respondents did not make use of validated forensic imagers. This provided a total of 23 instances where tools used were not proven to be validated.

With regard to Category Two, 15 respondents claimed that only the write blocker tools they used had been validated by the vendors of those tools, while 23 respondents claimed that only the forensic imaging tools they used had been validated by the vendors of those tools. The research could identify no instances where the tools that these respondents used had in fact been validated by the vendors, and as such the validation of these tools cannot be proven. This provides a total of 38 instances where the tools used were not validated.

In addition in Category Two, nine respondents stated that the write blocker tools they used had been validated either by colleagues who had tested the tools (although this could not be verified), or that the tools had been independently tested. Eight

respondents stated that the forensic imaging tools they used had been validated either by colleagues who had tested the tools (although this could not be verified), or that the tools had been independently tested. Certain of the tools used had been validated independently, however, this did not apply to all the tools used. It is for this reason that these 17 instances are considered to be inconclusive as there is no proof either way regarding the validation of these tools.

With regard to Category Three, seven respondents stated that they did conduct validation tests of their write blockers, but these tests were not documented in any way. Six respondents stated that they did conduct validation tests of their forensic imaging tools, but these tests were not documented in any way. In the practice of digital forensics documentation is critical, especially when needed to prove something in a court of law. Without documented tests, the validation of these tools cannot be objectively proven in court, and as such, these 13 instances show that the tools cannot be proven to be validated.

In addition in Category Three, 11 respondents conducted validation testing of their write blockers which was documented, while ten respondents conducted testing of their forensic imaging tools which was documented. However, all of the validation tests that were conducted, while providing a modicum of assurance of the reliability of the tools, fell short of providing conclusive objective proof that the tools were reliable. It is thus considered that these 21 instances do provide proof of validation, even though the weight of this proof is weak.

Based on this, in 66% of instances, the validity and/or reliability of the tools used for the forensic acquisition of digital evidence cannot be proven, and in 15% of instances the results are inconclusive. In 19% of the instances, there is proof of validation, but this proof is weak. This is illustrated in Figure 50.

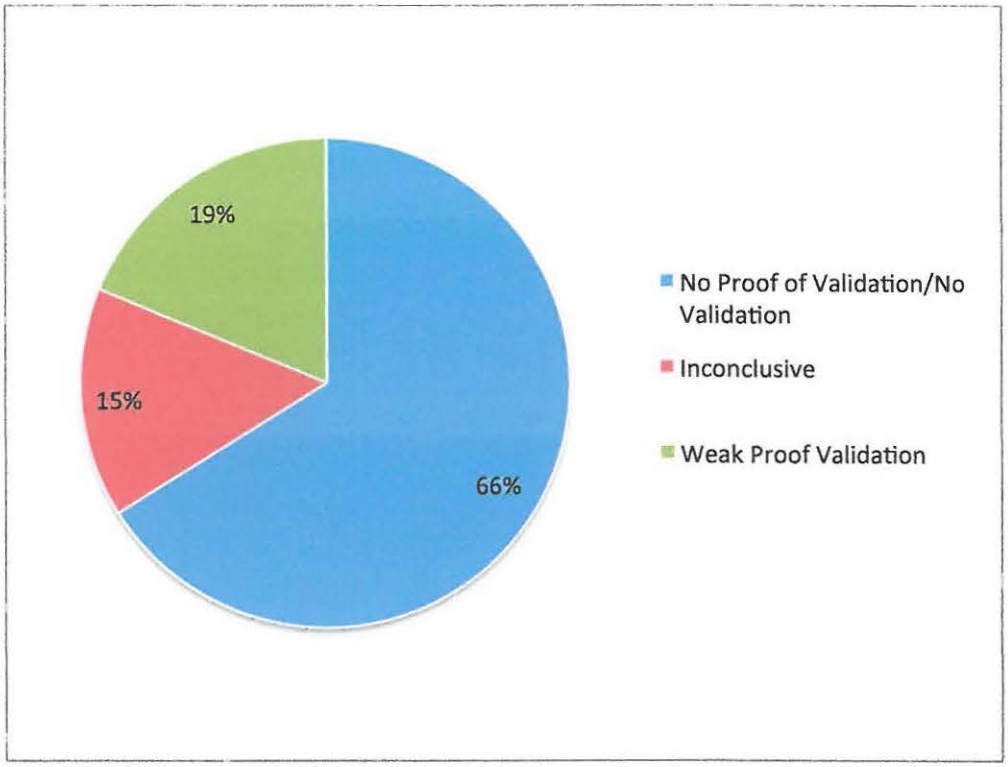


Figure 50 - Proof of Validation

These results support the core hypothesis in that the majority of digital forensic practitioners do not use tools in the forensic acquisition of digital evidence that can be proven to be validated and/or reliable. While just under a fifth of digital forensic practitioners can provide some proof of validation and/or reliability, the proof of validation does not meet formal standards such as those used by the National Institute of Standards and Technology Computer Forensic Tool Testing program, the Scientific Working Group on Digital Evidence, and the European Network of Forensic Science Institutes. Consequently, the practices in South Africa still do not adequately address the validity and reliability of these tools in an objective and scientifically valid manner.

In essence this means that digital evidence, which is preserved through the use of specific hardware and/or software tools, and is then presented and relied upon as evidence in a court of law, is preserved by tools where the objective and scientific validity thereof cannot be determined. Considering that South African courts must take into consideration reliability in terms of Section 15(3) of the Electronic Communications and Transactions Act 25 of 2002 in assessing the weight of digital evidence, the weight of digital evidence is undermined through the current state of practice in South Africa by digital forensic practitioners.

The researcher is of the opinion that digital forensic practitioners have so far managed to get away with these practices due to the fact that so few have actually testified in court (only 45% of the sample), and even fewer have been questioned about the tools they used (only 7% of the sample). The reasons for this have not been established, but it is possible that the contributing factor for this is the relative infancy of the use of digital evidence in South Africa court proceedings, as well as digital forensics. When one looks at established forensic sciences such as forensic toxicology, the validation and calibration of the instruments used in the forensic examination are regularly tested in court, and the validity and reliability thereof established through formal validation and/or calibration documents.

The researcher is of the opinion that a contributing factor to the current state of practice in relation to forensic tools used in the forensic acquisition process is the lack of training in the importance of the use of validated tools, and specifically in how to ensure that tools are validated and how to conduct validation tests. Only 2% of the sample had received training on how to conduct validation tests; it should be noted that this specific training course is not available in South Africa. With the exception of one training course, the training that members of the sample had undergone was generally inadequate in terms of addressing validation issues. The researcher is of the opinion that this is an area of critical concern, as validation is one of the core areas that is fundamental not only to the practice of digital forensics, but forensic science in general. When one takes into account the lack of comprehensive training and education in the field of digital forensics amongst the respondents, which has contributed to the poor state of validation practices, then serious questions need to be raised about the general competency of digital forensic practitioners in other fundamental areas of digital forensics, and what impact this could have not only on their effectiveness, but on the cases that they have been involved in.

6.2. RESEARCH CONTRIBUTION

The research has contributed to the understanding of the current state of practice with regard to the use of forensic acquisition tools that are proven to be valid and/or reliable, and identified areas of significant concern that could negatively impact on the use and value of digital evidence in South African legal proceedings.

It has identified that the majority of digital forensic practitioners do not make use of validated forensic acquisition tools, and those that do use validated forensic acquisition tool rely on weak validation protocols. This shows that the current state of digital forensics practice, especially when it comes to the forensic acquisition of digital evidence, is generally poor from a forensic science point of view, owing to the lack of validation practices, which are an important quality assurance process in forensic science. It has also identified the importance of training in this regard.

6.3. FURTHER RESEARCH

A number of issues have been identified through this research, which are suggestions for future research.

The first area of suggested research is the effectiveness of current digital forensics training and education in South Africa, especially in equipping digital forensic practitioners with the core technical and scientific skills required in the field of digital forensics. The research identified areas of concern with regard to technical training and academic education. Does the existing available academic education and technical training available in South Africa actually equip a digital forensic practitioner to be a competent digital forensics practitioner?

The second area of suggested research is the lack of understanding of digital forensics processes and procedures within the legal community, due in part to the limited number of instances where digital forensic practitioners have been cross-examined and questioned about the validity of the tools they use. If legal practitioners were more knowledgeable of digital forensics would they not be more vigilant in how they address digital evidence in court regarding its admissibility and reliability?

7. REFERENCES

Association of Chief Police Officers. (2007). *Good Practice Guide for Computer-Based Electronic Evidence (2nd Edition)*. London: Association of Chief Police Officers.

Association of Chief Police Officers. (2011). *Good Practice and Advice Guide for Managers of e-Crime Investigation (2nd Edition).* London: Association of Chief Police Officers.

Barbara, J. J. (2007). Quality Assurance Practices for Computer Forensics Part 1. *Forensic Magazine*, 4(1), 66-69.

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.

Beebe, N. L., & Clark, J. G. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Digital Investigation*, 2(2), 147-167.

Brennan, K. (2013, September). Learning Computing through Creating and Connecting. *Computer*, 46(9), 52-59.

Britz, M. T. (2009). *Computer Forensics and Cyber Crime: An Introduction (2nd Edition).* Upper Saddle River: Prentice Hall.

California Crime Laboratory Review Task Force. (2009). *An Examination of Forensic Science in California.* Attorney General's Office, Department of Justice. Sacramento: Department of Justice.

Carrier, B. (2003). Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. International Journal of Digital Evidence, 1(4), 1-12.

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

Casey, E. (2005). Growing Pains. *Digital Investigation*, 2(2), 71-73.

Casey, E. (2007). What Does "Forensically Sound" Really Mean? *Digital Investigation*, 4(2), 49-50.

Casey, E. (2011). *Digital Evidence and Computer Crime (3rd Edition).* London: Academic Press.

Casey, E., & Rose, C. W. (2010). Forensic Analysis. In E. Casey (Ed.), *Handbook of Digital Forensics and Investigation* (pp. 21-26). London: Academic Press.

Cusack, B. (2011, February). On Trial-Imaging Tool Performance. *Digital Forensics Magazine,* (6), 11-13.

European Network of Forensic Science Institutes. (2009). *Guidelines for Best Practice in the Forensic Examination of Digital Technology.* The Hague: European Network of Forensic Science Institutes.

Fereday, M. J., & Kopp, I. (2003, April). European Network of Forensic Science Institutes (ENFSI) and Its Quality and Competence Assurance Efforts. *Science & Justice*, 43(2), 99-103.

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and Verification of Computer Forensic Software Tools - Search Function. *DFRWS 2009: Proceedings of the Ninth Annual DFRWS Conference* (pp. S12-S22). Montreal: Elsevier.

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.

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

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

Irons, A. D., Stephens, P., & Ferguson, R. I. (2009, September). Digital Investigation as a Distinct Discipline: A Pedogogic Perspective. *Digital Investigation*, 6(1-2), 82-90.

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

Jordaan, J. (2012). A Sample of Digital Forensic Quality Assurance in the South African Criminal Justice System. *Information Security for South Africa*. Johannesburg: IEEE.

Kenneally, E., & Brown, C. (2005). Risk Sensitive Digital Evidence Collection. *Digital Investigation*, 2(2), 101-119,

Kessler, G. C. (2012, December). Advancing the Science of Digital Forensics. *Computer*, 45(12), 25-27.

Lyle, J. R. (2003). NIST CFTT: Testing Disk Imaging Tools. *International Journal of Digital Evidence*, 1(4).

Lyle, J. R. (2006). A Strategy for Testing Hardware Write Block Devices. *Proceedings of the Digital Forensic Research Workshop 2006* (pp. S3-S9). Lafayette: Elsevier.

Lyle, J. R. (2010). If Error Rate is Such a Simple Concept, Why Don't I Have One for My Forensic Tool Yet? *Proceedings of the Digital Forensic Research Workshop 2010* (pp. S135-S139). Portland: Elsevier.

Lyle, J. R., & Wozar, M. (2007). Issues With Imaging Drives Containing Faulty Sectors. *Proceedings of the Digital Forensic Research Workshop 2007* (pp. S13-S15). Pittsburgh: Elsevier.

Marcella, A. J., & Guillossou, F. (2012). *Cyber Forensics*. Hoboken: Wiley.

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.

Meintjes-Van der Walt, L. (2012). Electronic Evidence. In S. Papadopoulos, & S. Snail (Eds.), *Cyberlaw@SA III* (pp. 315-332). Pretoria: Van Schaik.

Meyers, M., & Rogers, M. (2005). Digital Forensics: Meeting the Challenges of Scientific Evidence. In *Advances in Digital Forensics* (pp. 43-50). New York: Springer.

National Institute of Justice. (2001). *Electronic Crime Scene Investigation*. Washington DC: National Institute of Justice.

National Institute of Justice. (2004). *Forensic Examination of Digital Evidence*. Washington DC: National Institute of Justice.

National Institute of Justice. (2007). *Digital Evidence in the Courtroom*. Washington DC: National Institute of Justice.

National Institute of Standards and Technology. (2003). *Software Write Block Tool Specification and Test Plan*. Washington DC: National Institute of Standards and Technology.

National Institute of Standards and Technology. (2004). *Digital Data Acquisition Tool Specification*. Washington DC: National Institite of Standards and Technology.

National Institute of Standards and Technology. (2005). *Digital Data Acquisition Tool Test Assertions and Test Plan*. Washington DC: National Institute of Standards and Technology.

National Research Council. (2002). *The Age of Expert Testimony: Science in the Courtroom*. Washington DC: National Academies Press.

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

Nelson, B., Phillips, A., Enfinger, F., & Steuart, C. (2008). *Guide to Computer Forensics and Investigations (3rd Edition)*. Boston: Course Technology.

Palmer, G. (2001). A Road Map for Digital Forensics Research. *Utica: Digital Forensic Research Workshop (DFRWS)*.

Pan, L., & Batten, L. M. (2009). Robust Performance Testing for Digital Forensic Tools. *Digital Investigation*, 6(1-2), 71-81.

Philipp, A., Cowen, D., & Davis, C. (2010). *Hacking Exposed: Computer Forensics (2nd Edition)*. New York: McGraw-Hill.

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.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 1(3), 1-12.

Republic of South Africa. (2002). *The Electronic Communications and Transactions Act 25 of 2002*. Pretoria: Government Printer.

Rogers, M. K., & Seigfried, K. (2004, February). The Future of Computer Forensics: A Needs Analysis Approach. *Computers & Security*, 43(2), 12-16.

Sammes, T., & Jenkinson, B. (2007). *Forensic Computing (2nd Edition)*. London: Springer.

Sansurooah, K. (2006). Taxonomy of Computer Forensics Methodologies and Procedures for Digital Evidence Seizure. *Proceedings of the 4th Australian Digital Forensics Conference* (pp. 67-77). Perth: Edith Cowan University.

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

Schloss, P. J., & Smith, M. (1999). *Conducting Research*. Upper Saddle River: Prentice Hall.

Schwikkard, P. J., & Van Der Merwe, S. E. (2002). *Principles of Evidence (2nd Edition)*. Cape Town: Juta.

Scientific Working Group on Digital Evidence. (2009). *SWGDE Recommended Guidelines for Validation Testing*. Washington DC: Scientific Working Group on Digital Evidence.

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. *International Journal of Computer Science and Network Security*, 8(10), 163-169.

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

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

United Nations Office on Drugs and Crime. (2011). *Staff Skill Requirements and Equipment Recommendations for Forensic Science Laboratories*. Vienna: United Nations.

University of Cape Town. (2013). Postgraduate Diploma in Management in Information Systems (CG022). INF4016W: Computer Forensics (Curriculum). Retrieved December 19, 2013, from University of Cape Town. Faculty of Commerce. Information Systems: *http://www.commerce.uct.ac.za/InformationSystems/Courses/inf4016w/*

University of Johannesburg. (2013). Faculty of Science Postgraduate Courses. Retrieved January 2, 2015, from: http://www.uj.ac.za/EN/Faculties/science/Students/Documents/Fac_Science_Postgraduate%20Courses%20and%20Research%20Projects.pdf

University of Pretoria. (2013). Honours Degree. Retrieved December 19, 2013, from Computer Science: *http://www.cs.up.ac.za/courses/COS783*

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

Valjarevic, A., & Venter, H. S. (2012). Harmonised Digital Forensic Investigation Model. *Information Security for South Africa (ISSA)* (pp. 1-10). IEEE.

Valli, C. (2006). Establishing a Vendor Neutral Skills Based Framework for Digital Forensics Curriculum Development and Competence Assessment. *Proceedings of the 4th Australian Digital Forensics Conference* (pp. 154-159). Perth: Edith Cowan University.

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

Volonino, L., Anzaldua, R., & Godwin, J. (2007). *Computer Forensics Principles and Practices.* Upper Saddle River: Prentice Hall.

Wilsdon, T., & Slay, J. (2006). Validation of Forensic Computing Software Utilizing Black Box Testing Techniques. *Proceedings of the 4th Australian Digital Forensics Conference* (pp. 113-120). Perth: Edith Cowan University.

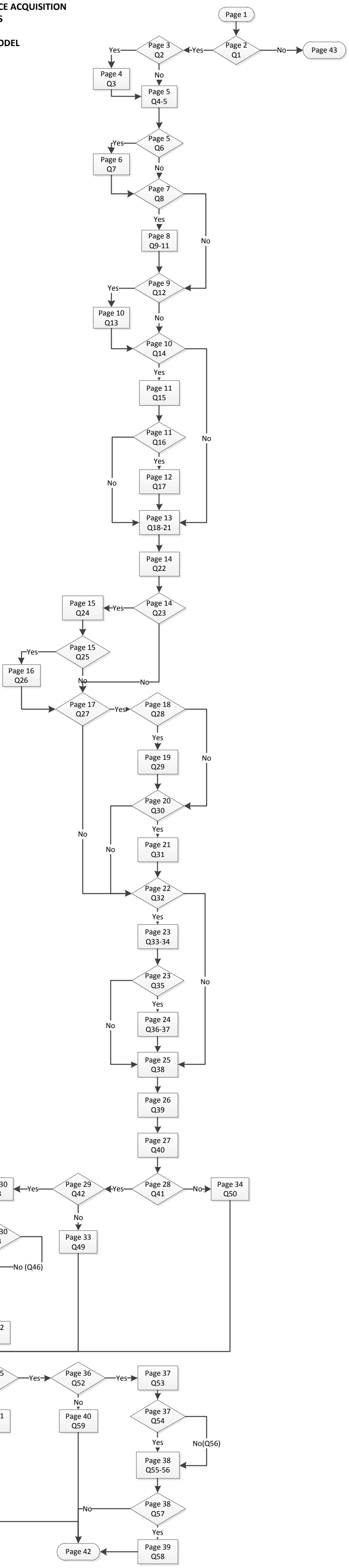
Zatyko, K. (2007, February/March). Defining Digital Forensics. (C. Janson, Ed.) *Forensic Magazine*, 4(1), pp. 18-22.

8. APPENDIX

This appendix contains a printed version of the Internet based research questionnaire that was used to collect the data from the respondents. It also includes a logic diagram showing how skip logic was used in the design of the questionnaire to ensure that respondents only had to answer questions that were relevant to themselves.

THE VALIDATION OF EVIDENCE ACQUISITION TOOLS IN DIGITAL FORENSICS

RESEARCH SURVEY LOGIC MODEL



The Validation of Evidence Acquisition Tools in Digital Forensics

Introduction

The forensic acquisition of digital evidence is perhaps the most crucial part of the entire digital forensics process, and the use of write-blocking hardware and software, and forensic imaging hardware and software are critical tools in this process.

The purpose of this study is to examine the current state of practice in South Africa in relation to the validation of write blockers and imaging tools used in the forensic acquisition of digital evidence, and to establish the reasons for the current state of practice in this area.

As practicing digital forensics practitioners, you are in a unique position to assist the research in better understanding the current practices in this regard in South Africa, and advance the field of digital forensic science through your participation in this research.

The research is being conducted as partial fulfilment for a MSc degree in Computer Science specialising in Information Security at Rhodes University.

The Validation of Evidence Acquisition Tools in Digital Forensics

Declaration

Researcher: Jason Jordaan
Supervisor: Dr. Karen Bradshaw

1. I have received information about this research project.
2. I understand the purpose of this research project and my involvement in it.
3. I understand that I may withdraw from this research project at any stage.
4.I understand that while information gained during the study may be published, I will not be identified and my personal results will remain confidential.
5.I understand that I will receive no payment for participating in this study.

*1. I agree to participate in this research:

◯ Yes

◯ No

Declaration

***2. Would you like to receive a copy of the final research paper(s)?**

- ◯ Yes
- ◯ No

Declaration

＊3. Please provide your e-mail address to which the research paper(s) can be sent. This will be kept confidential.

The Validation of Evidence Acquisition Tools in Digital Forensics

Demographic Data

***4. What is your gender?**

- ◯ Female
- ◯ Male

***5. Which category below includes your age?**

- ◯ 17 or younger
- ◯ 18-20
- ◯ 21-29
- ◯ 30-39
- ◯ 40-49
- ◯ 50-59
- ◯ 60 or older

***6. South Africa is bound to address racial inequalities in terms of our Constitution and other legislation. The following question will ask you to classify yourself in terms of a category in terms of the Employment Equity Act so that the distribution of digital forensic examiners can be determined by grouping. Are you comfortable answering a question of this nature?**

- ◯ Yes
- ◯ No

Demographic Data

***7. In which Employment Equity group are you?**

- ◯ Black
- ◯ White
- ◯ Coloured
- ◯ Indian
- ◯ Asian

Secondary Education

***8. Have you completed matric?**

- ◯ Yes, without University Exemption
- ◯ Yes, with University Exemption
- ◯ No

Secondary Education

***9. Did you have mathematics (not maths literacy) as a subject in matric?**

- ◯ Yes, I passed it in matric
- ◯ Yes, I failed it in matric
- ◯ No

***10. Did you have physical science as a subject in matric?**

- ◯ Yes, I passed it in matric
- ◯ Yes, I failed it in matric
- ◯ No

***11. Did you have information technology (or a similar subject) as a subject in matric?**

- ◯ Yes, I passed it in matric
- ◯ Yes, I failed it in matric
- ◯ No

Tertiary Education

***12. Have you completed an undergraduate degree or diploma?**

- ◯ Yes
- ◯ No

Tertiary Education

*13. Which undergraduate degrees or diplomas have you completed?

- [ ] National Diploma (Information Technology)
- [ ] National Diploma (Policing)
- [ ] BCom (Information Systems)
- [ ] BSc (Computer Science)
- [ ] BSc (Information Systems)
- [ ] BSc (Computer Science and Information Systems)
- [ ] BSc/BEng (Electronic Engineering)
- [ ] BSc/BEng (Computer Engineering)
- [ ] BSc/BEng (Software Engineering)
- [ ] LLB
- [ ] BProc
- [ ] BTech (Policing)
- [ ] BTech (Forensic Investigation)
- [ ] BTech (Information Technology)
- [ ] Other (please specify)

*14. Have you completed a postgraduate degree?

- ◯ Yes
- ◯ No

Tertiary Education

*15. Which postgraduate degree(s) have you completed?

- [ ] BScHons (Computer Science)
- [ ] BScHons (Information Systems)
- [ ] BComHons (Information Systems)
- [ ] MSc (Computer Science)
- [ ] MSc (Information Systems)
- [ ] MCom (Information Systems)
- [ ] MTech (Information Technology)
- [ ] MSc/MEng (Computer Engineering)
- [ ] MSc/MEng (Software Engineering)
- [ ] MSc/MEng (Electronic Engineering)
- [ ] MTech (Policing)
- [ ] MTech (Forensic Investigation)
- [ ] LLM
- [ ] PhD
- [ ] D Litt et Phil
- [ ] LLD

Other (please specify)

*16. Have you studied a module in digital or computer forensics as part of your postgraduate studies?

- ◯ Yes
- ◯ No

Tertiary Education

***17. Which of the following modules in digital forensics have you completed?**

- [ ] Computer Forensics (part of BComHons/PGDip in Information Systems at the University of Cape Town)
- [ ] Computer Forensics (part of BScHons in Computer Science at the University of Pretoria)
- [ ] Computer Forensics (part of BScHons in Computer Science at the University of Johannesburg)

Other (please specify)

Digital Forensics Work Experience

***18. In which industries have you practiced digital forensics?**

- [ ] Private Sector (Digital Forensics Service Provider to External Clients)
- [ ] Public Sector (SAPS, DPCI, SIU, SARS, SSA, Military)
- [ ] Public Sector (Other)
- [ ] Private Sector (In-House Digital Forensics)

***19. In which industry do you currently practice digital forensics?**

- ◯ Private Sector (In-House Digital Forensics)
- ◯ Public Sector (SAPS, DPCI, SIU, SARS, SSA, Military)
- ◯ Private Sector (Digital Forensics Service Provider to External Clients)
- ◯ Public Sector (Other)

20. In which province are you currently based?

- ◯ Eastern Cape
- ◯ Western Cape
- ◯ Free State
- ◯ KwaZulu Natal
- ◯ Northern Cape
- ◯ Gauteng
- ◯ North West
- ◯ Limpopo
- ◯ Mpumalanga

***21. How many total years experience do you have as a digital forensic practitioner?**

- ◯ Less than 1 year
- ◯ 1-2 years
- ◯ 2-5 years
- ◯ 5-10 years
- ◯ 10-15 years
- ◯ More than 15 years

***22. How would you rate your competencies in following areas of digital forensics practice?**

	Poor	Below Average	Average	Above Average	Good
Cyber Law	◯	◯	◯	◯	◯
Law of Evidence	◯	◯	◯	◯	◯
Criminal and Civil Procedure Law	◯	◯	◯	◯	◯
Acquisition of Digital Evidence	◯	◯	◯	◯	◯
Examination of Digital Evidence	◯	◯	◯	◯	◯
Analysis of Digital Evidence	◯	◯	◯	◯	◯
Drafting Forensic Reports/Affidavits	◯	◯	◯	◯	◯
Testifying	◯	◯	◯	◯	◯
General Forensic Science	◯	◯	◯	◯	◯
General Computer Science	◯	◯	◯	◯	◯
General Electronic Engineerings	◯	◯	◯	◯	◯
General Telecommunications	◯	◯	◯	◯	◯
General Mathematics	◯	◯	◯	◯	◯
General Statistics	◯	◯	◯	◯	◯
General Investigations and Criminalistics	◯	◯	◯	◯	◯

***23. Have you testified as a digital forensics practitioner in a court?**

◯ Yes

◯ No

Testifying

***24. In which courts have you had experience testifying as a digital forensics practitioner? Select all that apply.**

- [ ] Constitutional Court
- [ ] Supreme Court of Appeals
- [ ] High Court (Criminal)
- [ ] High Court (Civil)
- [ ] Labour Court
- [ ] Regional Court
- [ ] Magistrates Court

***25. During cross-examination, have you ever been questioned about whether or not your forensic imaging software/hardware, or hardware/software write-blockers have been tested or validated that they are working correctly?**

- ◯ Yes
- ◯ No

Testifying

***26. As a follow-up to the previous question, please describe what happened during cross-examination, and what the consequences were.**

Digital Forensics Training

***27. Have you received any formal training in the field of digital forensics?**

- ◯ Yes
- ◯ No

Vender Training

***28. Have you attended any vendor specific training courses?**

A vendor specific training course is one provided by a digital forensic software or hardware vendor and focuses on the use of the vendor's products in digital forensics.

- ◯ Yes
- ◯ No

Vender Training

***29. Indicate all vendor specific training courses that you have attended. Select all that apply.**

- [ ] EnCase Computer Forensics I
- [ ] EnCase Computer Forensics II
- [ ] EnCase Advanced Computer Forensics
- [ ] AccessData Bootcamp
- [ ] AccessData Forensics

Other (please specify)

Vender Neutral Training

***30. Have you attended any vendor neutral digital forensics training courses?**
A vendor neutral digital forensics training course is a course that focuses on digital forensics principles, processes, and methods, without focusing on specific tools.

- ◯ Yes
- ◯ No

Vender Neutral Training

***31. Indicate all vendor neutral training courses that you have attended.**

- [ ] EC-Council Computer Hacking Forensic Investigator
- [ ] SANS 408 Windows Forensics
- [ ] SANS 508 Advanced Incident Response
- [ ] IACIS Basic Computer Forensic Examination

Other (please specify)

Validation Training

32. Have you received any training on the importance of validation testing of the hardware and software used in the digital forensic process?

- ◯ Yes
- ◯ No

Validation Training

33. Which training courses that you attended covered the importance of validation testing?

***34. What specifically did they cover in relation to validation?**

35. Have you received any training on how to conduct validation testing of the hardware and software used in the digital forensic process?

- ◯ Yes
- ◯ No

Validation Training

***36. Which training courses that you attended covered how to conduct validation testing?**

***37. How did they teach you to conduct validation testing?**

Validation Standards

***38. How would you rate your knowledge of the following validation standards as they are applied in the science of digital forensics?**

	I do not know anything about this standard	I have heard about this standard	I have read this standard	I understand most of this standard	I understand this standard in detail
NIST CFTT	◯	◯	◯	◯	◯
IACIS	◯	◯	◯	◯	◯
ENFSI	◯	◯	◯	◯	◯
SWGDE	◯	◯	◯	◯	◯

Write-Blocking Methods and Tools

***39. Select all of the write-blocking tools or methods that you make use of.**

- [ ] WinFE
- [ ] Helix
- [ ] Helix Pro
- [ ] Raptor
- [ ] Paladin
- [ ] Deft
- [ ] Caine
- [ ] F-Response
- [ ] Tableau Hardware Write-Blockers
- [ ] Wiebetech Hardware Write-Blockers

Other(s) (please specify)

Forensic Imaging Methods Used

***40. Select all of the forensic imaging tools that you use.**

- [ ] Hardware forensic imager (e.g. Voom Hardcopy, Logicube Talon etc)
- [ ] dd (or other dd based command line variants)
- [ ] Paladin
- [ ] Raptor
- [ ] Helix
- [ ] Helix Pro
- [ ] FTK Imager
- [ ] EnCase
- [ ] X-Ways

Other(s) (please specify)

Use of Write-Blockers

41. Do you only use write-blockers that have been validated?

- ◯ Yes
- ◯ No

Validation Testing of Write-Blockers

42. Do you conduct validation testing of write-blockers?

- ◯ Yes
- ◯ No

Validation Testing of Write-Blockers

***43. When do you conduct validation tests on your write-blockers? Select all that apply.**

- [ ] Before it is used in a forensic acquisition environment
- [ ] As soon as there has been a firmware update (hardware write-blockers)
- [ ] As soon as there has been a software update
- [ ] As soon as there has been an error or problem identified
- [ ] On a regular scheduled basis (hardware write-blockers)

Other (please specify)

***44. Do you conduct your validation testing of write-blockers using a published standard?**

- ◯ Yes
- ◯ No

Validation Testing of Write-Blockers

***45. Which validation standards and methodologies do you comply with when conducting validation tests of write-blockers? Select all that apply.**

- [ ] NIST CFTT
- [ ] IACIS
- [ ] ENFSI
- [ ] SWGDE

Other (please specify)

***46. How do you test your write-blockers?**

***47. Are your write-blocker validation tests documented?**

- ◯ Yes
- ◯ No

Validation Testing of Write-Blockers

***48. How long do you keep these validation test documents?**

- ◯ Less than 1 year
- ◯ 1-2 years
- ◯ 2-5 years
- ◯ Longer than 5 years

Proof of Validation

***49. How do you know that the write-blockers that you use are validated? Select all that apply.**

- [ ] There is a validation document for the write-blocker that has been prepared by another member of the laboratory who has validated the write blocker
- [ ] There is a validation document for the write-blocker that has been prepared by an independent testing body
- [ ] There is a validation document for the write-blocker that has been prepared by a university or other research institution
- [ ] There is a validation document from the vendor

Other (please specify)

Reasons for Using Non-Validated Write-Blockers

***50. Why do you not make use of validated write-blockers? Please select all that apply.**

- [ ] It is not necessary to use validated write blockers
- [ ] There is no compelling case law or legislation that requires me to do so
- [ ] I have never been challenged in court on this matter so until I am, I do not do this
- [ ] I am not aware of the necessity of using validated write-blockers
- [ ] I do not have the time to validate write-blockers
- [ ] There is no protocol in place in my work environment compelling me to use validated write-blockers
- [ ] Validation testing is an expense

Other (please specify)

Use of Imaging Tools

***51. Do you use imaging software or hardware that has been validated?**

- ◯ Yes
- ◯ No

Validation Testing of Imaging Hardware and Software

52. Do you conduct validation testing of imaging software or hardware?

- ◯ Yes
- ◯ No

Validation Testing of Imaging Hardware and Software

***53. When do you conduct validation tests on your imaging software or hardware? Select all that apply.**

- [ ] Before it is used in a forensic acquisition environment
- [ ] As soon as there has been a firmware update (hardware imagers)
- [ ] As soon as there has been a software update
- [ ] As soon as there has been an error or problem identified
- [ ] On a regular scheduled basis (hardware imagers)

Other (please specify)

***54. Do you conduct your validation testing of imaging hardware and/or software using a published standard?**

- ◯ Yes
- ◯ No

Validation Testing of Imaging Hardware and Software

***55. Which validation standards and methodologies do you comply with when conducting validation tests of imaging hardware and software? Select all that apply.**

- [ ] NIST CFTT
- [ ] IACIS
- [ ] ENFSI
- [ ] SWGDE

Other (please specify)

***56. How do you test your imaging hardware and/or software?**

***57. Are your imaging hardware and software validation tests documented?**

- ◯ Yes
- ◯ No

Validation Testing of Imaging Hardware and Software

***58. How long do you keep these validation test documents?**

- ◯ Less than 1 Year
- ◯ 1-2 Years
- ◯ 2-5 Years
- ◯ Longer than 5 Years

Proof of Validation

***59. How do you know that the imaging hardware and software that you use are validated? Select all that apply.**

- [ ] There is a validation document for the imaging hardware and/or software that has been prepared by another member of the laboratory that has validated it
- [ ] There is a validation document for the imaging hardware and/or software that has been prepared by an independent testing body
- [ ] There is a validation document for the imaging hardware and/or software that has been prepared by a university or other research institution
- [ ] There is a validation document from the vendor

Other (please specify)

Reasons for Not Using Validated Imaging Hardware or Software

***60. Why do you not make use of validated imaging hardware or software? Please select all that apply.**

- [ ] It is not necessary to use validated imaging tools
- [ ] There is no compelling case law or legislation which requires me to do so
- [ ] I have never been challenged in court on this matter so until I am, I do not do this
- [ ] I am not aware of the necessity of using validated imaging tools
- [ ] I do not have the time to validate imaging tools
- [ ] There is no protocol in place in my work environment compelling me to use validated imaging tools
- [ ] Validation testing is an expense

Other (please specify)

The Validation of Evidence Acquisition Tools in Digital Forensics

Thank You

Thank you for participating in this research survey.

The Validation of Evidence Acquisition Tools in Digital Forensics

Thank You

Thank you for considering this research survey, and we respect your decsion not to participate in this research.