Evaluating A Selection of Tools for Extraction of Forensic Data: Disk Imaging

James Liang
B.C.I.S. (Auckland, New Zealand)

a thesis submitted to the graduate faculty of design and creative technologies
AUT University
in partial fulfilment of the
requirements for the degree of
Master of Forensic Information Technology

School of Computing and Mathematical Sciences

Auckland, New Zealand
2010

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

....

Signature

Acknowledgements

This thesis has been completed at the Faculty of Design and Creative Technologies of the AUT University in New Zealand. I would like to take this opportunity to thank all the people that have provided support to this research project. Without them this research might not have been completed. I have received support and motivation from many people, including friends and colleagues, and I would like to apologise to those I do not mention in here.

Firstly, I would to express my sincere gratitude to my supervisor, Dr. Brian Cusack, for the constant support, encouragement and guidance throughout the entire year of my Master’s study. This research would not have been possible without your help. It was a pleasure to discuss my work with you every week. You also suggest that I should publish my research in journals and conferences. You not only offered me advice for my thesis but also enlightened me about my future professional direction I strongly believe your guidance is going to be valuable for me for the rest of my life.

Also, I would like to express my gratitude to my beloved fiancés, ZiLing Qi, who has been taking care of me during my study. Without you I would not have made it to where I am today. I am eternally grateful from the depth of my heart for the sacrifices you made, for the freedom you gave me, for the food you cooked and for the happiness you gave me.

Abstract

The evaluation of digital forensic tools evaluation has been recognised as a challenging, and insufficiently examined research topic in the field of digital forensics. The mainstream digital forensic tools deployed in law enforcement and the private sector are close-sourced and expensive commercial packages. Open-source digital forensic tools are the alterative option for organisations with less funding. The reliability of digital evidence that is collected, analysed and presented using those digital forensic tools has been challenged. There are very few organisations that conduct validation research on digital forensic tools. Software vendors may conduct their own validation tests on the software but their findings are usually not available to the public.

Three areas related to digital forensic tools have been reviewed in this study, namely overview of the digital forensic environment, legal and technical implications of digital forensic tools and evaluation of disk imaging tools. Imaging the disk drives is a critical process in forensic investigation and disk imaging tools are the subject of this research. The review of relevant literature has guided the research to study the validity of disk imaging tools. A research model is designed and implemented with the aid of testing specifications, requirements, assertions, case scenarios and test sets. The model hypothesises that the completeness and accuracy of image data affect positively the validity of the disk imaging tools. A set of selected tools is subjected to validation to analyse if the disk imaging tools generate complete and accurate results. Various case scenarios are designed and the selected tools are validated under a set of forensically-sound procedures that are defined according to the test specifications.

The validation has exposed problems and issues of the selected disk imaging tools that have been evaluated. Some issues of software usability have also been pointed out and discussed. The study has shown that the attributes completeness and accuracy positively affect the validity of the disk imaging tools. The research findings will be valuable for law enforcement and the legal community where forensic disk imaging tools must produce consistent, complete and accurate results. Software developers should focus on ensuring completeness and accuracy of the

imaging data when building disk imaging tools. The usability of the tools should not be underestimated. The test result from this study could be used by software developers to improve their tools and by making the necessary changes. Also, this study could enable law enforcement communities or other interested parties to understand the capabilities of the software and become fully aware of the identified shortcomings and issues.

Table of Contents

Chapter 1. Introduction

Chapter 2. Literature Review

Chapter 3. Research Methodology

Chapter 4. Research Findings

Chapter 5. Discussion of Findings

Chapter 6. Conclusion

Appendix

List of Tables

List of Figures

List of Abbreviations

AI	Access Interface
AM	Access Method
AFF	Advanced Forensic Format
AFD, AFM	Variants of AFF
AHP	Analytic Hierarchy Process
ATA	AT Attachment
BIOS	Basic Input/ Output System
BSD	Berkeley Software Distribution
CART	Computer Analysis and Response Team
CBIR	Content-based Image Recognition
CFCE	Certified Forensic Computer Examiner
CFTT	Computer Forensic Tool Testing
CIFI	Certified Information Forensics Investigator
COTS	Commercial Off-the-Shelf
CVS	Concurrent Versioning System
DCO	Device Configuration Overlay
DD	Data Destination
DELVS	Distributed Environment for Large-scale Investigations System
DFRWS	Digital Forensic Research Workshop
DS	Digital Source
DOJ	Department of Justice
DOS	Disk Operating System
EE	Execution Environment
eSATA	External Serial Advanced Technology Attachment
FRE	Federal Rules of Evidence
FLETC	Federal Law Enforcement Centre
GA	Gap Analysis
GB	GigaByte
GPT	GUID Partition Table

GUI	Graphical User Interface
HFS, HFS+	Hierarchical File System, Hierarchical File System plus
HTCIA	High Technology and Criminal Investigation Association
HPA	Host Protected Areas
IACIS	International Association of Computer Investigative Specialists
IDE	Integrated Drive Electronics
IEEE	Institute of Electrical and Electronics Engineers
IISFA	International Information Systems Forensics Association
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
LBA	Logical Block Address
MAC SE	Macintosh System Expansion
MBR	Master Boot Record
MD5	Message Digest 5
SHA1	Secure Hashing Algorithm version 1
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NW3C	National White Collar Crime Centre
OS	Operating Systems
OSS	Open-Source Software
OTSO	Off-The-Shelf Option
PC	Personal Computers
PDA	Personal Digital Assistant
PECA	Plan, Establish, Collect, Analyse
RAM	Random-access Memory
RAID	Redundant Arrays of Inexpensive Disks
RCMP	Royal Canadian Mounted Police
SANS	SysAdmin, Audit, Network, Security
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SSD	Solid State Drive

SWGDE	Scientific Working Group on Digital Evidence
TB	Terabyte
TWGDE	Technical Working Group on Digital Evidence
USB	Universal Serial Bus
V&V	Verification and Validation
WSM	Weighted Scoring Method

List of Software & Hardware

AIR	Automated Image and Restore
Aimage	Software Data Acquisition
ASR	Brand Name
BackTrack	Linux distribution Penetration Testing Live DVD
CAINE	Computer Aided Investigative Environment
Data Copy King	Hardware Disk Imaging Tool developed by SalvationData
Dcfldd	Enhanced version of DD developed by Department of Defense Computer Forensics Lab
Dc3dd	Enhanced version of Dcfldd developed by Department of Defense Computer Forensics Lab
DD	UNIX Utility
DIBS	Brand Name – a US computer forensics company
DiskEdit	Norton Utilities – Disk partitioning tool
EnCase	Brand Name of Guidance Software
FastBloc software	Guidance Software
FTK	Forensics Toolkits Developed by AccessData
Gparted	GUI Disk Partitioning Tool
HardCopy 3	Hardware Disk Imaging Tool developed by Voom Technology
HDAT2	Disk drives testing and diagnosing program
Hdparm	Utility to set and view ATA hard disk hardware parameters
Helix 3 Pro	Forensics Live CD developed by E-fense
Logicube	Hardware Disk Imaging Tool developed by Talon
IIS	Internet Information Services from Microsoft
iLook	Forensics Toolkits developed by Perlustro
MHDD	Hard disk drive diagnostics program developed by Dmitry Postrigan
Pcap	Packet Capture
MySQL	Open-source Database recently acquired by Oracle
NetAnalysis	Forensics Toolkits developed by Digital Detective

NetIntercept	Network monitoring and analysis system developed by NIKSUN
ProDiscover	Forensics tool developed by Technology Pathways
TCT	The Coroner’s Toolkit - UNIX Forensics toolkits
TCPDump	Packet Analyser
SafeBack	Data acquisition tool developed by NTI
SilentRunnder	Network Traffic Analyser developed by AccessData
Sleuthkit	Open-source Forensics Toolkits developed by Brian Carrier
SMART	Forensics Toolkits developed by ASR Data
SQL	Structured Query Language
Snort	Network Intrusion Detection System developed by Sourcefire
Tableau TD1	Hardware Write Blocker developed by Guidance Software
WinHex	Forensics data recovery software developed by X-Way Software
XtreeGold	File manager software under DOS developed by Jeffrey Johnson

Chapter 1

Introduction

1.0 INTRODUCTION

Much of the research and work to date in digital forensics has been concerned with data collection and analysis. Many commercial digital forensics toolkits have been developed and widely employed in law enforcement and private sectors. Forensic practitioners have been using these toolkits on a regular basis to collect, analyse and present digital evidence. However, not all organisations can afford to acquire such expensive commercial packages. Organisations with lower funding for forensics may seek an alternative option, namely, the use of open-source tools. Many open-source tools have not been originally designed for forensic purposes so they do not satisfy forensics standards (Bukhari, Yusof, & Abdullah, 2010). According to the Daubert Standards, the techniques and methods used to derive evidence must be empirically tested and peer-reviewed. Open-source tools are also less likely to have been evaluated in an organised and comprehensive fashion. Sommer (2010) also states that even the most popular toolkits EnCase and FTK are not tested to the standard expected for most forensics scientists.

Studies that focus on the validation of digital forensics tool are very limited. This research attempts to empirically evaluate a selected set of disk imaging tools using an improved methodology based on the some related studies. A method called Function mapping has been adopted from Guo, Slay, & Beckett (2009). The method is incorporated into the methodology to help the research explore potential testing requirements. The main objective of the evaluation is to ensure that the tested disk imaging tools are able to extract data from the evidence in a complete and accurate manner. The selected tools are subjected to a series of designed tests and the generated results are analysed. The software usability not addressed in CFTT program is also examined and analysed during the evaluation. Research results are summarised and presented both descriptively and in graphical representation so readers can appreciate the results easily.

The aim of this chapter is to provide an overview of the research findings and the structure of the thesis. The rationales behind this research are explained from the legal and technology perspectives in Section 1.1. The main research findings are discussed briefly and presented in Section 1.2. The structure of the thesis is presented in Section 1.3.

1.1 MOTIVATION OF THE RESEARCH

Digital forensics has been well developed in the past decade and has become an important component of many investigations. Investigators from both private and public sectors are relying on the digital forensic tools on a daily basis to gather, assess and analyse digital evidence.

Garfinkel (2010) states that digital forensics is facing a crisis and the tool has gradually become obsolete. The digital forensics community is facing intimate challenges, especially in the process of data collection (Mohay, 2005; Mercuri, 2005). From a legal perspective, according to the guidelines established in Daubert Standard (*Daubert v. Merrell Dow Pharmaceuticals, Inc., 1993*), scientific evidence that is admissible to the court must be validated by five relevant factors. The five relevant factors will be described in Section 2.2.2. The techniques and methods that are used for the collection, analysis and presentation of the digital evidence can be challenged by lawyers as they become more familiar with the technology adopted. However, the progress of the validation of such techniques and methods is limited. The admissibility of the digital evidence can be guaranteed if underlying techniques or methods are scientifically validated and recognised (Erbacher, 2010). Guo et al. (2009, p.S12) also pointed out that one of the challenges the digital forensics practitioners are facing is the difficulty of assuring that the digital evidence extracted by the digital forensic tools is reliable.

There are also technical constraints for digital forensics that are presented and operated in a dynamic computing environment. Forensics practitioners are required to process enormous volumes of data. This task is so demanding that investigators are struggling to transform those data into investigative knowledge. Using a single tool or a forensics toolkit, such as EnCase or FTK, to fulfil all the requirements in different circumstances is unrealistic. Also, even the most popular tools can have flaws that cannot be discovered easily. Ayers (2009a) discovered flaws in EnCase when the dates and time values were handled and the problems were confirmed by the developer Guidance Software. Ayers (2009) also commented that the ability to gain insight into how the commercial tools are operating is very limited. Sometimes, open-source software may be required when the commercial tools fail to fulfil the tasks in certain parts of the investigation. Despite the fact that some types of the open-source software are well built and well documented, some of the tools are out-of-date and poorly documented. There is no doubt that forensic tools with varied quality and documentation must be validated and verified thoroughly. Comprehensive forensic tool validation is an important research topic suggested by many researchers (Peterson, Shenoi, & Beebe, 2009; Garfinkel, 2010; Ayers, 2009).

1.2 RESEARCH FINDINGS

The research has summarised some findings pertinent to different aspects of forensic tool performance testing. In terms of the testing environment, Windows and Linux platforms were chosen as the target validation environment. In order to evaluate the disk imaging tools extensively, the research is required to develop customised disk configuration tools to fulfil the requirements if the resources are allowed. The testers may not be able to comprehend fully knowledge of how the tools operate when using configuration tools that are developed by third-party developers. Details of the test environment setup and testing procedure are presented in Sections 4.2.1 and 5.1.1.

A disk imaging tools testing procedure has been adopted from NIST and redefined to suit the research. Before the start of every new test case, the test drive must be reset or wiped with some proven mechanisms. The test drive can be configured using various methods according to the test specifications. Hardware or tested software write blocker must be used consistently to prevent any alterations to the test drive. Hardware write blocker was not used in some pre-specified test cases. The reason why the hardware write blocker was not used is discussed in Section 5.1.7.3. Disk imaging tools must be operated according to the user manual to avoid producing unreliable results. Extra verification should be conducted over the acquired data with the application of another well-tested tool.

Three disk imaging tools were tested against different test scenarios. The performance of each evaluated tool varies. AIR has achieved higher overall pass rate than the others, followed by FTK Imager. Helix 3 Pro has not achieved 100% pass rate in any test cases (see Section 5.1.3 for more details). During the acquisition of HPA or DCO hidden areas, none of the evaluated disk imaging tools was able to acquire the hidden areas (see testing results in Sections 4.2.2.3 and 4.2.2.10). Helix 3 Pro has presented problems in some test cases. Some usability problems were observed and discussed as well. Better usability will improve the user experience of the software. The disk imaging tool AIR also presented a few problems both in terms of usability and performance (see discussion in Section 5.1.4). The research encountered technical challenges such as locating configuration tools, dealing with hidden areas and using Forensics Live CDs during the evaluation (further details are provided in Section 5.1.6).

1.3 STRUCTURE OF THE THESIS

The thesis consists of four main sections apart from Chapter 1. Introduction and Chapter 6. Conclusion. Chapter 1 sheds light on the gaps in the research areas and the motivation of this research.

Chapter 2 presents a literature review and studies the findings of other academic studies in this research field. The state-of-the-art of digital forensics is reviewed at the beginning of the chapter. The review of investigative processes & standardisations can help the researcher to understand the standard disk imaging procedures that are used in the industry. The research reviews the evolution of digital forensics tools and the characteristics of existing tools in the market (including their limitations). The chapter then investigates the legal and technical implications of digital forensics tools. It reviews the definition and characteristics of digital evidence and how it can be recognised as admissible in courtroom. Most of the digital evidence is collected, analysed and presented using digital forensic tools. The validity of the digital evidence extracted by the digital forensic tools may be challenged. Forensic practitioners are demanding research on the validation of digital forensics tools. The background and the existing works on digital forensic tools verification and validation are reviewed. Finally the chapter concentrates on the definition and discussion of the attributes, mandatory features and the problem areas of disk imaging tools.

In Chapter 3, academic or empirical studies conducted by scholars in this domain are analysed and their methodologies are studied. The research then identifies the model and methodology that can test the research hypotheses empirically and answer the research questions that have been defined earlier in this chapter. The data requirements and the limitation of the research are also reviewed and discussed.

Chapter 4 reports the research findings. The variations to the research specifications are acknowledged and explained. Following this are three major sections, namely field findings, research analysis and presentation of findings. The section on field findings reports the findings about the performance testing of disk imaging tools. The findings are summarised and analysed, followed by findings associated with graphic representations.

Chapter 5 discusses the research findings presented in Chapter 4 in terms of the testing environments and procedures and the performance of each tested disk imaging tool. Chapter 5 also specifies the differences between the present research and previous studies in the same field. It clarifies how the hypotheses defined in Chapter 3 are tested.

The final chapter of this thesis will summarise the research findings and answer the research questions. The areas for potential future research are also discussed, followed by the conclusion of the thesis.

1.4 CONCLUSION

Chapter 1 is concerned with presenting the background information for this research and its the main motivation. A snapshot of the research findings is also captured and presented in this chapter. The main purpose is to summarise the key research findings and present them in a concise manner. The structure of this thesis from chapter 1 to 6 has been laid out with a brief introduction.

The rationales behind this research are also explained from both legal and technological perspectives. The main rationale behind the research is to fill the gaps in previous studies in the same domain. The findings about the testing environment, procedures and the performance of the disk imaging tools are also explained briefly. The structure of this thesis also provides guidance for the readers.

To further explore the gaps in the research field, Section 2.1 offers an overview of the digital forensic environment, including the review of relevant literature about the investigative processes and the development of digital forensic tools. Some previously conducted studies on legal and technical implications of digital forensic areas are reviewed in Section 2.2. The legal significance of the digital forensic tools lies in the admissibility of digital evidence. The technical and legal challenges are demanding research of digital forensics tools verification and validation. The chapter also defines and investigates the contemporary state-of-the-art disk imaging tools.

Chapter 2

Literature Review

2.0 INTRODUCTION

The rapid development of communication and computing technology has led to the creation of large computer networks. However, this development has not come without a corresponding growth of electronic crimes (Brungs & Jamieson, 2005, p.57). Electronic crimes continue to pose a significant problem and cause huge financial losses, according to the CSI/FBI survey 2007 (Richardson, 2007). Computers and other electronic devices store many types of electronic data. Electronic data has played a crucial role as evidence in various court cases involving corporate litigation, theft of intellectual property, credit card fraud and pornography (Williams, 2006; Johnson, 2005). Detailed methods and procedures for evidence collection have developed within the digital forensics in order to combat the growing number of electronic crimes. Evidence collection is the procedure that ensures the evidence is reliable, intact, accurate and verified (Kenneally & Brown, 2005).

Electronic evidence is fragile in nature and can easily be modified, duplicated or damaged (Kleiman et al., 2007). Electronic evidence collected in an untested method may not withstand scrutiny in the court of law (Williams, 2006). A comprehensive procedure and fully tested tools must be utilised to acquire electronic evidence. A common industry practice is to acquire a bit-stream image of the storage media (Meyers & Rogers, 2004). Bit-stream image is the exact replica of the original device. As distinct from the normal hard drive backup, the bit-stream image will duplicate deleted files, file slacks, swap files, hidden areas and unallocated spaces. Also, the accuracy of the bit-stream image must be validated as well. A mathematical algorithm, such as MD5 or SHA1, is used to calculate a hash value for the original disk and compute another hash value for the bit-stream image to see whether both values are matched. Unfortunately, forensic software also has vulnerabilities like any other kind of software. US-CERT (2007) published a note that a bug has found in EnCase. Newsham et al. (2007) published an article to demonstrate how to break forensic software EnCase and SleuthKit. The validity of forensic software is required for the court to accept the software.

Two competing categories of software are proprietary and open source. Digital forensic software can also be either proprietary or open source. There is considerable debate around the strengths and weaknesses of both types (Kenneally, 2001). Proprietary and open source software has been a topic of enduring discussion for the software industry. For example, Kenneally (2001) presents an argument for using open source software as a mechanism to assess reliability of digital evidence by pointing out the dangers imposed by proprietary forensic software on the validity of such evidence. Carrier (2002) as a pioneer of open source forensic software development supports Kenneally's argument by assessing open source forensic tools with Daubert guidelines. To assess the validity of forensic software it is essential to understand every aspect of its capability. An overview of the digital forensic environment is presented in section 2.1 to capture a snapshot of the current status of digital forensic tools development. Section 2.2 reviews the legal and technical implications for digital forensic tools. The section reviews the criteria of evidence, namely admissibility and reliability, in relation to digital forensic tools. The development of digital forensic tools verification and validation is also reviewed in section 2.2.4. The scope and specifications of disk imaging tools are spelt out in section 2.3 and 2.4 based on the literature review in sections 2.1 and 2.2. Finally, section 2.5 summarises the key problems and issues raised in the reviewed literature. It is followed by the summary and conclusion.

2.1 OVERVIEW OF DIGITAL FORENSIC ENVIRONMENT

Different aspects of digital forensics are studied in this chapter. The investigation of various perspectives of digital forensics provides a foundation for building the testing requirements for disk imaging tools. The following section gives a brief introduction to computer forensics and digital forensics. It is followed by an analysis of digital forensic investigative processes and standardisation. Different digital forensic tools that are relevant to this study are discussed and analysed in the last section.

2.1.1 Computer Forensics And Digital Forensics

The movement from computer forensics to digital forensics is presented in this section. Wang, Cannady, & Rosenbluth (2005, p.119) defines computer forensic as a developing discipline rooted in forensic science and computer technology, focusing on acquiring, analysing and presenting evidentiary evidence from computer systems to prosecute computer involved crimes and offences. Another notable definition was provided by Britz (2008). Dixon (2005, p.7) stated that the central parts of computer forensics are the preservation, identification, extraction, documentation and interpretation of computer data.

Caloyannides, Memon, & Venema (2009) state that computer forensics is performing static analysis on a single compromised computer system and missing dynamic information, such as network connections, malwares in the memory and decryption keys. Many other electronic devices such as laptops, Personal Digital Assistants (PDAs), mobile phones, printers, fax machines and tablet PCs have been developed and widely used. The range of devices that are of interest to computer forensics investigation is broadened to include the new popular electronic devices. A new terminology “Digital Forensics” has been created and the term represents better the current state of computer forensic environment. The term “Computer Forensics” is still commonly used to refer to any investigation involving computers. The first Digital Forensic Research Workshop (DFRWS, 2001) defines digital forensic science as follows:

> The use of scientifically derived and proven methods toward 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 found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (p. 16).

Some practitioners now prefer to use Digital forensics to describe a greater scope of potential evidence than what is included in computer forensics literature and often use more specialised terms such as mobile forensics and network forensics.

2.1.2 Investigative Processes And Standardisations

The procedures for conducting digital forensics investigations are neither consistent nor standardised, but rather the result of disciplined professional practice (e. g. In Police laboratories) or the result of investigators adopting the many guidelines for best practice that come from various police sources. The procedures and the need for standardisation for digital forensics investigation are evolving continuously. The processes or approaches used for digital investigations are largely adopted from other investigation related discipline areas. If any steps of the process have been neglected or cannot be validated, it may lead to an incomplete or inconclusive result or findings (Baryamureeba & Tushabe, 2004). Investigation processes or procedures are driven by the technology and tools utilised in the investigation. If the technology or tools used in the investigation change, the associated procedures or processes have to adapt correspondingly. Many research groups such as the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have been dedicating their efforts to the creation of a standardised approach for digital forensics investigations (Noblett et al., 2000). Studying the investigative processes and standards will assure the tool validation follows procedures that are scientifically proven and recognised by the industry.

DFRWS, a research consortium lead by a group of academics, is a significant participant in the development of digital forensic investigative processes. DFRWS considers one of the biggest challenges in computer forensic science is that “analytical procedures and protocols are not standardized nor do practitioners and researchers use standard terminology” (Palmer, 2001, p.7). Therefore, DFRWS has worked to develop a generic digital forensics investigation process that includes such phases as “identification, preservation, collection, examination, analysis, presentation, and decision” (Palmer, 2001). This process depicted in Figure 2.1 lays down an important foundation for the future work on digital forensics standardisation. Another commendable effort in digital forensics standardisation was made by National Institute of Justice (NIJ) of the United States.

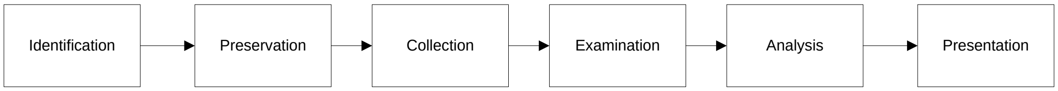


Figure 2.1. **DFRWS Investigation Process**

NIJ (2001) published an abstract process of digital forensics investigation including the phases of "collection, examination, analysis, and reporting". This process decipted in Figure 2.2 allows traditional physical forensic knowledge be used in digital forensic investigation. NIJ (2001) is a reference guide for the first respondent in the crime scene to identify different electronic devices and to handle any potential evidence. The process ensures that the digital evidence collected is complete, validated and acceptable in court. The emphasis of the guide is to instruct the first respondent how to handle digital evidence in physical crime scene but very little attention is paid on evidence examination and analysis (Carrier & Spafford, 2003). The guide also identifies different types of potential evidence that may be relevant to crimes, as well as the types of crime that may be associated with the evidence. One of the problems of the NIJ testing methodology is that the level of detail often does not go beyond considering the collection of physical hard drives. For example, it is unclear that hard drives contain relevant evidence at the point of the evidence collection. In addition to the first respondent guide, NIJ has also published several guides to help law enforcement and prosecutors to gain a better understanding of the investigation processes. The NIJ developed a program called Computer Forensic Tool Testing (CFTT). CFTT tests computer forensic tools according to well-defined methodologies, test specifications and methods developed by a group of industry experts. CFTT program helps the tool developers improve their tools, the users to make informed choices about acquiring and using computer forensic tools and the legal community and interested parties to understand the capabilities of those tools and reduce the challenges of admissible digital evidences (NIST, 2005). Hundreds of computer forensic software and hardware tools have been tested and all the results are publicly available over the Internet.

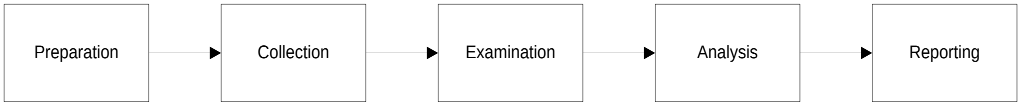


Figure 2.2. **NIJ Investigation Process**

Many academics, research groups and corporations have attempted to develop frameworks for digital forensics investigations including the examples presented in Table 2.1. Selamat, Yusof, & Sahib (2008) summarised that the existing digital forensics frameworks (see Table 2.1) can map onto five common phases, namely Phase1 - Preparation, Phase 2- Collection and Preservation, Phase 3 - Examination and Analysis, Phase 4 - Presentation and Reporting and Phase 5 - Disseminating the case. Table 2.1 summarises different digital forensic investigation frameworks so that standard digital forensics investigation procedures can be established. Different activities and processes are also incorporated into appropriate phases. This study not only summarised some previous frameworks in great detail but also simplifies the existing frameworks. According to the result analysis from Selamat et al. (2008), most of the existing frameworks include the critical phases phase 2, 3 and 4. On the other hand, many frameworks (Pollitt, 1995; Stephenson, 2003) do not include phase 1 and 5 as their standard processes. However, some frameworks (Baryamureeba & Tushabe, 2004; Beebe & Clark, 2004; Carrier & Spafford, 2003; Ciardhuain, 2004; Freiling & Schwittay, 2007; Rogers, Goldman, Mislan, Wedge, & Debrota, 2006; Kohn, Eloff, & Olivier, 2006; Reith, Carr & Gunsch, 2002) suggest that Phase 1 and 5 are significant to ensure the completeness of digital forensic investigations to produce accurate and conclusive results.

Some of the frameworks have similar approaches on how to perform an investigation. For example, Carrier & Spafford (2004) and Kent, Chevalier, Grance, & Dang (2006) have similar approaches on acquiring digital evidence specifically in hard disk imaging. It consists of two parts, namely disk imaging and forensic copy verification. A complete forensic disk image backup is required and the original evidence is preserved as physical evidence. After the forensic copy is made, its integrity is verified. Tools can be employed to compute the message digest of the original to the forensic copy, then compare the two values and make sure they are matched. To conclude, a universal and standardised scientific approach for digital investigation is yet to be established. Also, the investigative models reviewed above do not contain details of how disk imaging of evidence should be done in a standardised manner. Only fragments of details are mentioned about disk imaging.

Table 2.1

Existing Digital forensics Investigation Frameworks (updated from Selamat et al., 2008, p.164)

No	Digital forensics Investigation Framework	Number of phases	Phases Included
1	Computer Forensic Process (Pollitt, 1995)	4 processes	2-4
2	Generic Investigative Process (Palmer, 2001)	7 classes	2-5
3	Abstract Model of the Digital Forensic Procedure (Reith et al., 2002)	9 components	1-5
4	An Integrated Digital Investigation Process (Carrier & Spafford, 2003)	17 phases	1-5
5	End-to-End Digital Investigation (Stephenson, 2003)	9 steps	2-4
6	Enhance Integrated Digital Investigation Process (Baryamureeba & Tushabe, 2004)	21 phases	1-5
7	Extended Model of Cybercrime Investigations (Ciardhuain, 2004)	13 activities	1-5
8	Hierarchical, Objective-based Framework (Beebe & Clark, 2004)	6 phases	1-5
9	Event-based Digital Forensic Investigation Framework (Carrier & Spafford, 2004)	16 phases	1-4
10	Forensic Process (Kent et al., 2006)	4 processes	2-5
11	Investigation Framework (Kohn et al., 2006)	3stages	1-5
12	Computer Forensics Field Triage Process Model (Rogers et al., 2006)	4 phases	1-5

13	Investigative Process Model (Freiling & Schwittay, 2007)	4 phases	1-5

2.1.3 Development And Evolution of Digital Forensic Tools

It was common to use the evidentiary computer to gather evidence when no specialised digital forensics tools were available. The major risk of this traditional approach is that potential evidence can be overlooked such as deleted and hidden files. In addition, the integrity of the evidence is not verifiable. Software programs, such as DD (shown in Table 2.2), could be used to acquire the content of an entire hard disk and even capture the deleted data but these programs are not widely recognised as a forensic tool. It was adopted in the law enforcement sector but most of the forensic investigators were still performing investigations at file system level without showing much heed to deleted and hidden data. Several software programs are discussed through this section to analyse the development and evolution of the digital forensic tools. The analysis will help the research better understand the capability of the digital forensic tools. Table 2.2 summarises the main functionalities of the discussed software programs in this section.

Software programs that are capable of recognising different file types and recovering deleted files have appeared in the market such as Norton DiskEdit and XtreeGold (shown in Table 2.2). Some specialised forensic tools, such as SafeBack and DIBS (shown in Table 2.2), were developed with the capability of collecting electronic evidences without damaging the integrity of the original evidentiary data. The Law enforcement sector such as Royal Canadian Mounted Police (RCMP) also developed their specialised software tools for computer investigations (Casey, 2004). The introduction of large data storage devices caused new problems for forensic investigators (Akhter, 2008). Automated and integrated software toolkits such as, EnCase, FTK and iLook (shown in Table 2.2), were developed to help forensic investigators process digital evidence more efficiently and effectively and also overcome challenges such as large hard drives and evidence searching. The toolkits usually feature a user-friendly and clear graphical user interface (GUI) to assist the user locate potential evidence much promptly. Searching and indexing are optimised for fast searching of evidence from large amounts of data. EnCase and FTK are now becoming forensic proven software tools and commonly used in private and public sector for digital forensics investigation. A number of outstanding Linux and Unix based forensic tools with user friendly GUI have been developed, such as Sleuthkit, SMART and Helix (shown in Table 2.2). Farmer and Venema (1999) created a software toolkit called The Coroner's Toolkit (TCT) to respond to the lack of forensic software in UNIX platform. TCT (shown in Table 2.2) is capable of analysing all the activities in a live system and capturing all the current state information of the platform. However, this toolkit was not designed to produce court admissible evidence but to determine what happened on a compromised machine. A debate has arisen to discuss whether open source digital forensic tools can be used for digital forensic investigation. Kenneally (2001) and Carrier (2002) have published their articles to support the debate.

The popularity of the Internet has grown exponentially and crimes involving the Internet also have been increasing dramatically. The term network forensics has emerged. Cohen & Schroader (2007, p.172) define network forensics as the sniffing, recording, and analysis of network traffic and events. Progress has been made in innovation of network forensic tools. Sitaraman & Venkatesan (2006) maintain that several tools such as Snort, TcpDump, Pcap and NetAnalysis (shown in Table 2.2) can perform network forensic activities. Some commercial tools such as NetIntercept, SilentRunnder (shown in Table 2.2) provide integrated search, visualisation and comprehensive analysis features for forensic investigators to retrieve evidence from network traffic (Casey, 2004). Different forms of evidence in a networking environment post a challenge for digital forensics investigators because a single tool may not be able to support all types of evidence. Usually a combination of tools and excellent individual skills are required to extract and analyse different types of information.

Table 2.2 provides a list of products including software and hardware that are reviewed in Chapter 2. The purpose of the Table 2.2 is to make a ready comparison between different digital forensic tools. The digital forensic tools are listed and comparative data are provided to guide the research focus. Table 2.2 also helps the readers to have better understanding of the functionalities of the forensic software mentioned in this study.

Table 2.2

List of digital forensic software (Barbara, 2006, p.1)

Product Name	**Software Type**	**Description**
DD	Disk Imaging	DD is a common UNIX® program whose primary purpose is the low-level copying and conversion of raw data.
DiskEdit®	File Recovery	Recover deleted files
DIBS®	Forensic equipment	Industrial recognised forensic hardware toolkits. Evidences generated using these toolkits have never been rejected so far by court. (Adopted from DIBS, 2010)
EnCase®	Forensic Toolkits	• Its ability to support different operating systems and file systems • finding, parsing, analyzing, displaying, and documenting various types of digital evidences • Automatic report generation • Customize script language called EnScript to allow users to design their own scripts to fulfil individual needs. (Adopted from Guidance, 2010)
FTK®	Forensic Toolkits	Cutting-edge analysis, decryption and password cracking. Perform network-based, secure, single-system forensic acquisition of physical devices, logical volumes and RAM (Adopted from AccessData, 2009).
Helix®	Linux based forensics Live CD	With more than 35 forensic tools that can be used for incident response and forensic investigation. It's also able to wipe, recover data from slack space, and view the Windows registry. Open source applications are also included in Helix 3 to help digital investigation (Adopted from E-fence, 2009).
NetAnalysis®	Forensic toolkits	Provides Internet history analysis, view cache data, auto investigate feature and recover of deleted data (Adopted from Detective, 2010).
NetIntercept®	Host-based Network Forensic Tools	Capturing and storing network traffic, rebuilding and analysing of network sessions, retrieve data stored and view analysis results (Adopted from Sandstorm, 2009).
SilentRunner®	Network Analyser	It has state-of-war analysis and data-visualization tools. SilentRunner store selected packets and parses their contents to rebuild the files. The program can combine logs networking equipments like switches, routers and firewalls with saved information to provide complete and accurate

		network analysis (Adopted from PCMag, 2002).
iLook®	Disk imaging	Two major components IXimager and ILook v8. IXimager supports disk imaging of Windows and non-Windows devices. ILook v8 will run on both 32/64 Bit platforms and supports multiple file systems including FAT 12/16/32, NTFS, and Linux Ext2/Ext3 (Adopted from ForensicsWiki, 2010)
Pcap	Network traffic capturing	pcap (packet capture) is network capturing tools that can isolate packets headers and other information.
SafeBack®	Disk imaging	SafeBack is a DOS-based utility for backing-up and restoring hard disks. SafeBack can be used to create mirror-image (bitstream) backup files of hard disks. It can also make a mirror-image copy of an entire hard disk drive or partition.
Sleuthkit	Forensic Toolkits	The Sleuth Kit (previously known as TASK) is a collection of UNIX-based command line file and volume system forensic analysis tools.
SMART®	Linux Forensic Toolkits	• "Knock-and-talk" inquiries and investigations • on-site or remote preview of a target system • post mortem analysis of a dead system • testing and verification of other forensic programs • conversion of proprietary "evidence file" formats • baselining of a system
Snort®	Host-based Network Forensic Tools	Snort® is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) capable of performing packet logging and real-time traffic analysis on IP networks. Snort performs protocol analysis, content searching/matching, and is commonly used to actively block or passively detect a variety of attacks and probes, such as buffer overflows, stealth port scans, web application attacks, SMB probes, and OS fingerprinting attempts, amongst other features (Adopted from Sourcefire, 2010).
TcpDump	Network Forensic Tools	TcpDump is a command line tool used for network monitoring, protocol debugging, and data acquisition.
The Coroner's Toolkit (TCT)	UNIX® forensic toolkits	TCT components are the • grave-robber tool captures file information • ils and mactime tools can visualise and access patterns of files including deleted files • the unrm and lazarus tools recover deleted files • findkey tool recovers cryptographic keys from a running process or from files.
XtreeGold®	File recovery	XTree contained features like listing all files of a branch including subdirectories, listing of all files on a disk, or viewing a file's contents in

		text or hexadecimal format (Adopted from Wikipedia.org, 2010)

The current generation digital forensic tools have explicit limitations and performance issues. Traditionally, a single workstation is used to image the storage devices with a limited capacity. Using a single workstation to image hundreds of Terabytes (TB) of data is becoming completely inadequate and time consuming. Current generation digital forensic tools are never able to cope with the ever-increasing and massive data storage capacity (Roussev & Richard, 2006). A prototype of distributed digital forensics system has been developed to address the problem. Roussev & Richard (2004) have developed a Distributed Environment for Large-scale Investigations system (DELVs) to ensure even distribution of certain types of files across different workstations to maximise the usage of available Random Access Memory (RAM) when acquiring forensic images. Additionally, Solid State Drive (SSD) is the future storage device which uses memory as storage units and offers many advantages that traditional magnetic hard drives cannot match. There is no doubt that SSD will take over the market of magnetic hard drives when the price drops to an acceptable level. A few researches indicate that conducting forensics investigation in SSD is a challenge (Antonellis, 2008; Mitchell, 2009). The next generation of digital forensics tools will employ high performance distributed computing, sophisticated and automated data analysis techniques to discover potential evidence and cope with enormous data storage problem. Ayers (2009) proposed a few metrics that could be used to measure the next generation computer forensics analysis system. The study of the evolution of digital forensics tools can help this research understand the capabilities of various tools in the market.

2.2 LEGAL AND TECHNICAL IMPLICATIONS OF DIGITAL FORENSIC TOOLS

Tools for disk imaging form the foundation for examining digital evidence (Byers & Shahmehr, 2009). Tools that produce accurate, complete and reliable results are essential for the digital evidence to be acceptable by courts. There are legal considerations and risks that are associated with digital evidence. Most of the legal acts and litigation covered in this section are based those in the United States of America because of their advancement in the digital forensic technology and the growing number of cases and the advanced legal system regarding digital crimes. In order to clarify the considerations and risks of digital forensic tools, the definition and characteristics of digital evidence are covered in section 2.2.1. Admissibility, the most remarkable issue regarding digital evidence, is to be discussed in section 2.2.2, followed by the discussion in section 2.2.3 of the reliability of proprietary and Open source digital forensic tools. The digital forensic tools validation and verification covered in section 2.2.4 is to reveal the current state of the issue.

2.2.1 The Definition And Characteristics Of Digital Evidence

NIJ (2008, p. ix) defines digital evidence as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. Another definition for digital evidence proposed by SWGDE (2009) is that any information of probative value that is either stored or transmitted in a digital form. This means digital evidence can be any information that is electronically stored on computers and network storage media. Digital evidence has to meet various criteria before it is recognised as admissible in court. This is due to the characteristics of digital evidence as shown in Table 2.3.

Table 2.3

Characteristics of digital evidence (Compiled from Cohen, 2010; Lin et al., 2005, p.57; NIJ, 2008, p.ix)

Digital Evidence Characteristics	Description
1. Advanced Technology	Collection and analysis of digital evidence can be very difficult and often requires scientific technologies. Because of the constantly changing technology, the scientific methods used to collect and analyse digital evidence should change correspondingly.
2. Flexibility	Digital evidence consists of all kinds of electronic information such as images, videos, audios, text and also almost all patterns of traditional evidence.

3. Duplicability and Modifiability	Digital evidence can be easily changed, altered, stolen or duplicated without any trace. Information transferring across network can be lost or incomplete due to network failure.
4. Invisibility	During e-commerce, personal information such as IP address, web browser used, computer names will be transferred across the Internet. All the information can be considered as digital information if it is relevant and reliable.
5. Crosses jurisdictional borders	Digital crimes can happen anywhere. Different jurisdictions create extra barriers to prosecution of digital crime perpetrators.

The Table 2.3 describes five characteristics of the digital evidence in order to understand the admissibility of digital evidence in court and also why digital evidence has to go through different tests before it can be admissible in the court. The integrity and accuracy of the digital evidence can be easily compromised because of the characteristics. Admissibility of the digital evidence is discussed in the following section.

2.2.2 Admissibility Of Digital Evidence In Courtroom

US courts have a detailed and strict set of rules and policies regarding the admissibility of any type of evidence. There are three major guidelines that govern rules about handling digital evidence in US: the Federal Rules of Evidence, the Daubert standards and the case laws (Manes & Downing, 2009). Digital evidence is not unique and can be easily duplicated or modified without leaving traces therefore the admissibility of digital evidence is open to challenge.

From 1923 to 1993, admissibility of scientific evidence was tested by Frye standard which came from a case *Frye v. United States (1923)*. The Frye test held that expert testimony must be based on scientific methods that are generally accepted by scientific community. In 1993, Daubert standard (*Daubert v. Merrell Dow Pharmaceuticals, Inc., 1993*) replaced the Frye test as the standard for admissibility of expert evidence in federal courts. Under the Daubert standard, the United States Supreme Court ruled that the trial judge must serve as gatekeeper to scrutinize whether the evidence is not only relevant but also reliable (Adams, 2008). In other words, evidence must meet requirements of Federal Rules of Evidence 702. The rule 702 states that the expert testimony is based upon sufficient facts or data. The testimony is the product of reliable principles and methods and has applied the principles and methods reliably to the facts of the case. This rule suggests that scientific evidence is considered as competent and valid if the evidence is based on reliable scientific principles and methods. Daubert standard suggests that five factors should be considered when validating scientific evidence (see below bulleted list). In 1999, *Kumho Tire Co. v. Carmichael (1999)* case extended the applicability of Daubert approach to all non-scientific expert testimony. The court concluded that the five factors in the Daubert standard are not a definitive checklist. For example, the evidence that is not subject to peer review and publication should not be excluded from the case. Also, a theory or technique that is generally accepted by the scientific community does not mean the evidence is admissible in the court. Ryan & Shpantzer (2002) clarified that testimony may still be admissible by the court even if one or more of the Daubert factors are unfulfilled. Daubert Standard (*Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 1993, p.1) recommends the following five guidelines should be considered when evaluating the admissibility of the evidence:

- The theories or techniques utilised by expert witness have been tested.
- Subjected to peer-review and publication.
- Known or potential error rate and the existence.
- The existence and maintenance of standards and controls concerning its operation.
- Degree to which the theory and technique is generally accepted by a relevant scientific community.

In addition to reliability, the authenticity of the evidence is another criterion for the evidence to be admissible in court. Federal Rules of Evidence 901(a) (2007) defines evidence as sufficient to support a finding that the matter in question is what its proponent claims. In general, testimony clearly establishes that the exhibits presented as evidence are identical to the original and the content has not been changed by any means. Ridder (2009) describes that when trained law enforcement investigators gather evidence, they should eliminate problems that compromise evidence authenticity. For example, authentication of a duplicate hard drive mirror image can be achieved by a proven time-stamping technique. A hash value can be computed for both original and duplicate copy of mirror images. Both hash values must be the same to verify that both images are identical. A court case *United States v. Liebert* (3rd Cir. 1975) argued the exhibit presented as evidence against him should not be admissible because of the duplicability and modifiability nature of digital evidence. The argument presented in this case showed that the evidence obtained from an investigation must be properly authenticated before it can be admissible in court.

In conclusion, admissibility of digital forensic evidence must meet three requirements: first the evidence must be relevant to the case investigated, second it must be obtained with scientific methods, and third it must be confirmed by proper validation. The criterion is reliability when the evidence is regarded as admissible (Ryan & Shpantzer, 2002). When developing and using digital forensic tools that might be producing digital evidence that are introduced to court, these requirements must be considered.

2.2.3 Open Source and Proprietary Digital Forensic Tools

The fundamental principles of Daubert guidelines and other requirements of admitting evidence in the court are covered in section 2.2.2. Digital forensic software is a tool that assists digital investigators to acquire or locate potential digital evidence. The validity of digital forensic software must be fully assessed before the evidence is treated as admissible. Carrier (2002) and Dan et al. (2007) raised an argument of whether digital forensics using Open source tools would be better. Goel (1985) defined that software reliability is satisfied if software faults do not cause a failure during a specified exposure period in a specified environment. Understandably, unreliable digital forensic software will lead to untrustworthy results and may jeopardise the whole forensics investigation.

It is important to distinguish between Open source and Proprietary Software. The central defining point of Open source and Proprietary software is the availability of the source code. Open source software allows open access to the source code whereas Proprietary software makes their source code unavailable to the public. Some prominent examples of Open source software (OSS) include Ubuntu, Apache web server, Firefox web browser, and MySQL database. The counterpart proprietary software, also known as closed-source software, includes Microsoft® Office, Adobe® Photoshop, AccessData FTK® and Guidance software Encase®. Digital forensics software is available in both Open source and Proprietary software. Currently, there is a gap in the digital forensic industry. There is no program or project that focuses on testing the OSS to determine whether they function as supposed. Testing Open source disk imaging tools is what this dissertation will pursue.

There are many arguments and misconceptions of both OSS and proprietary software regarding the reliability. Source code made available to public can attract attackers to search and exploit vulnerabilities to achieve their goals (Boulanger, 2005). According to the OSS development process, source code publicly available can be evaluated by other developers. If problems or vulnerabilities of the software are identified, other developers would report them and the software programmers will analyse the problems and provide solutions to these problems. Collaboration of different efforts from large number of developers will make software much more reliable and secure than Proprietary software. Waring & Maddocks (2005) stated that this can also be enhanced with the availability of the source code to other programmers who can identify problems and propose solutions. Also, there five present research cases of UK public sectors adopted OSS and this indicate that reliability is a benefit to their organisations (Waring & Maddocks, 2005). Furthermore, OSS considers peer review procedure to have a central role in their development process. The peer review procedure also complies with the Daubert guidelines factor 2 as the evidence has subjected to peer reviewed and publication. Some people argue that peer review process of OSS is not effective as it is claimed to be. Viega (2000) raised an argument that source code open to the public does not automatically guarantee the code will be reviewed and analysed by competent developers. For example, a bug in Berkeley Software Distribution (BSD) UNIX caused a simultaneous file access conflict issue, that existed in the system for over 25 years (Perrin, 2008).

On the other hand, Payne (2002) suggested that the argument must always be taken with “a grain of salt” because a system such as Sun Microsystems Solaris is considered as reliable while operating as a closed source. Evidence can be found that closed source Proprietary software has less security vulnerabilities than OSS if we take

Apache web server and Microsoft Internet Information Services (IIS) as examples. Reichenkron (2006) presented evidence that the Apache web Server has more vulnerabilities than Microsoft IIS. Payne (2002) presented another argument that OSS is easily subjected to malicious code planted in the software. Most of OSS projects use Concurrent Versioning System (CVS) to keep track of project progress, publish new versions of the software and collaborate with multiple developers. Projects like the Apache web server will only publish patches or fixes to the public from trusted developers or submissions after careful examination and extensive testing.

Boulanger (2005) presented another argument claiming that hiding the source code does not provide additional security. A common way of looking for vulnerabilities is to send or input unexpected commands or codes to test the validation mechanism of the software. Knowledge of the source code is not required. If the software does not respond with a correct exception, this might indicate the existence of vulnerability in the system. For example, an online e-commerce website usually has customer login and password protection. If the web server did not implement proper input validation mechanism, the attacker may launch an attack like Structured Query Language (SQL) injection to exploit vulnerability to query sensitive and valuable information from the back-end database. Grossman (2007) reported that SQL Injection attack has been classified as one of the top ten website vulnerabilities.

Vulnerability can be discovered much faster in OSS than in Proprietary software. Raymond (2002) postulates the bug discovering in OSS as “Given enough eyeballs, all bugs are shallow”. In matter of days or even minutes, software bugs are to be reported once software is released or updated. For proprietary software, it can only wait for the vendor to release patch to fix the problem. In some cases, vendor may not even release a patch for a small problem because the problem may require huge effort to fix and it is not cost efficient. However, OSS may have a few options. If the vendor does not release patch for the problem, it is not unusual that some developers will program their own fix and release their products to the public. In some rare cases, no other developers offer any fix to a particular problem. Users still have options to develop their own patch to fix the problem but for proprietary software these options simply do not exist.

Only a limited number of arguments have been discussed about the reliability OSS and Proprietary software. The debate between supporters of OSS and Proprietary software has been continuing for decades and there is no obvious conclusion. Testing the validity of disk imaging tools demands further studies, as digital forensics is still an immature field.

2.2.4 Verification And Validation Of Digital Forensic Tools

Section 2.2.1 and 2.2.2 have discussed the legal implications of digital evidence. Digital forensic practitioners are relying on automated software tools to acquire and analyse digital evidence. The reliability of the digital evidence is determined by the completeness and accuracy of the tools employed by the forensic investigators. Imperious demands are raised by law enforcement, the intelligence community and other government agencies to verify and validate the validity of digital forensic tools. Rogers & Seigfried (2004) and Etter (2001) have pointed out that forensics tool testing or validation is one of the challenges or issues in forensic science research. The outcome of Daubert guidelines also indicates that the forensics tool must be validated if they produce evidence that is introduced to court.

2.2.4.1 Background of Verification and Validation (V&V)

Software Verification and Validation (V&V) concept emerged in late 1960's. V&V is one of the disciplines in software engineering that embeds the quality assurance process throughout the lifecycle of software development. V&V examines and analyses whether the functions of the software are working correctly and running as expected (Wallace& Fujii, 1989). Many models and standards have been developed over the years such as IEEE Software V&V standard 1012-2004, 1059 and 1074. The standard outlines the plan, process and documentation requirements of V&V (Rohilla & Malik, 2008). According to the IEEE (1990) Standard Glossary of Software Engineering Terminology, Validation is defined as "The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements" (p. 80).

In other words, the developed software should satisfy the pre-determined requirements. With regarding to the digital forensic tools, it confirms whether the forensic tools, process or procedure are functioning as intended. IEEE (1990) is defined Verification as "The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase" (p. 81). Verification can be interpreted as a process that makes sure the software tools conform to the specifications. With regard to the digital forensic tools, Guo et al. (2009) interpreted Verification as using laboratory tools, techniques and procedures to confirm that the software meets the specifications. The software V&V standard provides a foundation for forensic sciences to adapt the well-established model to its own requirements.

V&V must be tested or evaluated under a set of carefully designed requirements and procedures. Software testing can be categorised into two groups: White box testing and Black box testing. White box testing is appropriate if the examiner has access to the internal structure of the software but this is unrealistic in forensics industry. The mainstream forensic tools used by the Law enforcement or intelligence agencies are closed source proprietary software. The source code or the internal structure of proprietary software is maintained as trade secret to the public or to the law enforcement. On the other hand, Black box testing evaluates the software by comparing actual output against its expected output. The method of Black box testing can be applied to both open source and proprietary software. In the context of digital forensics, Black box testing is involved using the forensic tool to perform a series of pre-defined tasks under different testing scenarios. For example, the task is to use the forensic tool to acquire a hard disk using different hardware interfaces (USB, SATA, IDE and Firewire). The successful outcome of the test scenario suggests that the tool is validated for the given task under the specified conditions and environment. However, the confidence may not be extended to the environment or condition that is not covered in the given task.

2.2.4.2 Existing Work Of Forensic Tool V&V

CFTT is one of the programs that has dedicated much effort to evaluate the validity of the digital forensic tools. CFTT developed testing methodologies for each function that the digital forensic investigation may involve. The methodology of CFTT is belongs to Black box testing. Total of seven categories have been identified, such as disk imaging, hardware and software write block, forensics media preparation. In each category, detailed test plan (NIST, 2005), specification (NIST, 2004), assertions and support software are developed. Disk imaging and Write block are the most well-established and documented categories and many mainstream software and hardware are tested. For example, test result disk imaging software EnCase 6.5 (NIST, 2009), FTK Imager (NIST, 2008) and Write block device Tableau Forensics bridge (NIST, 2007). The tests performed by the CFTT are rigorous and is also extremely difficult for other organisations to replicate due to the amount of tasks that are required. The number of forensic tools is also overwhelming.

Another notable effect comes from the research group SWGDE. Instead of developing test specifications, plan, assertions like NIST, SWGDE (2009a) developed validation testing guidelines and templates that might be helpful to the interested parties or law enforcement agencies that undertake forensic tools validation. The guidelines recommended by SWGDE include the test purpose, scope, methodology, choices of test cases.

An independent researcher, Brian Carrier, has developed different test images to validate and verify the digital forensic tools. The test images can provide help to observing the behaviour of some key functions of the tools. Carrier (2005) described that the purpose of these small test images is to address the needs for developing some not too complicated and lengthy public tests. However, the numbers of test images is very limited and they are not enough for a comprehensive review of different tools.

Byers & Shahmehri (2008a) from the Swedish National Laboratory of Forensic Science have developed a systematic approach to evaluate the selected disk imaging software. The evaluation process is similar to the CFTT program but not identical. Their research has identified a set of technical variations that are the different contexts that the tool may encounter. It links the technical variations to the testing requirements to reveal more potential test cases for testing. The research identified several shortcomings of the evaluation methodology of the CFTT program. The research from Byers & Shahmehri (2009) provided deeper analysis of each test result than CFTT. Byers & Shahmehri (2009) also pointed out that CFTT has missed the area of usability of the tool.

Guo et al. (2009) have proposed a functionality driven approach for digital forensic tools V & V. The methodology has focused on measuring the accuracy and precision of the testing results. They identified several functional categories and also the components of each sub-category through the method referred as function mapping (Guo et al., 2009). Function categories have been identified, including search function and forensic copy function (Guo & Slay, 2010). After the function mapping, V & V requirements are specified. A typical group of reference sets that consist of different test scenarios is then developed. After the reference sets are confirmed, the task of V & V the defined function of digital forensic tools is conducted. Both functional requirements and reference sets are built in an extensible way that will enable tool testers to extend them to fulfil their special test requirements (Guo et al., 2009).

2.3 DEFINE DISK IMAGING TOOLS

A comprehensive understanding of digital forensic tools enables this research to better define disk imaging tools. Sadui (2001) from SANS Institute defines disk imaging as an image of the whole disk where the complete content of the disk is copied including the location of the data. Some types of validation mechanisms are provided to prove that the copy is exact and has not been altered. This is different from the normal computer backup. Disk imaging creates a bit-stream of the duplicate of original data (SWGDE, 2009). In other words, ambient or residual data such as deleted files, unallocated spaces, and file slack will be copied as well. The reason of creating forensic image of the original evidence is that the original evidence must be preserved without being altered or tampered. Schweitzer (2003) also emphasises that forensic examination needs to be conducted using only the image (copy) and not the original hard drive. Also, according to Federal Rules of Evidence 901(a), the forensic image copy must be authenticated and proven as same as the original copy in order to be admissible as evidence.

2.3.1 Attributes Of Disk Imaging Tools

NIST (2005) suggests that two critical measurable attributes of the disk imaging process are accuracy and completeness. NIST (2005) further defines accuracy as a qualitative measure to verify whether each bit of data of the forensic copy is matched to the corresponding bit of the source. Completeness is a quantitative measure to verify whether every bit of source data is imaged (NIST, 2005).

There are several factors that affect the two attributes outlined above. In order to access the evidence contained in a physical disk, the disk needs to be connected to the computer via a physical interface. The Physical interface of a hard disk may vary for different devices, such as, Integrated Drive Electronics (IDE), Small Computer System Interface (SCSI), Serial ATA (SATA), Universal Serial Bus (USB), IEEE 1394 and eSATA. Each interface may have different variants or revisions with very different specifications to those of its predecessor. For instance, ATA-6 standard allows 48-bit Logical Block addressing (LBA) which has maximum disk size 128 Petabyte (PB) whereas ATA-1 standard only allows 28-bit LBA. A disk imaging tool must be able to recognise different interfaces in order to access the physical disk. Another factor that might affect the completeness of the forensic image copy is to identify the true size of the physical disk. A host protected area (HPA), sometimes known as hidden protected area, exists in some hard disks and is an area that is not normally visible to the operating system. Gupta et al. (2006) raise concerns in HPA for digital forensic investigators given the potential of hiding data.

2.3.2 Mandatory Features Of Disk Imaging Tools

According to the disk imaging tool test specification from NIST (2004), some requirements are mandatory for disk imaging tool and are summarised in Table 2.4. NIST (2004) also include many other additional requirements that might be useful for this research. Byers & Shahmehri (2009) also identify some extra requirements based on NIST (2004) with further interview and discussion with industry experts. Further requirements identifying how investigation proceeds are reviewed and presented in chapter 3.

Table 2.4

Mandatory features of Disk Imaging Tools (NIST, 2004, p.8)

Requirements	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 & 05	The tool shall completely acquire all visible and 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 while reading from a digital source then the tool will notify the user of the error type and the error location.
DI-RM-08	If there are unresolved errors while reading from a digital source then the tool will notify the user.

2.3.3 Current Disk Imaging Tools

The purpose of surveying different disk imaging tools is to understand the state-of-the-art of the tools and filter out the best available tools to conduct performance evaluations on them. There are two types of disk imaging tools in the market, namely hardware-based and software-based. Hardware-based disk imaging tools usually have much better performance over software-based disk imaging tools. Corresponding to the performance, the cost is much higher than the software-based disk imaging tools. Hardware disk imaging tools usually come in a toolkit style with plenty of accessories such as different types of physical interfaces, adapters and cables to acquire different type of devices. Hashing verification, write blocking and read multiple devices simultaneously are the common functions hardware-based disk imaging tools (see Table 2.5) will provide. Logicube Talon, HardCopy 3 from Voom Technologies, Data Copy King from SalvationDATA and TableauTD1 from Guidance Software are some commonly used hardware disk imaging tools.

An alternative to the pricey Hardware-based disk imaging tools are Software-based solutions. The most commonly seen file copying program is DD and it was first released as a utility of UNIX. DD is one of the oldest imaging tools and it produces raw image format.

Table 2.5

List of Example Hardware-based Disk Imaging Tools

Product Name	**Make**	**Description**
Talon®	Logicube	Talon® simultaneously images and verifies data at up to 4 GB/min. The handheld system captures IDE/UDMA/SATA drives, and can capture SCSI drives via USB cable. Capture directly from desktop/laptop PCs and MAC computers (via PC interface) using the Forensic cloning software included with the Talon.
HardCopy 3	Voom Technology	Duplicate to 1 or 2 destination drives at up to 7.1 GB/min. with no slow down. Clone entire drive or select Image option to chunk data into a file or files. Purchase preloaded with MD5 and SHA256 verification; select 1 or 2 passes. Minimal training required. Field upgradable.
Data Copy King	SalvationData	Access to unstable drives with a lot of bad sectors and copy data fast. Automatically resets/reboots drives that get stuck to continue the data duplication process. Sector by sector copy and synchronous CRC checking.
Tableau TD1	Guidance Software	Disk-to-Disk and Disk-to-File Duplication, Format Disk, Wipe Disk, Hash Disk (MD5 and SHA-1), HPA/DCO Detection and Removal, and Blank Disk Check.

Many variants have emerged after DD to fit the purpose of forensic disk imaging. Apart from DD, some other disk imaging tools are developed based on a proprietary or open source format. The following sub-sections will discuss some of the popular open source and proprietary disk imaging tools in details.

2.3.3.1 dcfldd

Disk imaging tool dcfldd is developed and maintained by Nicholas Harbour who used to work for the Department of Defence Computer Forensics Lab. Dcfldd is an improved version of GNU dd with elements of digital forensics (Harbour, 2006). One of the improved features for forensics is hashing on-the-fly which allows hashing the input data while it is being transferred. Dcfldd can also verify an image to check whether it is a bit by bit match to the source. It can also split output or output the image to multiple locations.

2.3.3.2 dc3dd

Dc3dd is another enhanced version of existing DD program. It is developed and maintained by the US Department of Defense Cyber Crime Centre. Most of the features were inspired by dcfldd and modified for dc3dd (Kornblum & Medico, 2009). The major improvements over the original DD and dcfldd programs are the performance improvements, sector error recovery, detailed logging, error sector reporting and log file appending (Kornblum & Medico, 2009).

2.3.3.3 Helix 3 Pro

Helix 3 is compatible in multiple platforms and has several open source forensic applications to assist digital forensic investigations. Many open source applications are built in a bootable Live CD. Helix 3 Pro has a simple to use interface and it can boot to any x86 system in a forensically sound manner. Helix 3 Pro supports DD and Encase version 4, 5 and 6 imaging formats. Volatile data collection option is also available in Helix 3 Pro. Helix 3 Pro also compiles report with detailed data collection results.

2.3.3.4 Automated Image and Restore (AIR)

AIR is a GUI tool for DD/dc3dd with specific design for creating forensics images in a simple way (Gibson, 2010). It supports dd/dc3dd image formats and the block size is customisable. AIR detects wide range of devices such as IDE, SATA, SCSI and tape drives. It provides many choices of Hash algorithms such as MD5, SHA1/256/384/512 and Gzip/bzip2 compressions. AIR can split images into multiple segment parts for better storage option and image over a data network via encrypted or unencrypted connection. It can also wipe devices into specific patterns.

2.3.3.5 Aimage (Part of AFF Library)

Aimage is part of tool libraries of Advanced Forensic Format (AFF) which is open source forensic software. It is capable of creating files in dd, AFF, AFD or AFM formats and supports compression and uncompression. The AFF is a smart, tested system for creating and acquiring forensic disk images (Simson, Malan, Dubec, Stevens, & Pham, 2006). Aimage can recover a device with bad sectors or blocks and has similar recovery mechanism as dd_rescue. Byers & Shahmehri (2009) stated that aimage is a promising tool but the documentation and support are very limited which makes the validation difficult. The usage of this tool is still very limited in the current digital forensic practices.

2.3.3.6 Windows-based Imaging tools

Most windows-based imaging tools offered are proprietary and packaged inside a toolkit. Some commonly used tools are EnCase, FTK Imager, Forensic Replicator from Paraben, WinHex from X-way Software and ProDiscover® Forensics. AccessData made FTK Imager as a separate program that is available as freeware and comes with excellent support and documentation. The Lite version of FTK Imager does not require installation and it can be integrated into a collection of forensic tools. Due to the limited timeframe and budget of this research, proprietary disk imaging toolkits are not considered in this research.

2.3.3.7 Macintosh Imaging tools

Apple computers are becoming more popular. The latest electronic devices iPhone and iPad have sold tens of millions units in the consumer market. However, the field of Macintosh forensics is still growing and only a handful of companies have developed forensic software that targets Apple devices. BlackBag Technologies and MacForensicsLab are two leading companies that specialise in Macintosh Forensics.

2.3.4 Problem Areas In Disk Imaging Tools - Data Hiding

Data Hiding is an anti-forensic technique that has existed for as long as there have been digital computers. The technique has been further utilised by sophisticated criminals and hackers to conceal incriminating data in the storage device to avoid detection by digital forensic tools. Data hiding is also a major hazard for the law enforcement conducting forensics investigation. Berghel (2007, p.18) has presented eleven possible locations to conceal data in a disk drive. Slack spaces, unallocated space and unused space are the most common locations to conceal the data. However, some special tools may require storing data in these locations. On the other hand, Host Protected Area (HPA) and Device Configuration Overlay (DCO) area are more commonly used in today’s computing world. Typically, HPA and/or DCO can be located in laptop computers. Computer vendors usually create HPA or DCO reserved area to backup their Proprietary software or operating system for the purpose of diagnostics, manage or update users' computer systems. It is designed in a way that it is not easily be accessible, modified or deleted by normal users. Basic Input/Output System (BIOS) and Operating system normally cannot access these areas and it is restricted by the disk controller. HPA and DCO areas are one of the testing subjects in this research.

2.3.4.1 Host Protected Area (HPA)

HPA was first introduced in ATA-4 standard in 2001. HPA is located at the end of the disk. The starting address of the HPA is the maximum addressable sector plus one. There are three AT Attachment (ATA) commands (IDENTIFY DEIVCE, SET MAX ADDRESS and READ NATIVE MAX ADDRESS) that are involved in implementing an HPA area. Meyrick (2006) has demonstrated how an HPA can be created. First, IDENTIFY DEVICE is used to query the true size of the disk drive from the IDE/ATA hard disk controller. Command READ NATIVE MAX ADDRESS can also be issued to query the true size of the disk drive and this command will always return the true size of the drive even when the drive has been compartmentalized by HPA. Then, SET MAX ADDRESS command is issued to the controller to reduce the size of the drive to less than its true size. If command IDENTIFY DEVICE is used to query the size of the drive, the Registers of the ATA controller will return the reduced size of the hard drive due to the existence of the HPA. In addition of the commands described above, the ATA-6 standard (Technical Committee T13, 2001) introduced 48bit Logical Block Addressing (LBA) which enables the faster data access and maximum size of the hard drive up to 144 petabytes. ATA-6 also introduced another command SEX MAX ADDRESS EXT when 48 bit LBA addressing is implemented. SEX MAX ADDRESS and SEX MAX ADDRESS EXT are also used to reset the hard drive to its true size or native size. Modern hard drives with IDE interface are built to conform to ATA-6 or later standard. Hard drives with SATA interface are built to conform to ATA-7 or later standard. Software such as hdparm, The Sleuth Kit, ATA Forensics Tool can be used to identify or detect HPA area in the disk drive. Creating and implementing HPA in the hard drive can be done by tools such as HDAT2, MHDD and hdparm.

2.3.4.2 Device Configuration Overlay (DCO) Area

DCO feature was introduced in ATA-6. DCO is used by computer vendors to configure their hard drives to exactly the same number of sectors even when the drives are from different manufacturers and sizes (Gupta et al., 2006). Commands DEVICE CONFIGURATION SET, IDENTIFY AND RESTORE are introduced to create and manipulate DCO. Command DEVICE CONFIGURATION SET is used to reduce the size of the hard drive like commands SET MAX ADDRESS and SET MAX ADDRESS EXT in HPA. DCO command cannot be executed at where the drive has HPA in place. DEVICE CONFIGURATION RESTORE command is solely used to remove DCO. This command cannot be used to remove HPA. DCO and HPA can co-exist on the same hard drive (Gupta et al., 2006). However, a DCO area must be set before an HPA can be configured.

Software tools such as hdparm and FastBloc® software edition can be used to detect and manipulate the DCO area. FastBloc® Software Edition developed by Guidance software claims that it supports HPA and/or DCO detection and removal. However, Guidance software (2010, p.567) warns that using FastBloc® software edition to remove DCO or combination of DCO and HPA will permanently alter the hard disk. The HPA area can be removed temporarily but the disk is not permanent modified. Nevertheless, modifing DCO or the combination of DCO and HPA will modify the disk permanently. The controller settings of the hard drive is altered even the data contained in the drive is not been changed. Guidance Software (2010, p.567) states that there is no known way to access an entire hard drive without making such change. Unfortunately, FastBloc® Software Edition is not available in our laboratory.

2.3.5 Problem Areas In Disk Imaging Tools - Master Boot Record (MBR) & GUID Partition Table (GPT)

An MBR contains 512-byte boot sector located in the first sector of a hard drive. MBR holds the primary partition table and contains boot code, four primary partition records and an MBR signature. Detailed discussion of the structure of MBR is beyond the scope of this research. The maximum capacity of MBR supports up to 2.2 Terabyte (TB) because the partitions' start address and partition length are both fixed at 32 bits.

Also, MBR disks only support four primary partitions. In today's hardware products, 2 TB hard drives have become more affordable and common. It is only a matter of time, when 2 TB or larger hard drives will become the mainstream products in the market. In order to solve the limitations and problems with MBR, GPT is developed to replace MBR partition tables. The maximum disk size can go up to 9.4 billion TB and it supports 128 partitions by default. GPT also provides CRC32 checksums and backup utility to maintain the integrity of the partition table and header. GPT is widely supported by popular operating system vendors such as Apple OSX, Microsoft Windows and Linux. GNOME Partition Editor (GParted) and Windows Disk Management Tool support GPT creation and manipulation (Smith, 2009). GPT is more popular in current Apple Intel-based computers. With millions of Apple Intel-based computers have sold and the increasing usage of massive storage devices, GPT will become the mainstream partition scheme.

What's the implication of GPT for forensic tools? The support of GPT in forensic tools industry is still growing (Nikkel, 2009). Popular forensic tools such as Encase and FTK can recognise and provide access to a GPT disk. However, more improvements can be made to decode the GPT headers and entries, provide information about the backup GPT and GPT checksums (Nikkel, 2009). Part of this study aims at finding out whether the selected disk imaging tools are able to acquire a GPT disk and partition in complete and accurate manner. Nikkel (2009) has described that a full disk or a single partition acquisition can be done the same way as other partition schemes (DOS or BSD) or traditional MBR partitions.

2.3.6 Problem Areas in Disk Imaging Tools - Hash Function

Cryptography Hash function has a wide range of applications. For example, it identifies and classifies electronic information, authenticates data integrity and online security. One-way hash function is commonly used as a method of authenticating and verifying the integrity of electronic information. Hashing function has two very unique characteristics that are concern of to digital forensics. Thompson (2005) explains that it is computationally infeasible to derive or obtain any information about the original contents from the hash value and to have two pieces of content that have the same hash value. The hash function provided by the disk imaging software will ensure that the images or the clone copy created are exact duplicates of the original drive (Wang, Lai, Feng, Chen, & Yu, 2005, p.123). Comparing the hash value generated from the original content and the hash value derived from the image files will certain that the two copies of data are identical. In other words, the integrity of the original and imaged data is ensured. The most popular Hash functions adopted by disk imaging tools are Message Digest 5 (MD5), Secure Hash Algorithm version 1, 256 and 512 (SHA-1, SHA-256, SHA-512).

Hash function is built on the concept of collision-resistant. However, Wang, Feng, Lai, & Yu (2004) and Wang et al. (2005) have presented some popular hash functions that could generate same hash value on two different inputs. Malinowski & Noble (2007) referred the collision problem or hashing attack as “pigeon-hole problem” and that the problem exists in any algorithm. What are the ramifications of this problem to digital forensics? Thompson (2005) presents three arguments that the research of hash function collision problem should have little impact in computer forensics where the hash function is being used as method of evidence authentication. Firstly, the collision problem presented by Wang et al. (2004) can only be produced in a very particular piece of input content. Secondly, the hash function MD5 is not vulnerable to a brute force attack. It is still infeasible to alter the content of an input message and the hash value of the new message still to match the pre-calculated hash value on the original content. Furthermore, the chance of the collision attack is incredibly small and the problem presented by Wang et al. (2004) requires specific type of data and environment to occur.

2.4 THE FUNCTIONALITIES OF SELECTED DISK IMAGING TOOLS

Three disk imaging tools are selected for performance testing and their functionalities and advantages are discussed below and summarised in Table 2.6.

FTK Imager is a disk imaging tool provided by AccessData as a freeware. FTK Imager is an important component of the FTK toolkit, a world-class digital forensic tool. Evaluating FTK Imager will create a comparison baseline to the CFTT program to determine the accuracy of the project testing environment.

Table 2.6

Functionalities of Disk Imaging Tools (Compiled from Gibson, 2010, p.1; AccessData, 2007, p.31)

Functionalities	FTK Imager Version 2.9.0	Helix3 Pro	Automated Image and Restore (AIR) Version 2.0.0
Software Type	Freeware	Commercial	Open source
Platform supports	Windows & Linux	Windows, Linux and Mac	Linux
Support physical Interfaces	IDE, SATA, SCSI, USB, IEEE 1394	IDE, SATA, SCSI, USB, IEEE 1394	IDE, SATA, SCSI, USB, IEEE 1394
Partition format supports	NTFS, NTFS compressed, FAT 12/16/32, and Linux ext2 & ext3, HFS, HFS+	NTFS, NTFS compressed, FAT 12/16/32, and Linux ext2 & ext3	Linux partitions and more
Support image format	Encase, SMART, Snapback, Safeback (up to but not including v.3), and dd	Encase, dd	dd & dc3dd
Image copy compression/ decompression	PKZIP, WinZip, WinRAR, Gzip, and TAR compressed files	PKZIP, WinZip, WinRAR, Gzip, and TAR compressed files	Gzip and bzip2
Uses MD5 Hash	Yes	Yes	Yes
Uses SHA1 Hash	Yes	Yes	Yes
Can verify image integrity	Yes	Yes	No
Split images into segments	Yes	Yes	Yes
Logging	Yes	Yes	Yes
Wipe disk drives or partitions	Yes	No	Yes
Access HPA	Unknown	Unknown	Unknown

Helix 3, the most popular compilation of digital forensics on a bootable Live CD provided by E-fence and it was available publically as freeware until March 2009. Helix3 has been adopted as one of the digital forensics software suites in SANS Computer Forensics teaching course 508 (SANS, 2009). Helix 3 is also a tool of choice of Canadian Lead Security Agency (Webber, 2009). Darknet (2006), one of the best security websites, has rated Helix as top 10 best security Live CD distributions.

Automated Image and Restore (AIR) is an important constituent of the CAINE (Computer Aided Investigative Environment) project. CAINE is a specialised digital forensics environment based on GNU/Linux Ubuntu distribution. It offers a complete interoperable forensic environment that supports the collection, examination, analysis and reporting phases of digital investigations. CAINE provides a user-friendly graphical interface and the most important advantage of the project is that is Open Source and completely free. As Helix has become payware, CAINE has been nominated as an alternative to Helix3 as a popular free digital forensic toolkit (Gleason, 2009).

This research has a very limited budget and the choice of the disk imaging tools are tending to open source software or freeware. The selection of the disk imaging tools is also base on their functionalities provided. The candidate disk imaging tools must be satisfying the fundamental requirements defined in Appendix 2. The selection is also base on the availability of the software and the testing environment. For example, Mac OS X environment is not available for testing and the disk imaging tools that operating solely in this environment is not included in this study.

2.5 SUMMARY OF KEY ISSUES & PROBLEMS

The history of computer forensics can be traced back to 1970's and yet it is still an immature field. Computer technology has been more commonly used in people's daily life and its greater usage can lead to a great increase in court cases that involve the use of digital evidence.

The complexity and difficulty have significantly increased for digital investigations due to the large amount of data involved in today's computing environment. Also, digital crimes can be remotely triggered and their investigations may cross multiple-jurisdictional borders with an unknown number of suspects. Many research groups, government sections and organisations have attempted to build standardised frameworks for digital investigation. However, a globally recognised investigation framework is yet to be established. A standardised scientific approach for digital investigation must be built to provide the foundation or common practice for digital investigation to identify any misconduct and malpractice. Standardised investigation processes provide a legal basis for any court proceedings that raise arguments against the investigation process. A comprehensive investigation approach will help to identify whether all the elements are discovered during the investigation. If any steps are neglected, it may affect the result of the digital investigation and lead to question the validity of the digital evidence presented. The issue of investigation process and standardisation is covered in section 2.1.2.

The current generation of digital forensics tools have certain limitations. It is not efficient to process investigation data at a single workstation, considering the limited capacity of the data storage device today. More powerful computers must be used to process a large amount of data efficiently. Otherwise, a new data acquisition approach must be used to cope with the ever-increasing data capacity. Another issue with current digital forensics tools is the technique used to analyse digital photographs. The current approach is that digital investigators virtually identify the potential evidence from a large number of photographs but this will become impossible for millions of photographs. A new technique is required to dynamically identify potential evidence if certain search requirements are provided. The discussion of problems and issues of digital forensic tools is presented in section 2.1.3.

In the use digital evidence, users are concerned with the issue of whether the evidence is admissible in court. In US courts, the Daubert standard is currently in practice to determine the admissibility of the digital evidence. The digital evidence presented in court must be relevant to the case and the evidence must be extracted by scientific methods. Scientific methods comprise as investigation processes that are reviewed in section 2.1.2. A comprehensive and standardised scientific approach can establish the foundation that successfully allows evidence to be admissible in court. Also, appropriate validation of digital evidence must be performed as well. Digital evidence can be easily modified, altered or duplicated. If evidence has passed appropriate validation this ensures its accuracy and completeness.

Ensuring the reliability of the digital evidence produced by digital forensic tools is a vital issue that requires comprehensive study and research by both industry and academia. Unreliable digital forensic tools may lead to the original evidence being compromised which may further affect the admissibility of the digital evidence presented in court. In relation to the digital evidence, corresponding laws and guidelines are identified and discussed in section 2.2. Application of open source digital forensic tools in digital investigation has been questioned. However, open source digital forensic tools still have advantages that proprietary software does not have. A complete understanding of the reliability of digital forensic tools helps further define the mandatory requirements of disk imaging tools. The requirements will determine the required functions for a disk imaging tool and provide the foundation of tool testing requirements. Many digital forensic tools are still yet to be verified and validated before they can be used as forensic tools in the field. A standardised digital forensics tool verification and validation framework or procedures are yet to be established. Several issues and problems regarding digital forensic tools have been raised and developed in Chapter 2. A summary of key issues and problems are discussed in this section to provide a snapshot of the current trends in digital forensics.

2.6 CONCLUSION

Chapter 2 focuses on reviewing the contexts and discussions relevant to the evaluation of digital forensic tools. A comprehensive overview of the digital forensic environment has been developed. The overview covers the differences between computer forensics and digital forensics, Investigative Processes & Standardisations and most importantly the development and evolution of digital forensic tools. It shows the development, the most popular tools and problems of digital forensic tools. Digital forensics tools verification and validation are studied and discussed regarding the current trends in the industry.

The review covers background studies of digital forensics, the legal and technical issues of digital forensic tools. Digital evidence is defined in order to further analyse its admissibility regarding legal standard and Daubert guidelines of the United States of America. In relation to that, the reliability of digital forensic tools is discussed with respect to the perspectives of open source and proprietary software. Arguments between open source and proprietary software are presented. With the studies and discussions, the required attributes and requirements for disk imaging tools and choices of selected disk imaging tools are defined.

In order to study and test the reliability of the selected disk imaging tools, five relevant articles are to be reviewed and studied to find that how other researchers conducted similar research. Research questions and hypotheses can be defined in the problem areas identified in this chapter for disk imaging tools. In Chapter 3, the problems and issues that arise from the use of tools and technology will be discussed and specified to discover which tools are researchable. Subsequent data collection, processing, analysis and presentation methods can be found in the second part of Chapter 3.

Chapter 3

Research Methodology

3.0 INTRODUCTION

The literature survey in Chapter 2 has critically reviewed a set of articles related to digital forensic tools. The literature review has identified crucial factors that could affect the validity and the features of the disk imaging tools. In Chapter 3, the main research objective is to identify and construct a conceivable research method that can be used to investigate the relationship between the identified factors and the validity of disk imaging tools. The two factors related to the reliability of the disk imaging tools are completeness and accuracy.

In the development of the research model several steps must be prepared to empirically test the model. At the early stage of the research, disk imaging tool test requirements are derived from the standardised approach of the industry. The test requirements derived will provide the foundation for designing suitable test scenarios and assertions. Each selected disk imaging tool will be matching multiple test scenarios according to its functionalities. Each test scenario includes multiple test assertions that must be tested to confirm the selected tool has conformed to test requirements. After the test requirements are confirmed, test cases and test assertions are decided. The data is collected after the execution of the designed test scenarios and finally the data will be analysed and the findings will be presented.

An appropriate methodology for testing the research model will be developed based on a review of similar studies that report how other researchers have investigated similar problems. The review of similar studies provides vital information on what has been achieved in the field and what methodology has been used in their research. The review of similar studies is also necessary to ensure an appropriate methodology is adopted and properly applied in the research. The review of five similar studies is presented in section 3.1. Research questions and hypotheses derived from Section 2.6 are defined and justified in section 3.2. In section 3.3, the preferred research design is discussed in detail to show how the research question is to be answered. Details of data collection, processing, analysis and presentation are presented in section 3.4. The data mapping that links the question to the different data types and the hypothesis tests is shown in Figure 3.11. The limitation of the research will be discussed in section 3.5 and followed by a conclusion.

3.1 REVIEW OF SIMILAR STUDIES

Five relevant studies will be critically reviewed to analyse how other researchers are defining and implementing methodologies in areas related to the proposed research. The focus of Chapter 2 is on the definition of what is important in the area of digital forensic disk imaging tools. The task of Chapter 3 is to identify how to conduct the research in the topic area.

3.1.1 Standardised Approach Of Testing Disk Imaging Tools From NIST

The CFTT program is a joint project between a few organisations in the United States of America including NIJ, DOJ and NIST. The aim of the CFTT program is to actively provide a measure of assurance that the tools used during the investigation of digital crimes produce aacurate and complete results. The program addresses one key problem of the industry and legal community. This problem is that there is no standard or credible test to validate the accuracy and completeness of the result extracted by disk imaging tools. The test results are able to assist the forensic software vendors to improve their tools and provide best practice reference to support the results produced by those tools for presentation in the court. The primary studies of NIST (2004) and NIST (2005) of CFTT program present the testing of disk imaging tools. The studies initiated by NIST have a direct link to the proposed research because the approach taken has been widely recognised and acknowledged by the scientific and legal community. NIST is also one of the few research organisations dedicated to digital forensic tool testing.

NIST implements a systematic approach to identify and test the tool requirements. Figure 3.1 illustrates the methodology used by NIST for their disk imaging tool testing. They suggest that at the beginning, the category of forensic requirements will be determined by a group of expert users.

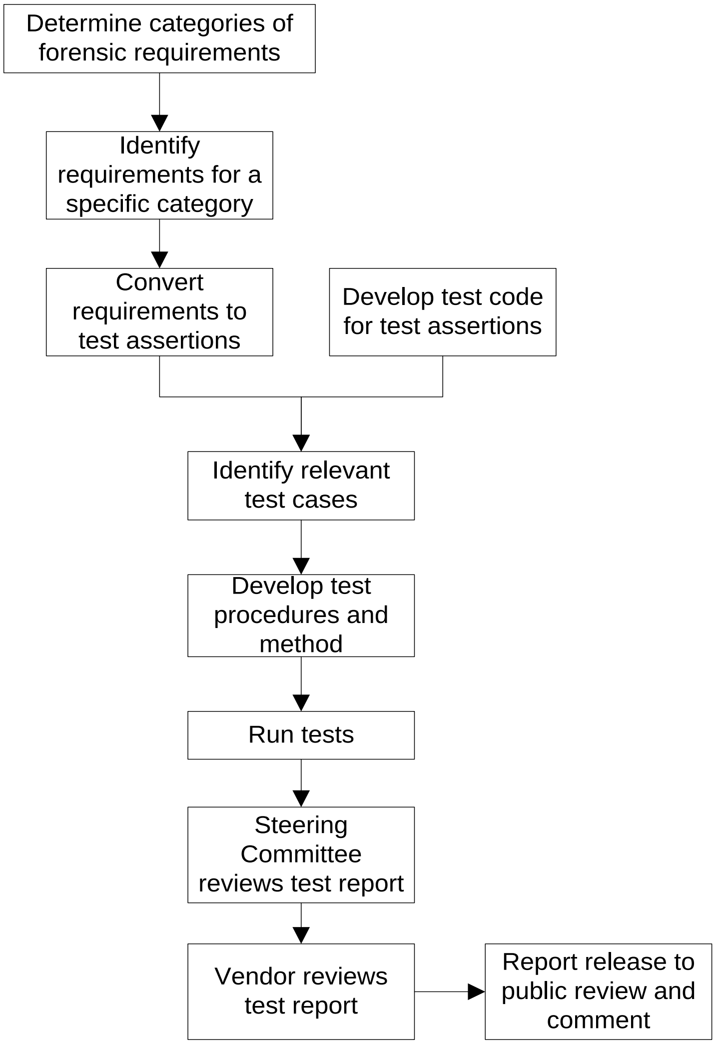


***Figure 3.1*. Methodology of disk imaging tools evaluation from NIST (2001)**

More precise requirements are then identified by forensic specialists and used to conduct tool testing. With category requirements defined, a list of requirements for the specific category will be identified by a group of local and national experts and the final requirements will be finalised by a consensus reviewed by forensic community users and public. A revision will be made and incorporated into the new testing specifications. The requirements identified are high level and may not be testable. It is necessary to convert the requirements to test assertions that bridge the gap between test specification and test scenarios. A test case includes one or more test assertions to specify what needs to be tested. Public review and opinion from forensic community experts will be used to narrow down to a small number of test cases. Finally a set of relevant test cases that contain a group of test assertions are identified. International guidelines and standards such as the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 17025 are adopted to standardise the test procedures and methods. NIST runs tests on selected tools and produces test reports according to the testing plan and procedures. Vendor and Steer Committee review the final test report and release the report to the public. The methodology used by the CFTT program is a systematic approach that is highly organised, robust and credible. Each step is reviewed and revised by experts from law enforcements and forensics communities. Test scenarios, tool requirements and test assertions can be modified and adopted in the proposed research. Also, the support software tools developed by NIST can improve efficiency of the testing process and also avoid unexpected problems arising from using untested software. From the test report, the test result is repeatable and reproducible. The test report serves as a reference point for the research to compare and analyse the test results that can identify any underlying problems.

3.1.2 Enhanced Approach For Disk Imaging Tools Evaluation

Byers & Shahmehri (2009) aim to provide a systematic approach to test disk imaging tools since tool testing is challenging, time consuming and expensive. Also, only few publications have been published in areas of digital forensic tool testing. The study focuses on evaluating Encase 6.8 and Linen 6.1 (Linux version of Encase), both developed by Guidance Software. The purpose of the evaluation in this research is the same as that of the CFTT program. Studies from the CFTT program and Byers & Shahmehri (2009) try to determine if the disk imaging tools used during the investigations perform as expected and produce accurate and completed results. Studies from Byers & Shahmehri (2009) have similarities to the CFTT program but also many major differences are identified during their evaluation. The methodology adopted by Byers & Shahmehri (2009) is shown in Figure 3.2. As the first phase, generic testing requirements are identified from three sources, namely formal interviews and discussions with law enforcements, CFTT program and existing literature review.

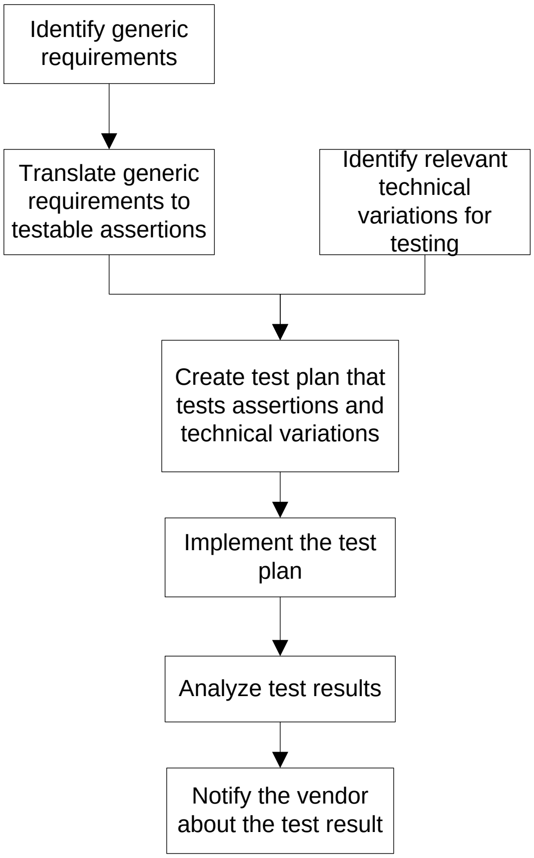


Figure 3.2. **Methodology of disk imaging tools evaluation from Byers & Shahmehri (2009)**

Technical variations are various environments where a disk imaging tool can be applied. These variations will affect how the tool behaves during the evaluation and the variations are necessary to be identified at the beginning. Each single variation is analysed. It is important to identify any further implications of other potential variation or evaluate whether it is in conflict with other variations. In the following stage, a list of high level requirements is converted to a set of testable assertions. Once technical variations and test assertions are defined, a test plan is built with a list of associated technical variations. Test cases are then created under a group of technical variations. Detailed setup procedures, testing environment, software required are outlined in the test plan. A generic procedure is also extracted from all common test cases. The plan is then executed and a test report is generated. Test results and anomalies are analysed to identify the underlying causes. The finalised test result reports to Guidance software for review and confirmation.

The research from Byers & Shahmehri (2009) is another good example of a study that is dedicated to disk imaging tool testing. Their research has many similarities to the CFTT program but also many improvements were made as well, has been added value to the research of the CFTT program. For example, Byers & Shahmehri (2009) developed a rationale of why some variations in some test cases should be eliminated and a guideline on how to combine variations for clearer test cases. These elements are absent from the CFTT program. Byers & Shahmehri (2009) also provide an in-depth analysis of the causes of unsuccessful tests, which are not provided by the CFTT program. Technical challenges are discussed in the Byers & Shahmehri (2009a)'s full research report, which provides an insight into the possible technical difficulties that may be encountered if their research approach is adopted.

3.1.3 Validating Forensic Software Utilising Black Box Testing Technique

Wilsdon & Slay (2006) proposed an evaluation framework to validate accuracy and reliability of forensic computing software. Wilsdon & Slay (2006) discussed the needs for the digital forensic tool evaluation at the beginning. Wilsdon & Slay (2006) pointed out that the evaluation framework of digital forensic tools from NIST and SWGDE is incapable of fulfiling the rapid demand of the industry because it can take up to months to evaluate a single piece of software thoroughly. CFTT program cannot test every single disk imaging tool in the market. The purpose of Wilsdon & Slay (2006) research is to develop and implement a more efficient testing framework than NIST and SWGDE with regarding to time, financial and output constraints. The differences regarding the reliability between proprietary and open source software are also discussed. The testing framework is built based on the software testing standards of ISO 17025-2005 and IEEE 610.12-1990.

A six-step evaluation process is developed in the research and illustrated in Figure 3.3. Software applications are acquired for evaluation at the beginning of the cycle. The documentation of software applications must satisfy standards ISO 17025-2005 and Australian Standard (AS) 4006-1992.

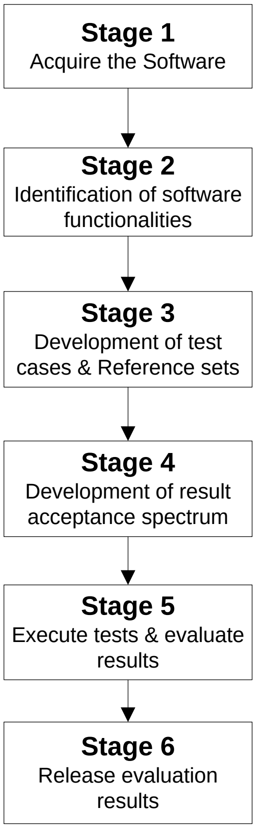


Figure 3.3. **Forensic computing software evaluation process from Wilsdon & Slay (2006)**

Signature of the software applications must be obtained using MD5 checksum or other hash functions to ensure the future updates of the software can be distinguished easily from the tested one. Software functionalities are identified according to the documentation provided or other sources such as discussion board, vendor websites, and related community input. All the functions must be identified and properly documented as an item to be tested. Completed documentation of all available functions in stage 2 will directly affect the output of stage 3. Test cases are developed based on black-box testing technique and all the test data is organised to test all identified functions. The organisation of collected data sets is presented as a reference set. The same reference set can apply in different contexts with the same functionality. Reference sets can be made available to the community to review the completeness and accuracy. The software may be used in different environments (Law enforcement, military, and commercial) and different levels of acceptance can be identified. The resulting acceptance spectrum can be divided into four levels, namely exceeds requirements, target range, minimally acceptable and unacceptable, according to ISO software evaluation standard 14598.1-2000. Tests will be executed and checked against requirements defined in stage 1. Test results are collected and assessed against the acceptance spectrum defined in stage 4. The complete evaluation result is released to the community for review in stage 6.

The framework developed by Wilsdon & Slay (2006) is a refined approach of NIST and SWDGE. Development of an organised reference set of different functions of the tested software can make the testing in the proposed research more efficient. Because multiple test subjects will frequently access different test cases for the same function, unified reference sets will save time for retrieving the same data again and again.

3.1.4 Applying Systematic Method For Commercial Off-the-shelf (COTS) Selection

Kontio (1996) presented a case study applying a systematic method for reusable COTS selection. The aim of the study is to prove that a more thorough definition of evaluation criteria will result in a more effective and reliable evaluation process (Kontio, 1996). A methodology called Off-The-Shelf Option (OTSO) has developed to assist the process of search, evaluation and selection of COTS for decision makers. The paper has placed the focus on how to define evaluation criteria and analyse data. In addition, two data analysis methods, weighted scoring method (WSM) and Analytic Hierarchy Process (AHP), were applied in the case study and compared and analysed against various standards such as efficiency. The process of OTSO method is illustrated in Figure 3.4, which demonstrates how the research was done. Evaluation criteria definition is gathered from five different resources, requirement specification, design specification, project plan, organisational characteristics and criteria feedback from the process of software searching. Then from the selection criteria a set of formal evaluation criteria is formed and these criteria will assist the software screening process to narrow down the candidate software for in-depth evaluation.

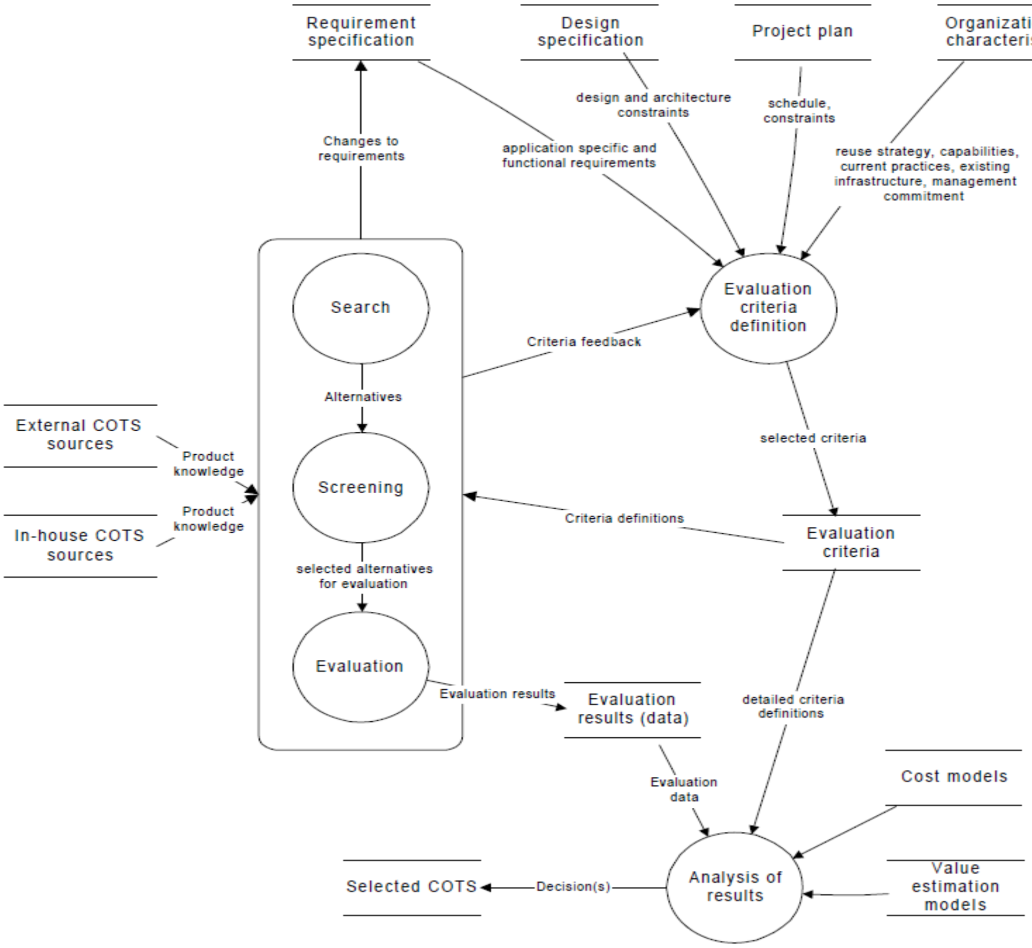


Figure 3.4. **Process of OTSO method (Kontio, 1996, p.3).**

A detailed flow chart of the evaluation criteria definition process is shown in Figure 3.5. The criteria definition flows logically from searching criteria definition, further defining criteria and assigning weighting criteria. Product evaluation is then conducted based on the criteria defined in the earlier stage. Analysis is done on the raw data generated from the evaluation. The data analysis using WSM assigns a value from 1 to 5 to each criterion.

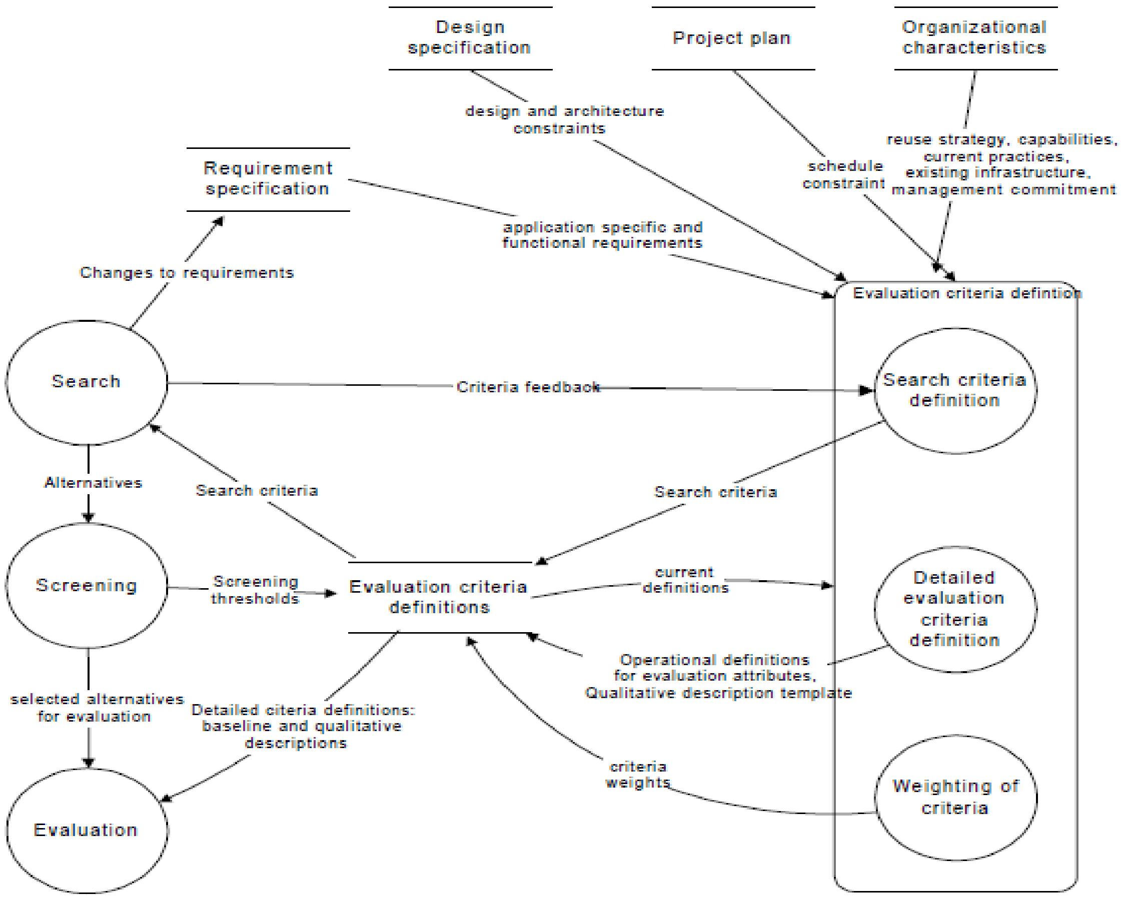


Figure 3.5. **Process of evaluation criteria definition from Kontio (1996, p.4)**

Weighting is assigned to each criterion in the previous stage and normalised into the total of 1. Then the score is calculated based on the following formula:

$$score_a = \sum_{j=1}^{n} (weight_j * score_{aj})$$

Another method called AHP was also used to analyse the data evaluation. AHP is a multiple criteria decision making method that decomposes the criteria into a hierarchical structure. Each level of hierarchy will assign its importance factor by comparing each item in the level in pairs. Finally, the alternatives will compare in pairs again to determine their rankings. The one with the highest ranking is recommended as the best alternative.

The reason for reviewing this article is that COTS evaluation has many aspects that are of value to this study, starting from requirement specification to software evaluation. The research process of OTSO is a logical development of a successful project with detailed research result presented as supporting evidence. In addition, the paper has provided two significant methods used for evaluation and data analysis with detailed application in a case study. The research result has shown that AHP, WSM or a combination of both can benefit the data analysis in the present study.

3.1.5 Function Oriented Methodology to Validate Digital Forensic Tools

The study of Guo & Slay (2010) proposed a function oriented methodology to verify and validate digital forensic tools. Guo & Slay (2010) first describe the background of the validation and verification framework within the field of digital forensics. The methodology proposed by Guo & Slay (2010) can be summarised into five major stages as illustrated in Figure 3.6. Stage 1 involves the systematic and scientific understanding of the field of the Electronic Evidence (EE). This stage identifies the position of the functions in the investigative process. For example, the function focused only at research was that forensic copy function. The forensic copy function belongs to the collection phase of the investigative processes reviewed in Section 2.1.2. The forensic copy function was broken down into many sub-functions. After the function is mapped to different detailed sub-functions, the requirements for forensic copy function are specified. A variety of diversifications were taken into account when specifying the requirements. After the requirements were specified, different test cases were developed according to each identified requirement. However, the authors have not applied the methodology on any disk imaging tool yet. They state that the tool would be tested against the test cases and measurement metrics would be applied to determine the accuracy and precision of the results (Guo & Slay, 2010).

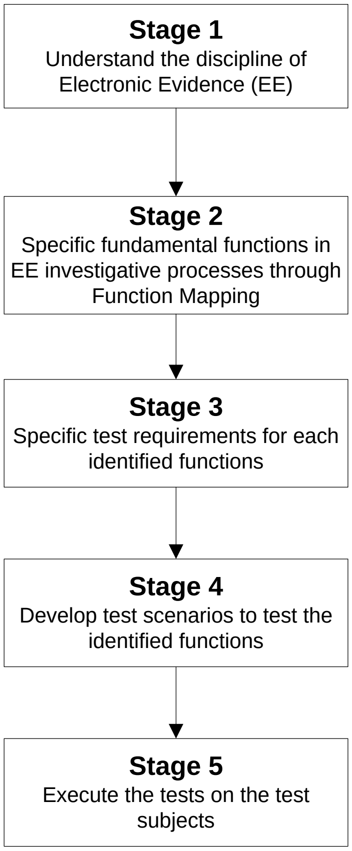


Figure 3.6. **Process of Function Oriented Paradigm from Guo & Slay (2010)**

The effort made by Guo & Slay (2010) is another notable research in digital forensic tools validation. The methodology adopted in this research is a systematic and scientifically sound approach to validate digital forensic tools. Compared to the traditional testing methods, the approach used in this research is extensible and tool neutrailised. As more requirements are found, they can be added to the specifications without compromising the entire framework. The approach is functionality oriented and it does not matter to what tool it is applied.

Unfortunately, this methodology has not been applied on any tools yet to evaluate its weaknesses or shortcomings. The development of the reference set in the research by Guo & Slay (2010) has a potential problem. The problem is that the authors have specified extensible function requirements and they assumed that the corresponding reference set (test scenarios) were also extensible. Each function requirement may have serveal variables that lead to different variations. But Guo & Slay (2010) missed out the possible combination of those variables that maybe meaningful to test. For example, the physical interface used for the tool testing is ATA and whose interface has different revisions. The version ATA-6 introduced 48-bit addressing but it’s also compatible with 28-bit addressing. Test cases can be added to the test specification to test the support of 28bit addressing in ATA-6 version. The reason for reviewing this article is that this methodology has aspects that can be valuable for this research. Developing a function map could help the research to specify detailed specifications of the functions for validating disk imaging tools.

3.2 RESEARCH QUESTIONS AND HYPOTHESES

The literature review in Chapter 2 provides a foundation for defining the main research question and particularly the discussion in section 2.1 as follows:

> *What is the performance of selected disk imaging tools that are available for tracing and mapping of digital evidence?*

In order to answer the main research question, a few relevant sub-questions need to be formulated. According to the literature reviewed in Section 2.2.4, digital forensic tools must be validated through a series of extensive and careful validation tests. The accuracy and completeness of the data generated by the disk imaging tools are the main focus of this study. Sub-questions can be derived from the relationship between the testing scenarios & confgiruations and test results are formulated as follows:

> *SQ1: Which testing scenarios are designed to test whether the disk imaging tools are extracting accurate and complete data?*
>
> *SQ2: What testing configurations are set to ensure the testing is a forensically sound approach?*
>
> *SQ3: How can the selected disk imaging tools be ranked in terms of the accuracy and completeness of extracted data?*

The relationship between selected tools and testing and validity of the tools is illustrated in Figure 3.7. The testing requirements are used as criteria for the validation testing. According to Figure 3.7, validation testing measures the accuracy and completeness of the data extracted by the selected disk imaging tools.

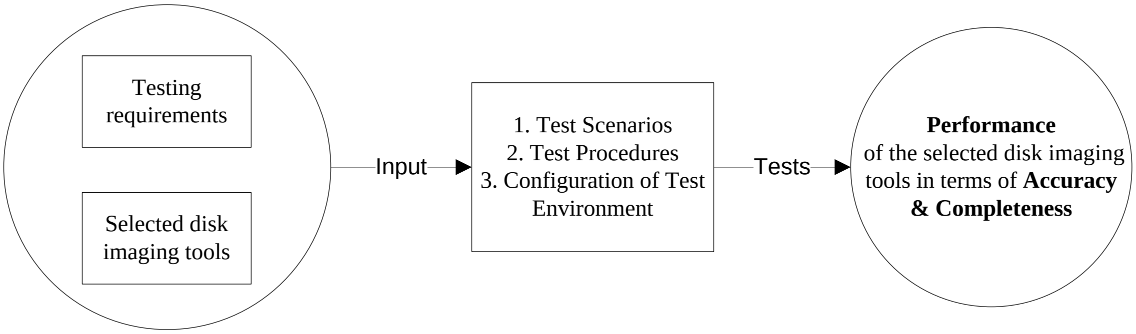


***Figure 3.7.* Research model.**

The hypotheses about the performance between the testing and the validity of the selected disk imaging tools are as follow:

> *H1: FTK Imager will perform better than the other two selected disk imaging tools in most of the common test cases;*
>
> *H2: Helix 3 Pro will perform better than AIR Imager in most of the common test cases;*
>
> *H3: AIR will perform better than the other two selected disk imaging tools in a very few common test cases.*

According to the literature reviewed in sections 2.2.2, 2.2.4.2 and 2.3.1, accurancy and completeness are two important criteria for evaluating the performance of disk imaging tools. Therefore, the research aims to find out which disk imaging tools are most successful under various testing scenarios.

3.3 THE RESEARCH MODEL

The five studies reviewed in Section 3.1 have investigated the standardised approach and other potential methods of assessing digital forensic disk imaging tools. The main objective that needs to be established is to empirically verify the validity of digital forensic disk imaging tools. The essential element of this research is to execute a series of test scenarios on the selected disk imaging tools based on the defined test requirements. It should be noted that the testing utilises black-box testing techniques by executing a set of pre-defined test scenarios to investigate the validity of disk imaging tools in a logical and standardised approach. Utilising test scenarios based on a set of pre-defined requirements to verify disk imaging tools is a common and recommended practice according to a variety of digital forensic tool studies (Byers & Shahmehri, 2009; NIST, 2004; Wilsdon & Slay, 2006; Yinghua & Slay, 2010; SWGDE, 2009a). A scenario-based testing approach is the most suitable method of assessing the validity of disk imaging tools.

The proposed research includes five phases and is illustrated in Figure 3.8 below. Disk imaging tools are selected based on the preliminary requirements (see Table 2.6) and a series of market and vendor researches. Disk imaging tools and their documentations are acquired and reviewed in phase one. Determination of which disk imaging tools will be selected for testing will be based on the budget of the study, reputation and publicity of the tools. Sources of the information are also a subject of research in relevant research articles, journals, websites, forums and books. Research budget is another important tool selection criterion. After a list of disk imaging tools has been selected, the method function mapping adopted from Guo & Slay (2010) will be used to provide a level of abstraction that would specify the required functions of disk imaging tools for the forensic software developers, industry practitioners and other researchers who are conducting their own forensic tools validation. The process of test requirements specification will be initiated once the function mapping is completed. CFTT program has made significant progress in specifying the requirements for the disk imaging function. Testing requirements from CFTT has been considered as a standard when testing disk imaging tools. In addition, a review of other releated research conducted in Section 2.2.4 and the documentation of selected tools will serve as input to requirement specifications in Phase 2. A list of mandatory and optional requirements is generated. The test requirements are designed based on the two testing criteria, namely accuracy and completeness. A completed list of mandatory and optional testing requirements is documented in Appendix 2. Quality of the test requirements is set through an informal discussion with some experienced industry experts.

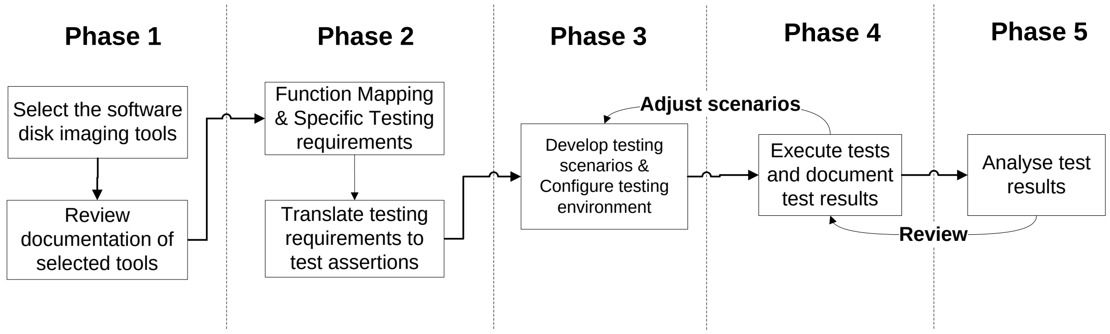


Figure 3.8. **Research phases.**

Test scenarios and assertions are developed in Phase 3 according to a few similar studies (Byers & Shahmehri, 2009; NIST, 2004; Guo & Slay, 2010), the available equipments, testing requirements and the functionalities provided by the selected disk imaging tools. A proper configuration of the testing environment is also completed in Phase 3. The complete list of testing scenarios and assertions can be retrieved from Appendix 3 and Appendix 4. Test scenarios are executed and test results are documented in Phase 4 based upon the specifications designed in Phase 3. Data gathered from Phase 4 are analysed in Phase 5. At the conclusion of the data analysis, the hypotheses will be fully tested and the validity of three selected alternatives can be compared and studied. The iterative research design can help to further improve the research methodology and generate more accurate results. The research phases in the proposed research have similarities with other widely used software evaluation approaches (Kontio, 1996; Wilsdon & Slay, 2006; Comella-Dorda et. al., 2002).

3.4 DATA REQUIREMENTS

Data collected from Phase 4 will be processed and analysed in Phase 5 to empirically test the hypotheses and the research model developed in sections 3.2 and 3.3 respectively. Information collected in Phase 1 and 2 contains review of related literatures, Internet survey, software vendor sources and consumer report. Development of test scenarios and assertions is based on the information collected in phase 1 and 2. A series of tests are to be performed in phase 4 according to test scenarios and assertions. Finally, test results are collected from the tests and analysed.

3.4.1 Data Collection Methods

Different data collection methods adopted in the proposed research are explained in the following sub-sections.

3.4.1.1 Market And Vendor Research And Internet Survey

Market and Internet survey and vendor research are among the common approaches to screen and select candidate software for a software evaluation project (Maiden & Ncube, 1998; Kunda & Brooks, 1999; Kontio, 1996). More than 50 open-sourced and proprietary vendors have been researched against the preliminary requirements and the research budget. Information reviewed includes the software user manuals, publically released notes, updated histories, consumer reports, user comments and related forum entries. A list of three candidate software is presented in Phase 1.

3.4.1.2 Function Mapping

Before the complete set of requirements is developed, a function map is created to map each identified function to the requirements of disk imaging tools. After each function and its sub-functions are identified, the requirements corresponding to each function category will be specified. Guo & Slay (2010) mentioned that function mapping can provide a level of abstraction of functions that should be included or tested for the tool testers or software developers. Byers & Shahmehri (2009) also employed similar method to identify more potential requirements for tool testing. The function map is tool independent and it can be applied to any disk imaging tools. Tool developers, testers and analysts can adapt the function map to identify their own requirements and start testing the tool in a focused and organised approach. Figure 3.9 depicts the function map built in a way that it can be reused to create suitable requirements for any disk imaging tools.

The function map (Figure 3.9) consists of six major schemes, namely Access Method (AM), Digital Source (DS), Data Destination (DD), Execution Environment (EE), Hidden Areas (HA) and Physical Interface (PI). The definitions of six major schemes can be found in Appendix 1. Each major scheme may have few sub-sections. Due to space limitation, function map only presents the important parts that are relevant to this research. To access the DS from the device, the device needs to be connected to the computer using a PI and the disk imaging tool will acquire the device by some command sets or protocols (NIST, 2005). In Figure 3.9, AM and PI combined will allow the disk imaging tool to run in an EE to acquire the DS. The DS will be stored in the DD. NIST (2005) refers the combination of AM and PI as Access Interface. For instance, a hard disk connects to the computer using a SATA PI and accesses the drive using the AM ATA command set. The disk imaging tool will run on top of the EE Microsoft Windows using some command sets or protocols and acquire the DS and save it into the DD of an external hard disk.

The Digital Source scheme contains two major classifications that are nonvolatile data and volatile data. Nonvolatile data is the information residing on a storage medium such as hard disk and the data will be retained in the medium even when the power is off. Volatile data does not fall into the research scope therefore the sub-section will not be expanded to a detailed level. In the field of digital forensics, investigators usually acquire the evidence in two ways: making a physical copy or a logical copy of the selected data. Making a physical copy of the evidence means every bit of the data in the storage medium will be read, acquired and stored as another copy in an external data destination (Refer to section 2.3 for more details). According to Guo & Slay (2010), physical copy can be divided into three common types which are magnetic, optical and semi-conductor. Optical and semi-conductor types are omitted because they do not fall in the scope of this research. Magnetic type can be further divided into two sub-categories, namely raw and structured. Category raw represents the data when it contains only data but nothing else. An example of the raw data could be DD raw image format. Category structured may contain other information that might be useful for the forensic investigators such as hash information, compression level and time of acquisition. EnCase, SMART and Advanced Forensics Format (AFF) could be the examples of the structured data.

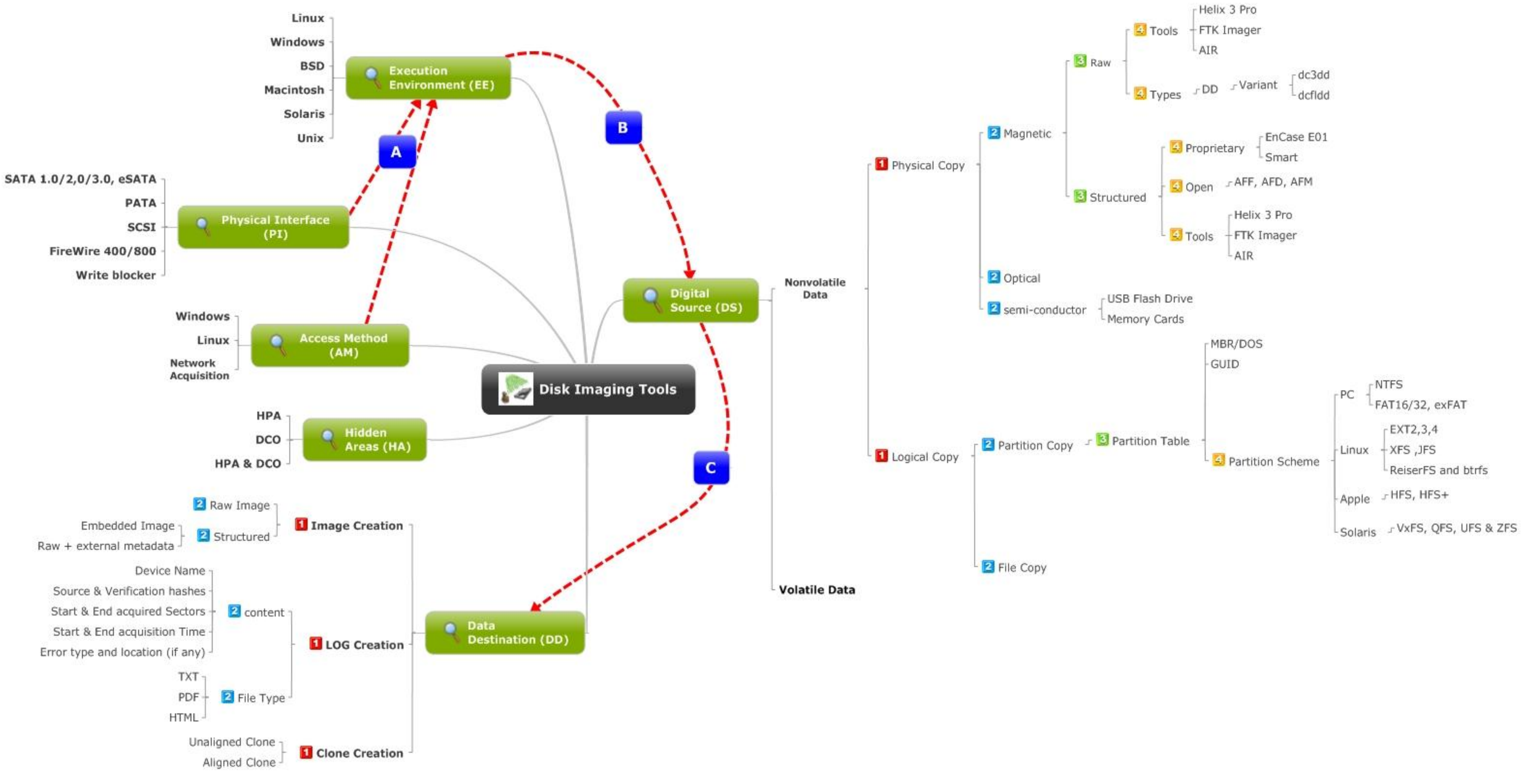


Figure 3.9. **Function Map (Adopted from Guo & Slay, 2010, p.667)**

When the acquired images are saved in the Data Destination, the log must be produced along with the image files if the log function is enabled. Some essential information, such as device name, number of acquired sectors, must be provided to the user. The log information is important to the forensic investigators as the information sometimes serves as evidence introduced to court.

3.4.1.3 Tool Test Requirements

With the function map completed, a series of research on prior literature will also be reviewed to determine the preliminary tool testing requirements. The literature review found that requirements from NIST research are a standardised approach for disk imaging tools testing. The NIST requirements are also recommended by other authors such as Byers & Shahmehri (2009), Wilsdon & Slay (2006), Carrier (2002) and Black (2005). A number of requirements have been adopted from NIST and some requirements are derived from other authors to complete the list of requirements in this research. An informal interview with industry experts confirms the final test requirements. A series of testable assertions are translated from the test requirements of each functionality category (see Appendix 4). This research is decided to focus on the the drives connected by using SATA drive with Tableau T35es Hardware write blocker (USB). The operating system is determined to concentrate on Microsoft Windows XP SP3 and Windows 7 for FTK Imager and Helix 3 Pro and Linux (32-bit) for Helix 3 Pro and AIR. These decisions provided on initial set of prelimilary requirements, from which the research derived additional requirements.

3.4.1.4 Development of Test Scenarios

The development of the test scenarios focuses on two validation metrics, namely accuracy and completeness. The CFTT program has provided a good starting point to develop a set of comprehensive test scenarios. Some parts of the specifications of the test scenarios are based on the standardised CFTT test sets. However, the test specifications were developed in 2005 and required update to fit in this research. The literature review found that the research presented in Byers & Shahmehri (2009) has developed a list called Technical Variations that can help this research to explore more possible testing scenarios (see Appendix 3). The Technical Variations defined the various contexts in which a tool can be encountered. Each test scenario consists of a set of assertions. Different scenarios may have different test assertions and each assertion is tested at least once. The completed list of test assertions is shown in Appendix 4.

3.4.1.5 Testing of Disk Imaging Tools

A series of tests are performed in Phase 4, according to the test specifications developed in Phase 3. The needs for digital forensic software validation and verification are demanding (Guo et al., 2009). The functionality driven approach is considered an effective approach for the proposed research since it has been adopted by many tool evaluation projects such as Lyle (2003), Carrier (2005) and Byers & Shahmehri (2009). The selected tools are tested against four functionality categories, namely: fundamental requirements, imaging creation, hidden sectors and logging function. Each selected disk imaging tool undergoes series of test scenarios and each scenario composes a series of test assertions developed in Phase 3. The test result for each test assertion is presented by two rating scales, which are pass and fail. Most of the test cases share common configuration procedures (see Appendix 5). Defining the procedures will ensure consistency in test scenarios and will enable other researchers to replicate or audit this research.

3.4.2 Data Processing Methods

The test result of the tool testing is in the form of different log files generated by the selected disk imaging tools. The format and the information contained in the log files are vary from tool to tool. Therefore, the results and the associated information are collected and summarised into a table, after each test is completed. The table consists of Test & Case Summary, Test assertion, Information of source device and its setup, log highlights, test result and analysis. When all the performance tests are completed, the result of each test will be entered into a spreadsheet to identify the passed and failed assertions of each test scenario. After the pass rate is identified for each tested tool, a comparison chart is generated to compare the performance of the selected three disk imaging tools in each test scenario. The data of this spreadsheet will help the research to construct a Gap Analysis (GA) matrix.

3.4.3 Data Analysis Methods

GA is adopted as the data analysis method in the proposed research. GA is able to identify the differences of the final scores and to reveal the relative superiority between the evaluated tools. GA compares the measured values to the required values based on the criteria. For example, Figure 3.10 illustrates three possible results that might be achieved during the evaluation on selected tools. Figure 3.10(a) shows the selected tool meets the test requirements. The second result in Figure 3.10(b) shows that the selected tool only partially fulfils the test requirements, while the third case (Figure 3.10c) is when the selected tool may fulfil some or all the test requirements, as some of the features may fall outside the boundary of the defined requirements (Sheng & Wang, 2008).

A GA evaluation matrix is designed to assess the gap between the selected tools and the defined requirements. The gap can be identified as:

Gap = Required Requirements – Actual performance of the Tool

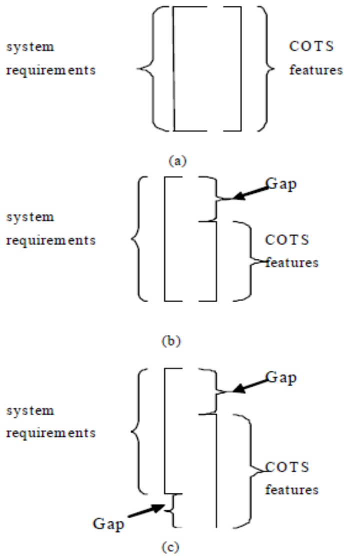


Figure 3.10. **Example of Gap Analysis (Sheng & Wang, 2008, p.1249).**

An example of GA matrix is demonstrated in Table 3.1. The testing requirements defined in Phase 2 are considered as differentiated factors to identify the gap between the three selected disk imaging tools. The value for each criterion against each product can be categorized as textual value, numerical value or other type of value. The value of each criterion defined in this research is textual value.

Ratings "passed" and "failed" are sufficient enough to identify the gap between the requirements and the actual performance of the tool. Vatis (2004) adopted the technique of GA matrix in a national research on investigating the gap between the cyber-attacks and the law enforcement security tools.

Table 3.1

Example of Gap Analysis Matrix

Product **Criteria**	**FTK Imager**	**Helix 3 Pro**	**AIR**
Requirement 1	PASSED	FAILED	PASSED
Requirement 2			
……………			
Requirement X			

Figure 3.11 illustrates the mapping of the research questions to the research stages. The data map demonstrates how the research questions will be answered in a logical and scientific manner. Figure 3.11 also illustrates the detail flow of logics how this research is conducted.

3.5 LIMITATIONS OF THE RESEARCH

The proposed research proposes to examine the performance of the selected disk imaging tools in different validity tests. However, certain limitations are expected in the proposed research.

A manageable number of disk imaging tools are tested against the designed test scenarios in the proposed research. Many other disk imaging tools are available on the market at variable cost but this investigation is focuses on the selected tools. No attempt is made for the findings to be representative but rather a case is built on the use of well-known tools. The main problem of this approach is overgeneralisation and also a sense of incompleteness as there are many other software tools that could be tested.

There are many other types of hardware interfaces that are popular in the market, such as USB drives, SSD and SCSI drives. Due to the time constraint of this study, certain type of storage devices with specific hardware interface is chosen for investigation. The disk imaging tools test results may only be applied to those hardware interfaces that are evaluated. The reliability of the research may be limited to the hardware interfaces that are tested on the selected disk imaging tools. If different hardware interfaces could be included in the research, it would provide a more comprehensive view of the validity of the selected disk imaging tools and would be the starting point for further research.

A limited set of test scenarios are designed and tested due to the time constraint and the complexity of each test. Also, there are challenges with the testing methodology in the proposed research. Results of the disk imaging testing may only be reliable in the controlled environment. Sometimes, it is difficult to replicate the environment used in the testing. Wilsdon & Slay (2006) highlight that there are no two laboratories that use the same examination workstations with the same configuration. The test scenarios used are designed to be as hardware independent as possible. More robust testing scenarios could be added to the research to enhance its reliability.

Technical difficulties are expected during the disk imaging tools testing and these difficulties may prevent certain tests from being conducted or completed. Hardware failure is also expected and this may produce false results for the research. Certain precautions can be undertaken to resolve these issues such as running hardware against diagnostic software and reviewing test logs of each test. However, challenges are expected and issues of both reliability and validity are defended in Chapter 5.

3.6 CONCLUSION

The research model developed in Section 3.2 captures the relationships between testing requirements, testing execution and the performance of the disk imaging tools. The model forms three main hypotheses. The hypotheses assume that the performance of each tested disk imaging tool are vary in terms of the accuracy and completeness.

A review of similar studies revealed that testing the selected disk imaging tools against different scenarios is the most appropriate method for this research. Informal interviews were conducted to gather feedback on the testing requirements from industry experts. Testing requirements includes four categories and each category contains a number of test assertions. Series of carefully designed test scenarios are executed against the selected tools to obtain the test results. Certain limitations are imposed on the forensic tools testing. Once all the test results are collected, raw data will be processed for later analysis.

GA and test result comparison are utilised as data analysis methods. GA is able to identify the gap between the actual measured values (as determined by the tool testing) and the required values. The gap between the testing requirements and the actual performance of the tools can be recognised and differentiated according to the tool testing. The analysis enables tool developers to realise the shortcomings or weaknesses of their tools in order to further improve them to address the demands. The methodology developed in Chapter 3 guides the execution of tool evaluation accordingly and the results of the evaluation findings are presented in Chapter 4.

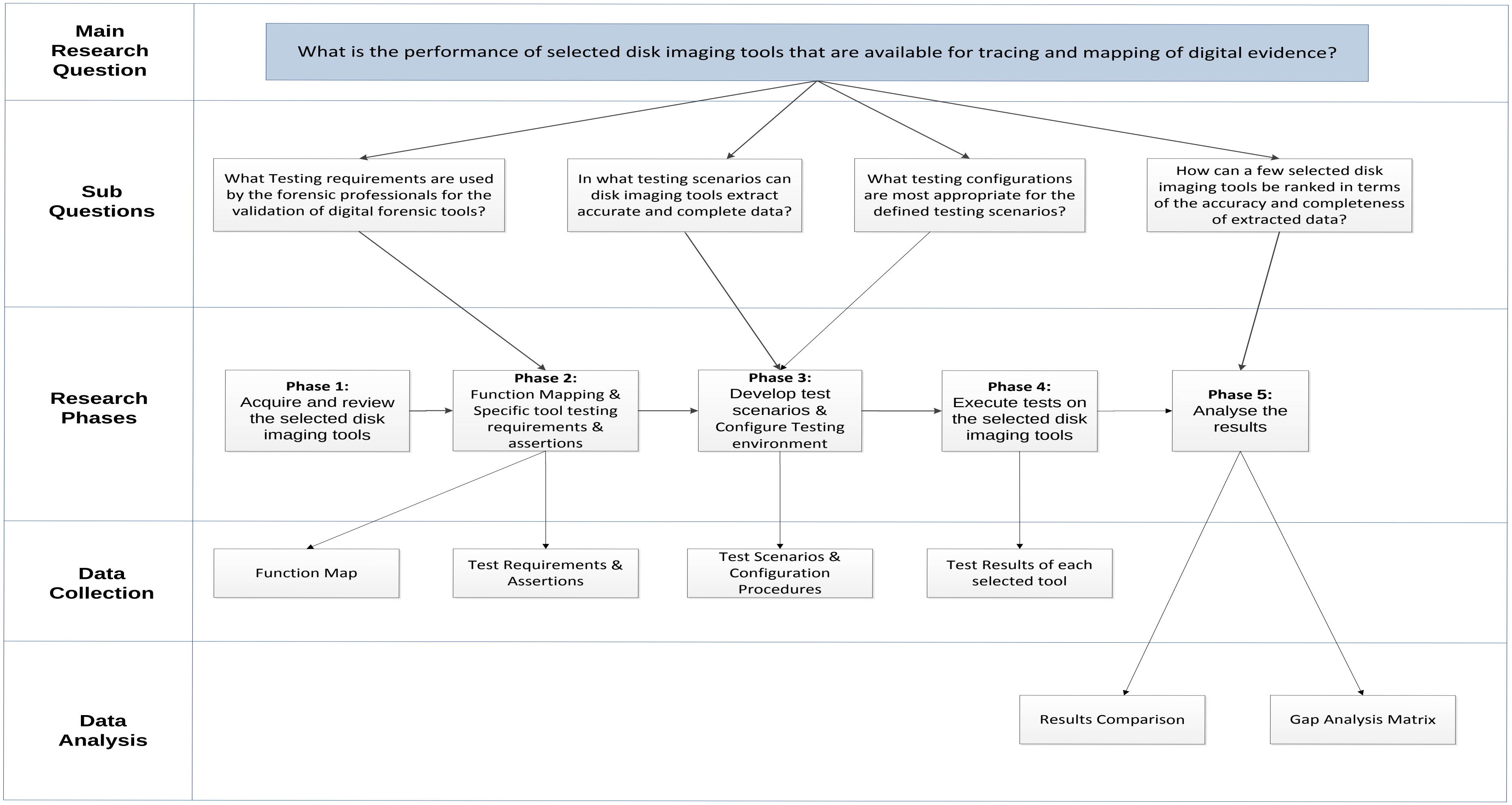


Figure 3.11. **Data Map.**

Chapter 4

Research Findings

4.0 INTRODUCTION

The Literature review in Chapter 2 has paved the path for standardising the testing requirements and a list of detailed assertions is derived from the requirements. Chapter 3 outlines the research methodology that is adopted in the various research phases to answer the research questions. The literature review and research methodology provide guidance in terms of how to approach the evaluation of disk imaging tools. The main objective of Chapter 4 is to report and summarise the findings from the performance testing of disk imaging tools.

The data collection, processing and analysis proceeded according to the specifications described in Chapter 3. This chapter reports the variations in the research specifications and how each evaluated disk imaging tool is performed in each test case. The collected results of the test case are summarised and analysed. This chapter discusses different aspects of the tool testing stage. Collected data is analysed using GA to study the gap between the testing requirements and the actual performance of the tool. The collected research data is organised following the steps defined in Chapter 3 to ascertain whether the data fits the pre-specified model so that the research question could be answered.

This chapter firstly reports and discusses the alteration of methodologies for practical research based on the benchmark methods specified in Chapter 3. The two different environments for hardware and software configuration are discussed and their implications for the tool testing are also reviewed. There are three testing disk imaging tools and 18 test cases. Three selected testing disk imaging tools have been tested in different test cases and the individual report of each tool has been generated for each test case. Some test cases may only be applied for one or two of the tools. In the last section, the testing results for each disk imaging tool are presented and the comparison of the test results for three tested tools is carried out.

4.1 VARIARTIONS IN RESEARCH SPECIFICATIONS

Most of the evaluations were conducted according to the test plan specified in Chapter 3. However, certain deviations were encountered during the evaluation. The deviations are explained in the following sections.

4.1.1 Data Collection

Some of the planned tests were not carried out and some other tests were performed instead due to issues encountered during testing. For example, test case TC-04 requires a digital source that has at least one faulty data sector and was not carried out since a suitable simulation environment is not available. Byers & Shahmehri (2008) point out that issues of faulty sectors are made apparent in forensic software testing. Lyle (2007) also points the issue of faulty sector is difficult to emulate. After the first few trail tests with the disk imaging tools, the number of test cases was increased to total number of 18. Test cases of acquiring GUID partitions were added to study how the disk imaging tools respond.

Execution environment was changed in some test cases due to the hardware incompatibility of the disk imaging tools. When testing the tool Helix 3 Pro using the Live CD, problems were encountered during the acquisition processes that prevented the testing from proceeding further. Therefore, virtualised environment was used to eliminate the problem of hardware incompatibility. Details of the test error encountered during the acquisition are discussed further in section 4.2.

Hardware write blocker was not utilised at all time despite the fact it was planned to be adopted for the purpose of preventing accidental writing to the source hard disk. In the scenario where HPA and DCO hidden areas are involved, the Tableau T35e hardware write blocker will automatically override HPA and DCO when they are detected which would defy the test purpose. The original testing purpose is to utilise disk imaging tools to acquire the source hard drive and analyse how the tool responds to the designed hidden sectors. In order to prevent any unauthorised writing to the source disk, the source disk will be hashed in an execution environment where no partition is mounted during the operating system start up. Also, the source disk will be hashed again after the acquisition if necessary. If two hash values match, it would indicate that the source disk has not been modified. The end results are not affected even if the hardware write blocker is not used at all times.

Some metadata of the case such as examiner, case number, evidence number are required manually enter into the software. However, sometimes the information was not entered exactly in accordance with the actual test. Disk imaging tools should prompt the user to input correct information to identify the data acquired and to differentiate each individual case. However, this does not affect the end result of the acquisition and the whole evaluation.

A tool package developed by NIST were originally planned to be used in the project to verify the acquired image. However, the tool only supports IDE hard drive connection interface and this was only discovered at the data collection phase. The main testing interface in this research is SATA which is currently the most popular hard drive interface.

4.1.2 Data Processing & Analysis

Data processing and data analysis were carried out exactly as from what defined in section 3.4.2 and 3.4.3 respectively.

4.2 FIELD FINDINGS

The field work was carried out in three phases: Phase one: Testing environment is properly configured for each test; Phase two: evaluating three different disk imaging tools; Phase three: verifying results produced by the tested disk imaging tools. All phases are interdependent and logically connected. Phase one configures the appropriate testing environment for each test case. Correct configuration has a direct impact on the results and findings. Phase two involves evaluating three different disk imaging tools to examine their responses in the designed test cases. The final phase three verifies the results generated by the disk imaging tools. The verification result indicates whether the disk imaging tool passes or fails a particular test case. The field findings of Phase three are reported in section 4.2.2.

4.2.1 Testing Environment

Two execution environments, namely Windows and Linux, were tested during the tool testing. Complete hardware specifications are shown in Table 4.1. A list of support software that were utilised during the testing is also summarised in Table 4.2. The software has a hardware incompatibility problem with the hardware resources that were available; virtualised environment was utilised instead as secondary test environment to minimise the problem. The hardware specifications of virtualised environment are based on test station 1.

Table 4.1

Test Stations & Operating Systems

<table>
<tr><th>Test Station 1
Windows Environment</th><th>Test Station 2
Linux Environment</th></tr>
<tr><td>**Hardware**
Intel® Core(TM) i5 CPU 750 @2.67GHz
Gigabyte Motherboard GA-P55A-UD4
BIOS version F6
On board USB 2.0, USB3.0, Ethernet, SATA and PATA controllers
Texas Instruments 1394 OHCI Host controller
4GB Ram
ASUS DVD-RW DRW-24B1ST ATA Device
SAMSUNG HD103SJ SATA drive 1TB</td><td>**Hardware**
Intel® Core2(TM) CPU 6300 @1.86GHz
EPox 5P965 Motherboard
On board USB 2.0, Ethernet, SATA and PATA controllers
1.44 MB floppy drive
3GB Ram
Pioneer DVD-RW DVR-111D ATA device
Seagate ST3250823AS SATA drive 250Gb</td></tr>
<tr><td colspan="2">**Operating Systems & Test Cases Involved**
Windows 7- 32bits
• **All test cases of FTK Imager**
• **Helix (TC-02 NFTS, TC-05, TC-07, TC-08, TC-17, TC-18)**
Windows XP SP3 with latest system updates or Virtualised Windows XP SP3
• **Helix (TC-01 USB, TC-14, TC-15, TC-16, TC-18)**
Live CD Environment
• **Helix (All TC-01 except TC-01 USB, All TC-02 except TC-02 NTFS, TC-03, TC-06, TC-12, TC-13**
Ubuntu 9.04 LTS
• **All test cases of AIR**</td></tr>
</table>

Most of the test cases followed the generic procedures: reset test drive, partition drives if required, acquire test drive using disk imaging tools and verify the results. Test cases TC-01, TC-02, TC-05, TC-07, TC-11 and TC-17 are the examples that followed the generic procedures (see Appendix 4). However, some test cases were setup and configured differently than the others. Test cases TC-03, TC-12 and TC-16 were required to setup hidden sectors in the test drive after the drive was partitioned. HDAT2 was used to configure HPA and/or DCO hidden areas in the test drive (see Appendix 4.4). TC-06 used a tool called MHDD to emulate uncorrectable (UNC) data error in particular sectors of the test drive. TC-15 is a test case that used Hex editor to corrupt the data in the Master Boot Record (MBR) of the test drive. A DOS-based partition editor was used in test case TC-13 to create the status known as "partitions overlapping".

Table 4.2

Support Software that used to configure and setup the test drives

Software	Version	Description
MHDD	4.5	Low-level HDD Diagnostics Software
UltraEdit	16.10.0.1036	Hex Editor
Darik's Boot and Nuke	2.2.6	Used to securely wipe the test drive
Hdparm	9.29	Linux Hard drive tool, used to check and change parameter of the test hard drive
Gparted	0.6.2	Linux hard drive partitioning tool
Disk Management Tool	1.0.0	Windows hard disk partitioning tool (Supports GUID partition table partition style)
Disk_stat	3.1.2	Used to check the existence of Host protected areas
EnCase	6.16.1	Used to verify the hash value of the acquired images
WinHex	15.6	Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor from X-Ways Software

A combination of tools was required to create and build up different testing environments for the analysis and evaluation of the actual performance of the tools. Test case TC-04 was not conducted due to the tool used to configure the test environment not being available. Specially-developed programs would be required to meet the requirements in order to conduct some specific test cases in this research. HDAT2 is program for testing or diagnostics of various types of storage devices.

Using program HDAT2, HPA and DCO areas could be setup in the source device for test cases TC-03, TC-12 and TC-16. When the HPA and DCO were setup, a tool had to be used to verify if those areas were properly configured. Hdparm and Disk_Stat were the tools that used to query an ATA disk to detect the existence of HPA and/or DCO areas.

4.2.2 Field Findings: Disk Imaging Tools Evaluation

The evaluation involved configuring the proper testing environment and the test drive to allow disk imaging tools to acquire disk images. The evaluation followed a set of procedures. Most of the tests followed generic procedures defined in Appendix 4. The generic procedures had to be modified or changed to allow some of the test cases to be completed. At the beginning and the end of each test case, the test drive or evidence drive had to be reset. The generic drive reset procedures are specified in Appendix 4 Section 1. After the drive reset, the test drives were setup according to the specification of each individual test case. Once the test drives were properly configured. The disk imaging tools were executed to acquire the test drive and the acquisition result was verified. After the verification, the acquisition results were further analysed in terms of the tool’s responses to each configuration. The generic verification method is to compare the hash values computed before and after acquisition. In some test cases, extra verification methods were used to confirm the results. The findings from the tests of three disk imaging tools for each test case are summarised and discussed below.

4.2.2.1 TC-01: Acquiring Various Physical Interfaces

TC-01 involved using different physical interfaces to test if disk imaging tools were able to acquire the digital source using the required physical interfaces. The tested physical interfaces included SATA2, USB and Firewire. Devices were connected to the test station(s) and the three disk imaging tools were used to acquire the test drive and generate a set of image files and log files as output.

Table 4.3

TC-01 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-05, AFR07, AIC01,AIC05, ALOG01-03		
Failed Assertions	None	ALOG02	None
Pass Rate (%)	**100%**	**90.9%**	**100%**

The hash values of the acquired images were compared to the source hashes to check whether they matched. Three disk imaging tools successfully passed all the assertions in three different tested physical interfaces. Table 4.3 shows a summary of the test results for test case TC-01.

4.2.2.2 TC-02: Acquiring Various Digital Sources

Test case TC-02 involved testing whether the disk imaging tools were able to acquire different digital sources correctly. The digital sources tested included NTFS, FAT16, FAT32, EXT2, EXT3, HFS, HFS+ and SWAP. The tests have found that all three disk imaging tools tested were able to acquire all data correctly from different digital sources. Table 4.4 shows a summary of the test results for test case TC-02.

Table 4.4

TC-02 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-05, AFR07, AIC01,AIC05, ALOG01-03		
Failed Assertions	None	**ALOG02**	None
Pass Rate (%)	**100%**	**90.9%**	**100%**

The test has found that Helix 3 Pro was not able to recognise either digital source HFS or HFS+ when acquiring the test drive.

4.2.2.3 TC-03: Acquiring A Hard Drive With Hidden Sectors

Test case TC-03 involved testing if the tested disk imaging tools were able to acquire the hidden sectors configured in the test drive. Certain amount of sectors in the test drive was configured as hidden using HPA configuration.

Table 4.5 shows that all three disk imaging tools were failed to acquire the HPA or DCO hidden area in the test drive. However, all the data that were accessible were acquired correctly by all three tested tools. FTK Imager was crashed twice when acquiring the DCO configured test drive (see Section 1.12 in Appendix 7).

Table 4.5

TC-03 Result Summary

	FTK Imager		**Helix 3 Pro**		**AIR**	
Test Cases	**HPA**	**DCO**	**HPA**	**DCO**	**HPA**	**DCO**
Tested Assertions	AFR01-07, AIC01-02, AIC05-08, ALOG01-03, AHS01-03					
Failed Assertions	**AFR06, AHS01-03**		**AFR06, AHS01-03, ALOG02**		**AFR06, AHS01-03**	
Pass Rate (%)	**85%**		**75%**		**85%**	

The program was crashed when FTK Imager was attempting to create a list of directories of the acquired data. The debugging information of the crash is provided by FTK Imager.

4.2.2.4 TC-05: Acquiring A Digital Source In An Alternative Supported Format

Test case TC-05 involved testing if the disk imaging tools were able to produce complete and accurate image files in alternative supported format. Not all the tested tools support more than one format. The image format dd is supported by all tools. FTK Imager supports the most alternative image formats, which are dd, SMART and Encase E01. AIR supports dd and dc3dd image formats and Helix 3 pro supports dd and Encase E01 formats.

Table 4.6

TC-05 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-05, AFR07, AIC01-02, ALOG01-03		
Failed Assertions	None	ALOG01-02	None
Pass Rate (%)	**100%**	**81.81%**	**100%**

Table 4.6 provides a summary of the results of test case TC-05. During the testing of Test case TC-05, FTK Imager and AIR were able to acquire the digital source correctly in all supported alternative formats. Helix 3 Pro was able to acquire successfully the data of the supported formats. However, the verification based on comparison between the source and acquired data was not performed (see Section 2.12 in Appendix 7).

4.2.2.5 TC-06: Acquiring A Digital Source With Unresolved Read Error

Test case TC-06 tested whether the tested disk imaging tools would notify the user about unresolved read error and would attempt to recover the data. Program MHDD was utilised to mark the sectors as "bad sectors" so they could be remapped to spare sectors on the drive. Fifteen sectors were marked with UNC error (refer to sections 1.16, 2.13 and 3.13 in Appendix 7 for more details). FTK Imager AIR have passed this test and all the assertions were fulfilled. Table 4.7 has shown the summary of the test case TC-06 results.

Alternative verification method was employed to verify whether the disk imaging tools had replaced the inaccessible data sectors with value 0 as they were described. Hex editor UltraEdit was used to check each pre-configured data sector that had UNC error and to confirm whether the sector had been replaced with pre-configured value. All three disk imaging tools had replaced the inaccessible data sector with value 0.

Table 4.7

TC-06 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-05, AFR07-09, AIC01-03, AIC06-08, ALOG01-03		
Failed Assertions	None	**AFR08, ALOG02**	None
Pass Rate (%)	**100%**	**81.81%**	**100%**

FTK Imager and AIR were able to notify the user about the type and location of the error and the content was replaced with binary value Zero. Helix3 Pro was able to recognise the UNC error and replace the inaccessible sector with binary Zero during the data acquisition. However, the type and location of the error were not reported to the user and recorded in the log file.

4.2.2.6 TC-07 & TC-08: Insufficient Space At Destination Device

Test case TC-06 involved testing the responses of disk imaging tools when there were insufficient spaces in the destination device to save the image files. FTK Imager and Helix 3 Pro passed this test and all the assertions were fulfilled. Table 4.8(1) and 4.8(2) have shown the results of test case TC-07 & TC-08 respectively.

Table 4.8(1)

TC-07 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-04, AIC04, ALOG01-03		
Failed Assertions	None	**ALOG02**	**AIC04**
Pass Rate (%)	**100%**	**87.5%**	**87.5%**

FTK Imager notified the user about the insufficient storage space in the destination and offered an alternative location to continue the imaging process. Helix 3 Pro provided space checking prior the disk imaging and notified that the user the destination drive did not have enough space.

Table 4.8(2)

TC-08 Result Summary

	FTK Imager	**Helix 3 Pro**	**AIR**
Tested Assertions	AFR01-05, AFR07, AIC04-05, AIC10, ALOG01-03		
Failed Assertions	None	**AIC-10, ALOG02**	**AIC04, AIC10 ALOG02**
Pass Rate (%)	**100%**	**83.33%**	**75%**

AIR tool failed to achieve the expected result of this test. The imaging process of AIR tool started the acquisition process for about and after a few seconds the process stopped supposedly when it was discovered that the destination device did not have enough storage space. No notification was issued to the user about insufficient space in the destination and no record in the log file indicated why the program stopped.

4.2.2.7 TC-09: Verify A Correct Image

Test case TC-09 involved testing whether the image verification function provided by the tool run correctly. This test case only applied to FTK Imager because it was because the only imaging tool that supported the function. Table 4.9 shows the test results of FTK Imager in test case TC-09.

Table 4.9

TC-09 Result Summary

	FTK Imager
Tested Assertions	AFR03, AIC06, ALOG01-03
Failed Assertions	None
Pass Rate (%)	**100%**

FTK Imager successfully verified the corrupt image file of FAT16 partition. The verification hash values matched the source hash values.

4.2.2.8 TC-10: Verify A Corrupted Image

Test case TC-10 involved testing whether FTK Imager was capable to identify the corrupted image. This test case only applied to FTK Imager because it was the only imaging tool that supported the function. Hex editor was used in the test case to change the data in the image file where the hex value of address 35df5f70h offset 8 was changed from value 43 to 42. Table 4.10 shows the test result of FTK Imager in test case TC-10.

Table 4.10

TC-10 Result Summary

	FTK Imager
Tested Assertions	AFR03, AIC06-08, ALOG01-03
Failed Assertions	AIC08
Pass Rate (%)	**85.71%**

FTK Imager successfully detected that the image files had been corrupted. The verification hash values did not match the source hash values. However, the location of the corrupted data was not reported to the user.

4.2.2.9 TC-11: Converting Existing Image Files To Another Image Format

Test case TC-11 involved testing whether the disk imaging tool could convert an existing image file to another supported image file format. This test case only applied to FTK Imager because it was the only imaging tool that supported the function. FTK Imager supported three different image formats; therefore, six combinations of format conversions were derived for testing.

Table 4.11

TC-11 Result Summary

	FTK Imager					
Test Cases	**DD to Smart**	**DD to E01**	**E01 to DD**	**E01 to SMART**	**SMART to E01**	**SMART to DD**
Tested Assertions	AFR03, AFR09, ALOG01-03					
Failed Assertions	None					
Pass Rate (%)	**100%**					

FTK Imager successfully converted from one image format to another in all six cases. All verification hashes were matched the source hashes.

4.2.2.10 TC-12 (1&2): Acquiring Partition that is Partially Or Completely Hidden

Test case TC-12 involved testing the responses of the disk imaging tools when they encountered partitions that either were partially or completely hidden with the help of HPA configuration. In the configuration of the test drive, partition FAT32 was setup either partially or completely hidden through using HPA configuration. All three tested tools attempted to acquire the hidden partition instead of the entire test drive. All three evaluated tools failed to detect and acquire the hidden sectors that existed in the test drive. Table 4.12 shows the test results of both test cases-TC-12(1) with partially hidden partition and TC-12(2) with completely hidden partition.

Table 4.12

TC-12 Result Summary

	FTK Imager		**Helix 3 Pro**		**AIR**	
Test Cases	**TC-12(1) Partial**	**TC-12(2) Complete**	**TC-12(1) Partial**	**TC-12(2) Complete**	**TC-12(1) Partial**	**TC-12(2) Complete**
Tested Assertions	AFR01-07, AIC01-02, AIC05-08, ALOG01-03, AHS01-03					
Failed	AFR06	**EXCEPT**	AFR05-06 Failed		AFR06, AHS01-03	

Assertions	AHS01-03	AFR01-03	AFR01-04, AIC02 Passed Others are N/A	
Pass Rate (%)	**78.95%**	**15.79%**	**28.57%**	**78.95%**

Instead of reporting that the partition was partially hidden, FTK Imager reported to the user that imaging failed with error of “block index out of bounds”. FTK Imager froze at the stage of preparing to create image, when the program was trying to acquire the completely hidden FAT32 partition (see Sections 1.26 and 1.27 in Appendix 7).

Helix 3 Pro was not able to complete the entire imaging process. In the test case TC-12(1) of partially hidden area, Helix 3 Pro was acquiring the image at an extremely slow speed. The imaging process was stopped by the tester 20 hours into the imaging process since the time for imaging an 80GB hard drive was considered unreasonable. In the case where the partition was completely hidden, Helix 3 Pro was not able to recognise the partition table of the hidden partition.

AIR was not able to detect and acquire the hidden data in the test drive. In the test of partially hidden partition, AIR was able to acquire all the accessible data correctly. On the other hand, AIR tool stopped instantly when it attempted to acquire the completely hidden partition.

4.2.2.11 TC-13: Acquiring Overlapping Partitions

Test case TC-13 involved testing whether the disk imaging tools were able to acquire two partitions that had overlapping boundaries (The ending address of partition A was positioned after the starting address of Partition B). Table 4.13 shows the test results of test case TC-13.

FTK Imager was able to recover the partition table and display the correct information to the user. All the data acquired were correct and complete. However, the irregularity of the partition table was not reported to the user.

Table 4.13

TC-13 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-05, AFR07, AIC01-02, AIC11, ALOG01-03		
Failed Assertions	AIC11	AIC11, ALOG02	AIC11
Pass Rate (%)	**91.67%**	**83.33%**	**91.67%**

Helix 3 pro was unable to recover the partition table and the irregularity of the partition table was not reported to the user. However, all the data were acquired correctly and completely.

AIR failed to report to the user that irregularities were detected in the digital source. However, all the data were acquired correctly and completely.

4.2.2.12 TC-14: Partition Out Of Physical Boundary

Test case TC-14 involved testing whether the disk imaging tools were capable to acquire a partition whose end address was outside the physical boundary. The end address of a partition was set to 156,350,047 but the physical boundary of the drive was 156,301,488. Table 4.14 shows the test results of test case TC-14.

Table 4.14

TC-14 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-05, AFR07, AIC01-02, AIC11, ALOG01-03		
Failed Assertions	AIC11	AIC11, ALOG02	AIC11
Pass Rate (%)	**91.67%**	**83.33%**	**91.67%**

FTK Imager was able to recover the partition table and display the correct partition information to the user. All the data acquired were correct and complete. However, the fact that the partition ended outside the physical boundary was not reported to the user.

Helix 3 pro was unable to recover the partition table and the fact that the partition ended outside the physical boundary was not reported to the user. However, the data acquired were complete and accurate.

AIR failed to report to the user the irregularities in the digital source. However, the data acquired were complete and accurate.

4.2.2.13 TC-15: Acquiring A Hard Drive With A Unreadable MBR

Test case TC-15 involved testing whether the disk imaging tools were able to acquire the test drive with unreadable Master Boot Record (MBR). The entire 512 byte boot sectors were replaced by value 0. Table 4.15 shows the test results of test case TC-15.

FTK Imager was not able to recognise the partition table existed in the device. The entire device was recognised as unallocated space. The irregularity in the MBR was not reported to the user. However, all the data acquired were complete and accurate.

Table 4.15

TC-15 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-05, AFR07-09, AIC01-02, AIC05-08, AIC11, ALOG01-03		
Failed Assertions	AIC11, ALOG02	AIC11, ALOG02	AIC11
Pass Rate (%)	**88.89%**	**88.89%**	**94.44%**

Helix 3 Pro was not able to recognise the partition table in the device. However, all the data acquired were complete and accurate. The irregularity of the MBR was not reported to the user. AIR was able to acquire all the data in a completed and accurate manner. However, the irregularity of the MBR was not reported to the user.

4.2.2.14 TC-16(1): Acquiring A Single GUID Partition

Test case TC-16(1) involved testing whether the disk imaging tools were able to acquire a single GUID partition. The entire hard drive was created as a GPT disk and six GUID partitions were created. The testing was meant to acquire partition 4 as a NTFS partition. Table 4.16 shows the test results of test case TC-16(1).

Table 4.16

TC-16(1) Result Summary

	FTK Imager	**Helix 3 Pro**	**AIR**
Tested Assertions	AFR01-05, AFR07, AIC01-02, AIC05-08, ALOG01-03		
Failed Assertions	None	AFR-01 & 03 Passed AFR-02 FAILED Others are N/A	None
Pass Rate (%)	**100%**	**33.33%**	**100%**

FTK Imager was able to read the partition information from the test drive and to display it correctly to the user. All data acquired for the NTFS partition were correct and complete. Helix 3 Pro was not able to identify the six pre-configured GUID partitions in the test drive. Only the whole drive acquisition option was available. AIR achieved the expected result in this test case. AIR acquired the single GUID partition successfully and the images produced were complete and accurate.

4.2.2.15 TC-16(2): Acquiring A GPT Disk

The pervious test case TC-16(1) tested if the imaging tools were able to acquire a single GUID partition. The test case TC-16(2) tested if the tested tools could acquire a whole GPT disk. FTK Imager displayed to the user the correct partition information of the test drive and all data acquired were correct and complete.

Table 4.17

TC-16(2) Result Summary

	FTK Imager	**Helix 3 Pro**	**AIR**
Tested Assertions	AFR01-05, AFR07, AIC01-02, AIC05-08, ALOG01-03		
Failed Assertions	None	ALOG02	None
Pass Rate (%)	**100%**	**93.33%**	**100%**

Helix 3 Pro was not able to read the partition table information from the test drive. However, all the data acquired were correct and complete. The source hash values matched the verification hash values. AIR achieved the expected result in this test case. AIR acquired the GPT disk successfully and produced accurate and complete image files.

4.2.2.16 TC-17: Acquiring a partially hidden GPT Partition

Test case TC-17 was involved testing whether the disk imaging tools were able to acquire a single GUID partition that was partially hidden through using HPA configuration. The result summary is shown in Table 4.18. The results were similar to those in the test case TC-12(1). All three evaluated tools failed to detect and acquire hidden sectors that existed in the test drive. However, the visible data sectors were all acquired completely and accurately.

Table 4.18

TC-17 Result Summary

	FTK Imager	Helix 3 Pro	AIR
Tested Assertions	AFR01-06,AFR07, AIC01-02, AIC05-08, ALOG01-03, AHS01-03		
Failed Assertions	AFR-06, AHS01-03	AFR-06, AHS01-03 ALOG02	AFR-06, AHS01-03
Pass Rate (%)	**78.95%**	**73.68%**	**78.95%**

FTK Imager reported that the block index was out of bound instead of the partition was partially hidden. Helix 3 Pro was not able to recognise the GUID partition. AIR was able to acquire all the visible data sectors completely and accurately.

4.2.2.17 TC-18: Acquiring Single Partition Using Local Network Connection

Test case TC-18 involved testing if the tools were able to produce complete and accurate images and to transfer them over a locally connected network. Table 4.19 shows a summary of the performance of the three tested tools. This test case only applied to AIR and Helix 3 Pro since FTK did not support image acquisition over network.

Helix 3 Pro was able to acquire a single partition into the specified image format and to transfer it using a local network connection. However, the successful result was only obtained after a few attempts in different operating systems and configurations.

Table 4.19

TC-18 Result Summary

	Helix 3 Pro	AIR
Tested Assertions	AFR01-05,AFR07, AIC01-02, AIC05-08, ALOG01-03	
Failed Assertions	ALOG02	None
Pass Rate (%)	**93.33%**	**100%**

Two problems were encountered in both Windows 7 and Windows XP environments. In the Windows 7 environment, the program crashed with an exception that was not handled properly by the software (see Section 2.23 in Appendix 7). In the Windows XP environment, the program froze when the images were being transferred to the destination over the network (see Section 2.23 in Appendix 7).

4.3 RESEARCH ANALYSIS

The field findings are reported in section 4.2. The section summarises the results and explains the field findings. The field findings are reported on per test case basis and for each test case a table is presented with summarised results for the three tested disk imaging tools.

4.3.1 Analysis Of The Testing Result

The results for each test case presented in section 4.2 are analysed and discussed in this section. A summary of the tool testing results for all test cases is shown in Table 4.20. The pass rate and failed assertions for each test case are displayed in the table.

The method of data analysis is described in section 3.4.3. GA is selected as the method to analyse the data in this research project. According to Table 4.20, The GA matrix can be constructed based on Table 4.20 (see Appendix 6). The Gap of each evaluated tool can be identified as:

Gap = Required Requirements – Actual performance of the Tool

There are few major gaps between three tested tools. None of the three tested tools was able to acquire the disk image in test cases TC-03, TC-12 and TC-17 that involved HPA or DCO configuration. Furthermore, none of the tested tools were able to detect and report to the user the irregularities configured in test cases TC-13 to TC-15 according to the test assertion TSP-AIC-11.

According to the results presented in figure 4.1, FTK Imager achieved the expected test result in more than half of the test cases that were applied. FTK Imager presented problems in areas where hidden areas are existed and where the source drive had irregular configuration. Helix 3 Pro did not achieve the expected result in most of the test cases.

The testing requirements for this research specified that each tested tool was required to provide essential information (such as start and end sectors) to the user in the log file. In the log file of Helix 3 Pro, start and end sectors were not provided as standard output in the log file. Therefore, Helix 3 Pro was marked as failed on the test assertion ALOG-02 in each test case. Some popular file systems and partition table formats, such as HFS, HFS+ and GUID partition table are not supported by Helix 3 Pro. On the other hand, FTK Imager and AIR successfully identified and acquired the file system types and partition table that were not supported by Helix 3 Pro. AIR also presented few problems during the evaluation. Whenever there was a problem, AIR would stop the acquisition process immediately and no information as to why the process had stopped would be provided to the user. For example, when the destination device did not have enough storage space to store the image files, AIR program would stop immediately and would not provide information to the user why the process terminated.

Table 4.20

Summary of Tools Testing Results

Test Cases	FTK		Helix3 Pro		AIR	
	Pass Rate	Failed Assertions	Pass Rate	Failed Assertions	Pass Rate	Failed Assertions
TC-01	100%	None	90.90%	ALOG02	100%	None
TC-02	100%	None	90.90%	ALOG02	100%	None
TC-03	85%	AFR06 AHS01-03	75.00%	AFR06 AHS01-03 ALOG02	85.00%	AFR06 AHS01-03
TC-05	100%	None	81.81%	ALOG01-02	100%	None
TC-06	100%	None	81.81%	AFR08 ALOG02	100%	None
TC-07	100%	None	87.50%	ALOG02	87.50%	AIC04
TC-08	100%	None	83.33%	AIC-10 ALOG02	75.00%	AIC04 AIC10 ALOG02
TC-09	100%	None	N/A	N/A	N/A	N/A
TC-10	85.71%	AIC08	N/A	N/A	N/A	N/A
TC-11	100%	None	N/A	N/A	N/A	N/A
TC-12(1)	78.95%	AFR06 AHS01-03	28.57%	AFR05-06 AHS01-03	78.95%	AFR06 AHS01-03
TC-12(2)	15.79%	EXCEPT AFR01-03	28.57%	AFR05-06	78.95%	AFR06 AHS01-03
TC-13	91.67%	AIC11	83.33%	AIC11 ALOG02	91.67%	AIC11
TC-14	91.67%	AIC11	83.33%	AIC11 ALOG02	91.67%	AIC11
TC-15	88.89%	AIC11 ALOG02	88.89%	AIC11 ALOG02	94.44%	AIC11
TC-16(1)	100%	None	33.33%	AFR-01 & 03	100%	None
TC-16(2)	100%	None	93.33%	ALOG02	100%	None
TC-17	78.95%	AFR-06 AHS01-03	73.68%	AFR-06 AHS01-03 ALOG02	78.95%	AFR-06 AHS01-03
	N/A	N/A	93.33%	ALOG02	100%	None
Overall Passed Rate (Common Test Cases)	88.73%		73.62%		90.81%	

4.4 PRESENTATION OF FINDINGS

A summary of the field findings of section 4.2 is presented in graphic form to help the reader understand the test results better. The evaluation results of the three evaluated tools are presented as a bar chart in Figure 4.4.

Figures 4.1 to 4.3 represent the individual evaluation results of tools FTK Imager, Helix 3 Pro and AIR in the test cases that were applied to them. As mentioned previously, each tool may have different test cases specifically applied. Therefore, the test result of each tool is presented in their individual figure. Figure 4.4 is a comparison chart of the results obtained for three evaluated tools in each of test cases. The number of test cases performed for each tool depends on the functions that the tool provided. FTK Imager had 18 test cases tested versus 15 test cases for Helix 3 Pro and AIR. The horizontal axis in Figure 4.1 to 4.3 represents the test cases that applied to each individual tool. The horizontal axis in Figure 4.4 represents the test cases that tested all three tested disk imaging tools. The vertical axis in Figure 4.1 to 4.4 represents the pass rate of all test cases in percentage. The percentage is derived from the total number of passed assertions divided by the total number of tested assertions.
Figure 4.1 indicates that FTK Imager passed many test cases with 100% pass rate and its worst performance was in test case TC-12(2). According to Figure 4.2, Helix 3 Pro did not achieve 100% pass rate and in three of the test cases, namely TC-12(1), TC-12(2) and TC-16(1), it had a pass rate lower than 35% pass rate. Figure 4.3 shows that AIR reached over 75% pass rate overall performance across all applied test cases. Figure 4.4 indicates that FTK Imager and AIR outperform Helix 3 Pro. Helix 3 Pro has lower than 35% pass rate in three tests, whereas AIR has more than 75% of pass rate in every test case and FTK Imager has average pass rate over 70%. The overall pass rate in the common test cases indicates AIR outperforms FTK Imager and Helix 3 Pro.

4.5 CONCLUSION

Chapter 4 concentrates on reporting the various findings during the process of evaluating the tools. Certain variations of what is defined in Chapter 3 were expected during the evaluation. The main focus of Chapter 4 is on reporting and comparing the evaluation results of the three tested tool in each test scenario, as well as across all tests.

Chapter 4 outlines the variations in research specifications defined in Chapter 3. The findings about the test environment are described in section 4.2.1. Total of 18 test cases are reported but not all of the evaluated tools underwent all 18 test cases. Some test cases only applied to one or two tools. Each test scenario is illustrated with a table that summarises the failed assertions and the pass rate of that particular test case. In section 4.3, GA is applied on the test results of the disk imaging tools to study the gaps between the pre-defined requirements and the actual performance of the tool. A separate table that summarises the test results of all test scenarios is also presented in Table 4.20.

Figures from 4.1 to 4.4 are visual representations of the summary Table 4.20 and they present the individual test results of the test cases. The findings of the evaluation are discussed in detail in Chapter 5. They are also use as evidence to test the hypotheses and answer the research question.

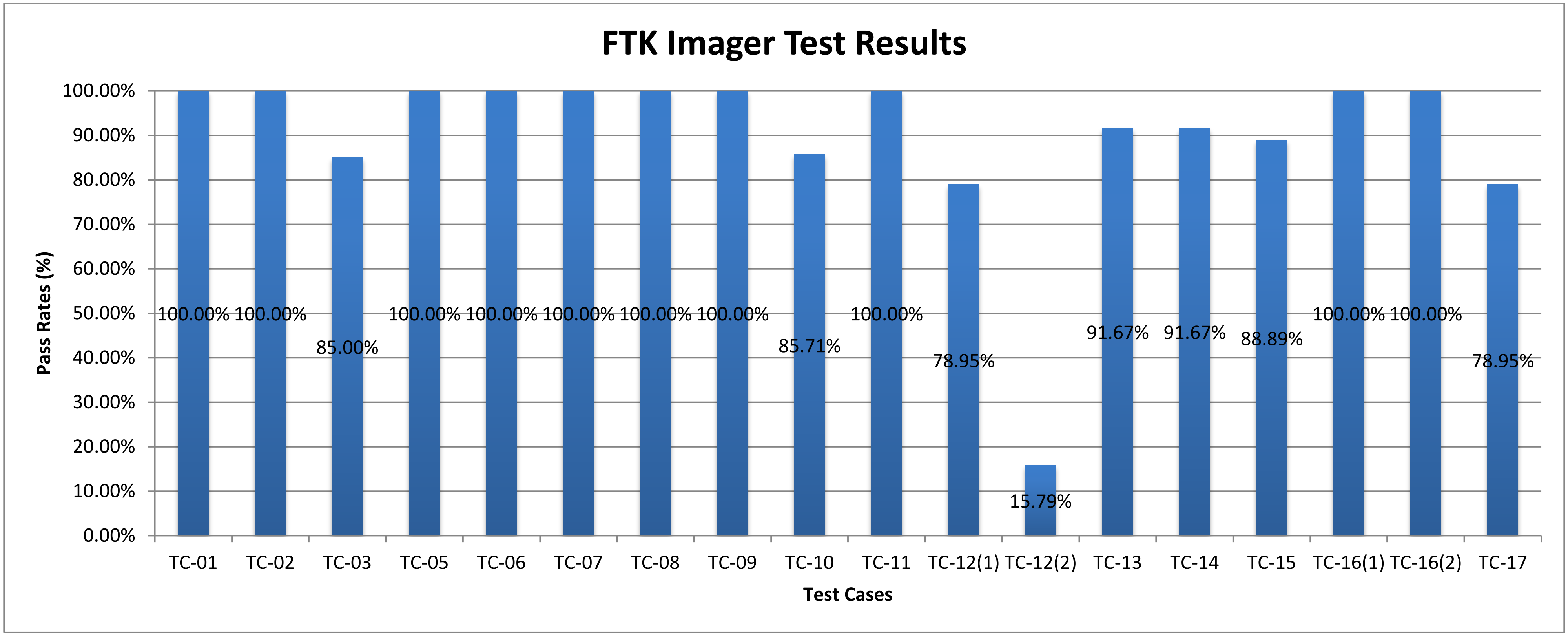


Figure 4.1. **Summary of FTK Imager Test Result**

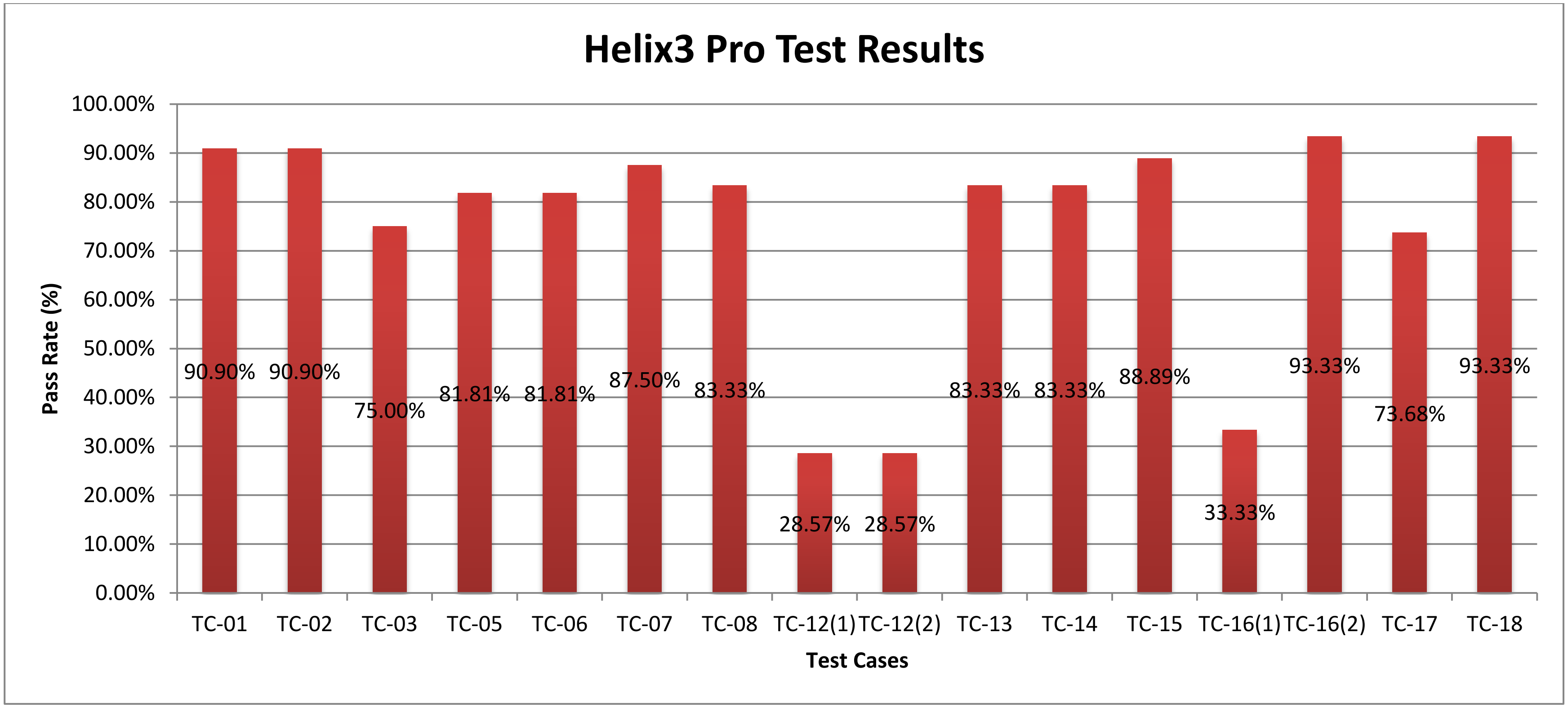


Figure 4.2. **Summary of Helix 3 Pro Test Results**

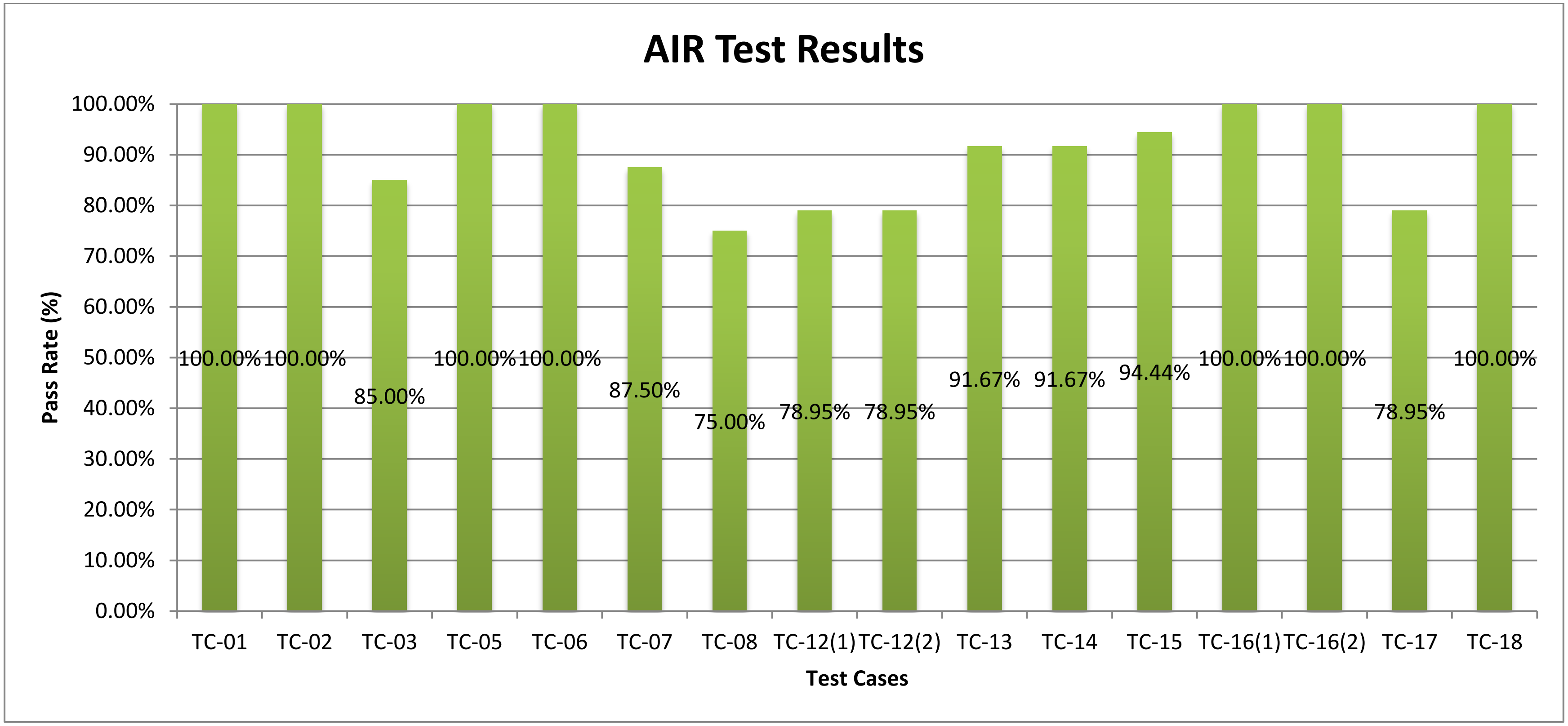
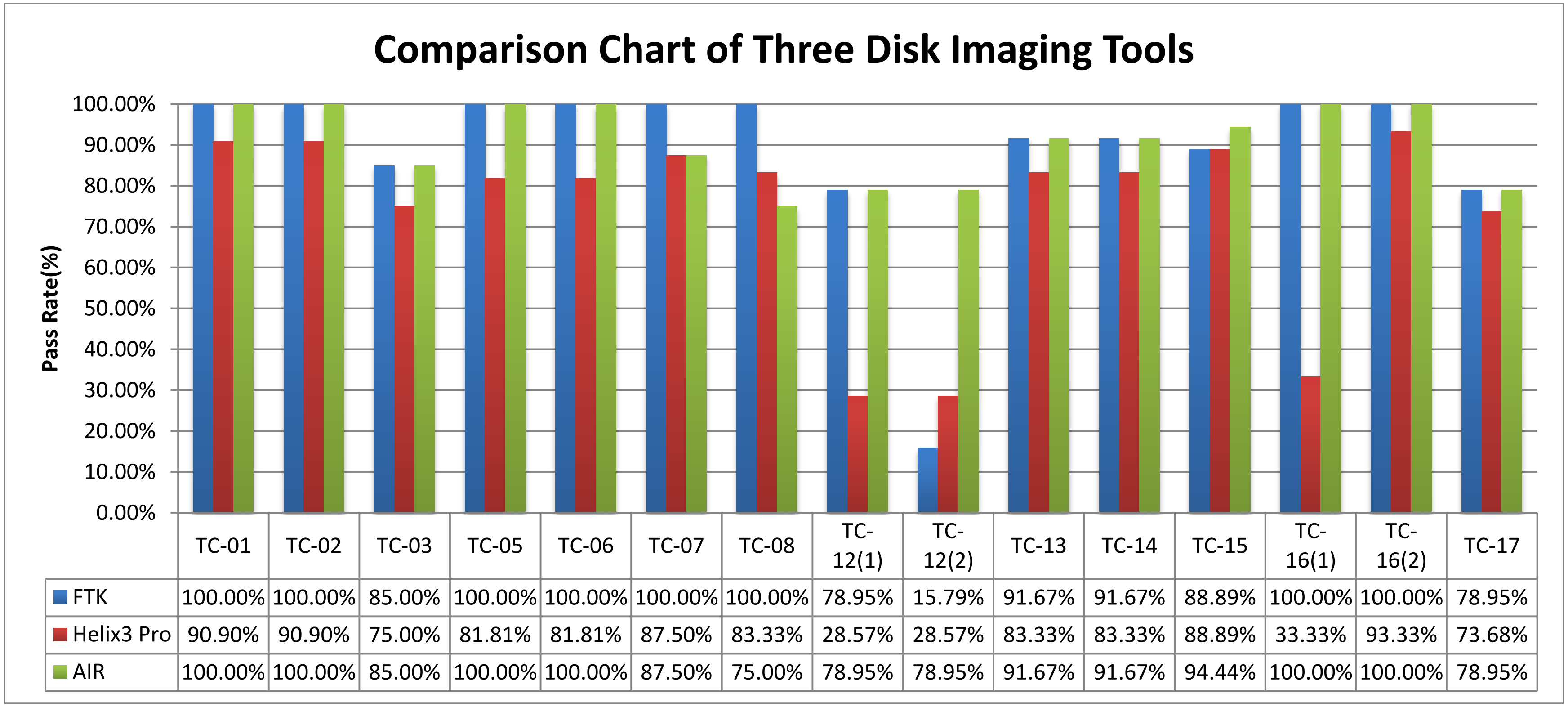


Figure 4.3. **Summary of AIR Test Results**



	TC-01	TC-02	TC-03	TC-05	TC-06	TC-07	TC-08	TC-12(1)	TC-12(2)	TC-13	TC-14	TC-15	TC-16(1)	TC-16(2)	TC-17
🟦 FTK	100.00%	100.00%	85.00%	100.00%	100.00%	100.00%	100.00%	78.95%	15.79%	91.67%	91.67%	88.89%	100.00%	100.00%	78.95%
🟥 Helix3 Pro	90.90%	90.90%	75.00%	81.81%	81.81%	87.50%	83.33%	28.57%	28.57%	83.33%	83.33%	88.89%	33.33%	93.33%	73.68%
🟩 AIR	100.00%	100.00%	85.00%	100.00%	100.00%	87.50%	75.00%	78.95%	78.95%	91.67%	91.67%	94.44%	100.00%	100.00%	78.95%

Figure 4.4. **Summary of Three Disk Imaging Tools**

Chapter 5

Discussion of Findings

5.0 INTRODUCTION

The main research question is concerned with the performance of the disk imaging tools in terms of their accuracy and completeness. An extensive review of related literature is conducted and presented in Chapter 2. Chapter 3 defines the research questions and model and the tool testing methodology. According to the research methodology, a comprehensive testing of three different tools in various test scenarios has been completed and the findings are presented in Chapter 4. When the main research question is defined, some sub-questions are also raised about how to measure and what metrics should be used to test the validity of disk imaging tools.

The findings for each tested disk imaging tool are reported in Chapter 3. The research encountered some problems and challenges in the setup of the testing environment and configuration for different test scenarios. Chapter 3 reports the findings from the tools testing and discusses their significance. Analysis is performed on the findings obtained from the test environment setup and configuration for different scenarios as well. The implications of research challenges and problems will be further discussed and studied in section 5.1.6. Different hypotheses are proposed in Chapter 3 to answer the main research question. The proposed hypotheses can be tested based on the findings from the selected tools evaluation.

Chapter 5 contains two main sections: discussion of findings from the disk imaging tools testing and evaluation of hypotheses. The discussion of evaluation findings includes the discussion of the test environment and the performance testing procedures. It is followed by the analysis of the results for the three tested disk imaging tools. The present research is compared with other studies in this area and the implications of the research challenges are also outlined. The subsequent section is a review of how hypotheses are tested, followed by a conclusion.

5.1 DISCUSSION OF THE FINDINGS FROM TOOLS TESTING

This section discusses the findings from the testing of three disk imaging tools in the present research. The section first discusses the settings, configurations and problems of the testing environment and then describes the tool testing procedures. The findings for each tested disk imaging tool are discussed and reviewed in separate sections, followed by the discussion of the research challenges and how the research differs from other related studies.

As a result of the review of some previous studies in this domain, a group of programs were selected and adopted as configuration tools to create an appropriate testing environment for testing the disk imaging tools. The selected configuration tools were the best possible tools that were available in the research. However, most of the configuration tools were not meant to be used for the purpose of configuring environments for digital forensic software testing. Programs such as MHDD and HDAT2 have been designed to test or to diagnose storage devices. These tools were utilised as hard drive manipulation tools to configure a proper testing environment. Both MHDD and Hdat2 were used to configure Hidden areas HPA. However, when Hdat2 was utilised to create HPA, the HPA could not be recognised by MHDD and vice versa. The reason was unknown and the developer has been informed of the problem. Unfortunately, the developer could not determine the exact cause for this problem. Hex editor UltraEdit was used as a verification tool to ensure that the disk imaging tools had replaced the inaccessible data with a specified value. EnCase was also used as a verification tool to verify the hash values of the image files acquired by the disk imaging tools that were subjected to test.

Both CFTT programs from NIST and research from Byers & Shahmehri (2009) have developed their own configuration tools to meet the requirements of their tool testing. However, the tools developed by other researchers could not fully meet the requirements of this research. Resources were also limited for the development of customised configuration and verification tools that could fully fulfil the research requirements. The type and number of tests that could be ran on the tested tools were constrained by the availability and functionality of the configuration and verification tools. For instance, the test case TC-04 could not be performed because the tools that could manipulate a faulty data sector were not available.

5.1.1 Disk Imaging Tools Testing Procedures

The disk imaging tool testing procedures are summarised in Table 5.1. The first step needed to reset the test drive at the beginning to ensure that no data from previous use still remained in the hard drive. Normal reformatting of the storage device does not guarantee that all the data in the device are completely removed. A program called Darik's Boot and Nuke were used in order to wipe the test drive securely to a clean state.

The second step of the tool evaluation procedure was the configuration of the test drive. After the configuring the test drive to the appropriate test state, the entire drive was hashed with the utilisation of EnCase and the computed hash values (MD5 and SHA1) were considered as source hashes. Hardware write blocker was used after the source hashes had been computed. This tactic ensured that no change would be made on the test drive after they had been configured to the proper testing state. In some cases, SHA512 could be used instead of SHA1 and this should not affect the end result. The concern in this procedure was that hashing was not computed for the entire drive in the HPA or DCO active test drives. Only the accessible areas were hashed. The removal of the HPA or DCO active areas was inconsistent with the testing purpose of the test. Standardised forensic procedures were followed when the test drive was acquired or imaged. Segmented image files were generated and stored in the designated destination. The hardware write blocker was utilised consistently with pre-specified test cases as the exception (to prevent any tampering of the test drive). Hashes were calculated after every acquisition and the acquisition logs were properly stored and documented.

Step 4 was specifically designed in this research to verify the accuracy of the acquired images. The hash values of the acquired images were verified again by the use of EnCase to assure that the values generated by the disk imaging tools were accurate.

Table 5.1

Tool Evaluation Procedure

Evaluation Procedure	Actions Taken
Step 1. Drive Reset	Wipe out the test drive with DoD method
Step 2. Configure Test Drive	Drive (UNC error, HPA and/or DCO) and Partition setup
Step 3. Perform Data Acquisition	Write-blocked device will be hashed before the acquisition. Windows or Linux data acquisition of the test drive.
Step 4. Perform Result Verification	Verify the correctness of the acquired images. Image files are verified again by using EnCase.
Step 5. Drive Cleanup	Remove any effect on the test drive and prepare the test drive for the following tests

When testing some special test cases, some other software were utilised as verification tools to confirm the results. In the final steps, any effects that were rendered upon the test drive would be reversed and the data would be securely wiped out to prepare for the execution of other test cases.

5.1.2 FTK Imager

FTK Imager achieved the expected results in 11 out of 17 test cases in this research. According to the NIJ (2008a) report, FTK Imager (version 2.5.3.14) was not able to acquire a completed logical copy of the NTFS partition and the last eight sectors of the test drive were omitted from the acquisition. However, a similar problem was not found in the newer version (2.9.0.1385) of FTK Imager that this research evaluated.

In the test case TC-03 where hidden sectors existed, FTK Imager could not detect and acquire the designed hidden sectors. The findings of test case TC-03 do not contradict the result presented in the NIJ (2008a) report. The matter of HPA and DCO acquisition is not clearly stated in the FTK Imager user manual. Email communication was established with the AccessData support team regarding the matter of HPA and/or DCO acquisition. They responded by stating that FTK Imager is currently not able to support HPA while DCO acquisition and the function will be added in the future release.

In the test case TC-10, FTK Imager was able to successfully identify that disk images were corrupted but was not able to report the location of corrupted data to the user. In their latest FTK Imager release notes (AccessData, n.d., p.6) mentioned that FTK Imager now reports the location of any corrupted data in the image (when possible). The location of corrupted data was not reported to the user during the evaluation. The release notes from AccessData does not clearly state that the condition of when the software will report the location to the user about the corrupted data in the image. Knowledge of the location of the corrupted data would be helpful for the investigator or user so they would know of what kind of data might be unavailable.

In the test case TC-12 where partition was partially or completely hidden by using HPA configuration, FTK Imager presented some problems. The partition deployed for testing was started from sector 149,565,150 to 156,296,384. The HPA area was set from sector 150,301,488 to the last sector of the drive 156,301,488. FTK Imager reported to the user that the test was failed with error "Block Indexes out of bounds" (see Appendix 7 section 1.26). However, the test case was set up to check whether the disk imaging tool could identify that the partition had been partially hidden by HPA. However, FTK Imager was still able to detect the correct partition information and acquire the 736,338 visible sectors. Furthermore, FTK Imager failed to operate when attempting to acquire the completely hidden FAT32 partition. FTK Imager stopped functioning during the preliminary process of image-forming (See Appendix 7 section 1.27). When FTK Imager was attempting to read the partition, the access was denied by the hard disk controller. Appropriate ATA command SEX MAX ADDRESS had to be issued to the hard disk controller to restore the size of the hard disk to its original size. FTK Imager should have recognised that the partition was not accessible and should have issue appropriate error message to the user instead of trying to access the partition repeatedly, which could render the program unresponsive. FTK Imager crashed whenever an attempt to create list of file directories was initiated and whenever hidden areas were presented in Windows 7 environment. Error of type "memory access violation" occurred. The problem is believed to have originated in the program during the programming stage. Unhandled exceptions could affect the stability of a program adversely and it could also force the program to exit in some cases. The directory list creation commenced after the imaging process but worked concurrently with image verification process. The research did not overlook the possibility that the verification process could be dysfunctional if the program was unstable, although this was not the case during the evaluation.

Test case TC-14, TC-15 and TC-16 were designed to test the responses of the FTK Imager when irregular configurations were present in the hard disk. FTK Imager did not report to the user any of the irregularities configured in the hard disk. However, in cases where configuration of irregularities existed, all the visible data were acquired correctly and verified. The tool should have notified any irregularities of the hard disk because the irregularities might generate unreadable data or data corruption in some cases. Byers & Shahmehri (2009, p.20(23)) stated that the existence of configuration irregularity in the digital source might lead to data acquisition unviable. For example, if the signature of the Master Boot Record is not the hexadecimal value 0xAA55, the partition table will not be recognised. In most cases, disk imaging tool will recognise the data as unallocated space. The MBR signature can be simply modified or changed with the assistance of any Hex Editors such as UltraEdit. A simple modification of the drive can create barriers for the forensic investigator to boot from the drive if a clone has been created based on the evidence drive. Booting the drive to its operating system is still important even if evidence can be analysed without booting the drive using Forensics toolkits such as EnCase or FTK. Investigators can recreate the work environment using virtual machine to analyse evidence. However, this will not be viable if the MBR signature is modified.

5.1.3 Helix 3 Pro

Helix 3 Pro did not achieve 100% pass rate in any of the test cases. This can be explained by the fact that testing assertion TSP-ALOG-02 in the testing requirement required that the tool should provide the user with some essential information regarding the acquisition. The information provided by the tool should include information such as start and end sectors, start and end time of the acquisition. However, Helix 3 Pro did not provide any information in the log file regarding the amount of data that had been acquired from the digital source. The user may obtain the information of the total number of sectors that had been acquired by calculating the size and number of image files generated by the tool and converting it to the sector. The calculation is beyond the scope of this research. The tool is able to obtain the information when acquiring the digital source but choosing whether to record the information in the log file was the choice of the tool. The information is important for the forensic investigators. With more relevant information provided by the disk imaging tools, forensic investigator will have more chance to locate and capture crucial information from the digital evidence.

Helix 3 Pro supports EnCase version 4, 5 and 6 as alternative disk image formats besides raw image format. Helix 3 Pro successfully acquired the digital source to EnCase version 6 format during the testing. However, the log file that Helix 3 Pro generated did not clearly state that verification had been performed like the log file generated in raw image format. The hash value was only calculated over the acquired data but not on the digital source. The user could not ascertain whether the acquired data was a bit-by-bit copy of the digital source. Forensic investigators may rely on the log file generated as part of the evidence or audit trails by the tool. Users may be required to take extra steps to verify the hash values of both acquired and source data. It is not a major flaw of the software because when the tool acquiring the source to image files, both hash values could be calculated. The tool should clearly indicate that integrity has been verified on both acquired and digital source.

Helix 3 Pro failed to acquire hidden sectors configured in cases where HPA or DCO setting was used. The fact that FTK Imager and AIR imaging tools also failed in the same test should be noted. In the test case where Helix 3 Pro acquired hidden areas, it was not able to obtain the partition table information of the hard disk whereas the other two tools were able to perform this task. Helix 3 Pro's performance was unsatisfactory in the test case TC-12 where partially and completely hidden partitions were involved. Helix 3 Pro was not able to complete the acquisition process within a reasonable timeframe. The tool acquired the digital source at an extremely slow speed when it encountered the hidden partition. The tool was attempting to access the hidden data in the same way as FTK Imager in the same case. Appropriate error message should have issued to notify the user of the situation when an excessive amount of unreadable data is presented. Otherwise, the user would assume that the tool is making attempts to recover problematic sectors in the digital source.

When the Helix 3 Pro tested in the case (TC-06) where the hard disk contained unresolved errors, the program did not report the errors that occurred during the acquisition process and when the inaccessible data sectors had been replaced with the pre-configured value. The location and the type of errors had to be reported to the user; otherwise, the user would be unlikely to have any knowledge of what data were not acquirable during the acquisition. An investigation may be compromised if the investigator was incapable of accounting for the lost data, which might constitute some critical evidence.

GUID partition table is not supported by Helix 3 Pro and this is not a flaw of the program. However, it is useful to add different partition types to the program to extend the capabilities of Helix 3 Pro in order to suit different environments. As suggested in the review of literature in section 2.3.4, GUID partition table possesses many advantages over MBR. For instance, the limitation of the maximum disk size is up from 2TB in MBR to 9.4 billion TB in GUID. As in the future, the MBR is to be replaced by GUID, the support of GUID partition type will become essential.

The network acquisition function of Helix 3 Pro was unstable during the evaluation. In Windows 7 environment, the program crashed with an unhandled exception which is a programming issue of the software. Similar issues were reported by other users in the support forum of Helix (Staarfanger, 2010). It is noteworthy that Helix 3 Pro is not fully tested in Windows 7 environment. Furthermore, Helix 3 Pro sometimes stopped transferring image files to the destination in a locally networked Windows XP SP3 environment. The cause for the incident is unknown (see Appendix 7 section 2.23 for more details).

Helix 3 Pro also presented some other problems during the evaluation. It had a problem when the Tableau T35es Write blocker was used in both the Windows 7 and the Helix Live CD. The acquisition process could not be activated. Helix 3 Pro reported that the source disk could not be initialised. Similar issues were reported by other users in the support forum of Helix (Balzanto, 2010). The support team is aware of the issue and the solution may come in the next release.

Helix 3 Pro presented some usability problems and the user experience could be improved if the solution for those problems is found despite the fact that those problems are not serious. As indicated in Section 2.2.4.2, other researchers have pointed out that CFTT program have omitted the usability problem in their tool evaluation. When using the Helix Live CD, there was a long period (more than a few minutes) after which the traces of moving the desktop window could be removed completely. The progress bar also stopped progressing even when the actual acquisition continued in the background. For example, when the software was acquiring 80GB hard disk, the progress bar was still in the first block even after the acquisition of another 40GB. The progress bar only indicated the single file progress when the image files were being verified. The overall progress of the verification process was not shown to the user and the user had no idea when the verification would be finished. The overall progress and the estimated time to finish should be provided to the user for better experience of the software. In the test case where the acquisition over the network was tested, the receiving side of the image files was clearly provided with the speed of the file transferring and the amount of data left to be transferred. However, the information was not provided to the sender.

5.1.4 AIR

AIR achieved the expected results in 7 out of 15 test cases. AIR also had 75% or over of successful rate in all test cases. However, some problems in the software itself were detected. The major problem for AIR was that no appropriate error message was displayed to the user or in the log file when it emerged during the image acquisition.

In the test case TC-07 and TC-08 where the destination device did not have sufficient storage space, AIR also stopped immediately when it detected space insufficiency at the destination but no message was provided to the user to indicate why the process stopped. AIR did not support the storage of image files on alternative storage devices if the destination device did not have enough storage in the first place. It is not a flaw in the software but it would be useful to have this function in cases where Terabyte disk drives are involved. Section 2.1.3 discusses that digital forensics tools has never been able to cope with ever-increasing and massive data storage capacity. Providing the option to store image files on alternative storage devices is becoming more and more valuable for users.

Unlike FTK and Helix 3 Pro, AIR would not handle HPA and/or DCO hidden areas in test cases TC-03 and TC-12. However, all the visible data sectors were acquired correctly and completely. When AIR detected any partially hidden partition, the program stopped acquiring data at the precise location of the first sector where the hidden area began. AIR stopped also immediately when acquiring the completely hidden partition and indicated that the partition did not exist. AIR indicated in their read file that HPA detection was supported but the detection was only available in the dc3dd common line option. The front-end GUI did not support HPA detection. The hidden area DCO is not mentioned in the read file.

In the test cases TC-13, TC-14 and TC-15, AIR failed to notify the user that the source device had irregular configurations. However, all the visible data sectors were acquired accurately and completely. Report or notification of configuration irregularity is not a compulsory function for the disk imaging tools but the function is useful when the digital source is unreadable. The notification would provide a starting point for troubleshooting if the device is unreadable or if the suspect has changed settings of the disk drive to conceal data.

AIR also presented some problems regarding the software usability that also require solutions. AIR is designed for easily creating forensic images as described in Section 2.1.4.3. The user is not prompted to record information related to a forensic case such as the name of the examiner, case number and description, item number and notes. Those metadata are important and should be saved in a safe location for legal or auditing purposes. Generally, software will allow to record necessary information related to the case. However, the only option provided by AIR is to add comments in the log file. Furthermore, the log file is not automatically saved as a default setting. If the user accidentally closes the window displaying the acquisition result, the only way the log file can be located again is in the temporary folder (assuming the data has not been cleared yet). A proper user manual is also not provided due to the time limitation and the task of creating a user manual is overwhelmingly laborious for the author.

Software support is minimum and the support is provided by submitting help to the Source Forge discussion board or sending email to the author directly.

5.1.5 Comparison With Other Related Studies

A Function Map (see Figure 3.12) was created to assist this research to identify the essential and potential components for testing the disk imaging tools. With more potential components identified, the specification of the testing requirements could become more comprehensive. Guo& Slay (2010) state that Function Mapping provides the level of abstraction that could provide tool testers or forensic software developers with a comprehensive representation of the functions required for the tool.

Sections 3.1.1 and 3.1.2 in Chapter 3 review two previous studies that provided this study with valuable information about how to extensively test disk imaging tools. CFTT program has specified mandatory testing requirements that are taken into account in this research. Some of the optional requirements specified in CFTT program are omitted. Clone creation and Block hashing are excluded from the scope of this research due to the fact that these functions are not available in the disk imaging tools chosen in the present research. Following the review of another research in Section 3.1.2, a section called Hidden Sector is added to the requirements that are considered as an important component of the disk imaging tools testing. The test assertions derived from the requirements for Hidden Sector section are based on the research reviewed in Section 3.1.2 (see Appendix 1 and 3). CFTT specification and assertions are only concerned with the information being accurately logged in the log file but do not specify what log information is essential for the forensic investigation. It has not been measured whether the information displayed by the tool is the same as the information recorded in the log file. Therefore, requirements and correspondent assertions of TSP-RLOG-02 and TSP-RLOG-03 have been added to the research.

In both CFTT (NIST, 2005) and Byers & Shahmehri (2009) studies, GPT partitioning scheme is not included but the popularity of the scheme has been increasing exponentially as indicated in Section 2.3.4. Test cases TC-16 and TC-17 that involve GPT partitions are added. The file systems HFS and HFS+ are also added to the testing requirements. GPT partition and HFS, HFS+ file systems are commonly seen in Apple computers. The number of Apple computers in the market has been increasing exponentially over the past few years. In October 2010, Apple revealed that 3.89 million Macs were sold in the previous quarter (Oliver, 2010, p.1). The number of investigations that involve Apple computers has been expected to increase. Adding such file systems and partition types is a logical choice for the evaluation to expand the testing range and types. Research reviewed in Section 3.1.2 suggests that usability of the disk imaging tools is the area that CFTT program has not addressed. Poor usability of the tools may lead the user to the mistaken action that could possibly affect the acquisition process. For instance, a poorly structured user interface may lead the user to choose wrong acquisition options and may affect the quality of the acquisition. This motivates this research to include usability-related observations in the research discussion.

5.1.6 Research Challenges

A number of technical problems were encountered during the process of tool testing. One of the challenges arose from the tool used to configure the test drive for testing. Hidden areas caused problems because they were automatically removed when booting into the Linux environment. The only write blocker available in the forensics laboratory was from Tableau but the product of this brand would automatically override the test drive if the hidden areas were present. Some of the challenges were posed by the use of Linux Forensics Live CDs during the testing as well.

5.1.6.1 Configuration Tools

One of the challenges of the research is to locate the right tools for the designed test cases. The evaluation requires the researcher to perform low-level manipulation over the test drives. The tools that are available to the researcher and able to meet the researching requirements are limited. As mentioned in section 4.2.1, the tools that are available for the research are not specifically designed for forensic software testing. The tool sets developed by NIST are the only specialised forensic software validation tools that are publicly available. In section 2.2.4, forensics software testing and/or validation are discussed as one of the challenges for the industry and the adoption of such tools to support the validation is technically demanding. As reviewed in section

2.2.4, forensic software validation and verification methodology, techniques and frameworks do exist but the tools to support the process are yet to be developed.

5.1.6.2 HPA or DCO

As reviewed in section 2.3.3, hidden areas such as HPA and DCO are one of the challenging subjects for disk imaging tools. Problems have been encountered during the configuration of the testing environment. Windows and Linux are the two execution environments in the tool evaluation. The disk imaging tool AIR is run in Linux environment. At the beginning of the environment configuration, Ubuntu 10.04 distribution was used as the Linux environment. However, it was soon found that Linux disabled HPA temporarily (although it was restored after a complete power down) during the booting process and this contradicted the purpose of the evaluation. HPA had to be preserved to test the responses of the disk imaging tools. Removing HPA by default can create problems in some cases. For example, some motherboard manufacturers may set up a HPA at the end of the hard drive to store a backup copy of the BIOS to use for restoring corrupted BIOS. Removing the HPA would increase the likelihood of the backup BIOS being overwritten over time. The data might not be overwritten immediately but it will be corrupted eventually if the same operating system has been used for a long period of time. If the disk imaging tool AIR was used to image the evidence hard disk and Ubuntu automatically removed the HPA area in the drive, the HPA would be exposed and the data contained, which may be a key piece of evidence, would be destroyed.

In a hypothetical case, a server is collected from a crime scene as evidence and the data storage of the server is constructed with Redundant Arrays of Inexpensive Disks (RAID). Some of the RAIDs were built based on the something called Firmware RAID or Fake RAID. This kind of RAID does not have the full RAID functionality and relies on dedicated drivers to operate properly (AtlanticLinux, 2009). It should be noted that many users might encounter problems when HPA is removed (during the boot process) and RAID is used simultaneously. An active bug in Ubuntu involves data loss due to HPA being disabled by default (Whitcroft, 2009). The problem stems from the RAID metadata stored in HPA. When the HPA is disabled during the boot process, the data or configuration of the RAID is lost, leading to an unbootable RAID.

Rebuilding the RAID to analyse the drives may become unfeasible if an investigator has used a Live CD with similar HPA issue to boot the drive. Because of all this, another Linux distribution called BackTrack was used in this research to avoid the problem of HPA being disabled by default. The Linux kernel used in BackTrack has been patched to fix the problem.

5.1.6.3 Issue Of Hardware Write Blocker

Another problem that involved HPA hidden areas was with Tableau T35es Write Blocker, the only write blocker that was available in the research laboratory. In test cases that had HPA or DCO hidden areas, no write blocker was used. The standardised forensic acquisition procedure requires a write blocker to be used at all time to prevent any intentional or unintentional tampering with the evidence drive that would be subsequently used in court. The Tableau T35es write blocker is able to detect and override both HPA and DCO hidden areas but this defies the purpose of the testing which is to analyse the behaviour of disk imaging tools when HPA and/or DCO are present. The research made some efforts to prevent any tampering with the test drive. As indicated in Step 3 and 5 shown in Table 5.1, the test drive would be hashed before and after the forensic acquisition. The hash values computed before and after the acquisition had to be matched to verify if data tampering on the test drive had occurred.

5.1.6.4 Linux Forensics Live CDs

Helix 3 Pro is a Linux Forensic toolkit in the Live CD. AIR is also a constituent part of another forensics Live CD toolkit called CAINE. Moll, Prokop, & Morgenstern (2009) argued that Linux forensic toolkits are required to satisfy various requirements. Firstly, the File system of the evidence device should not be automatically mounted at boot up. The swap space (if any) in the evidence drive is not activated. Software RAID arrays on evidence drives is not automatically activated at the operating system boot up process (Maxim, 2009). Maxim (2009) also suggests that all the block devices are set to read-only mode to avoid any write attempts to the evidence drive. Maxim (2009) conducted the testing to assess whether the Linux Forensic Live CDs mount file system during the start-up process. The testing results indicate that BackTrack 4 Prerelease version mounts file systems during the start-up process. However, the problem is not presented in BackTrack 4 final version that was used for the evaluation in this research. Maxim (2009) discovered that some forensic Linux distributions use only "-o ro" option to provide write protection, which is not a forensically sound approach for write blocking. A few methods can be employed to mount the file system in a forensically sound manner. Command "blockdev" can be used to set the block devices to read-only mode (Al-Azhar, 2009). Additionally, "ro,loop" mount option can also be used to set the mounting point to read-only (Maxim, 2009). The loopback mount option was applied during the evaluation in Linux environment and it was only applied in test cases that involved HPA or DCO hidden areas. In the other test cases, the evidence drive was connected to Tableau write blocker at all times.

5.2 HYPOTHESES TESTING

This section lends support or poses challenges to each hypothesis. The hypotheses are adopted to test the performance of the disk imaging tools in the validity testing conducted in the research Phase 4 (see section 3.3). The evidence supporting or challenging the hypotheses is displayed in Table 5.2. The evidence consists of the results obtained from the testing of three disk imaging tools.

Hypothesis H1 is supported. FTK Imager has better or equal performance than other tested disk imaging tools in most of the common test cases. FTK Imager performed better than the other two disk imaging tools in test cases TC-07 and TC-08. FTK Imager successfully notified the user about the insufficient storage space in the destination and offered alternative storage location to continue the imaging process. FTK provided accurate result to the user. On the other hand, AIR Imager and Helix 3 Pro were failed to achieve 100% pass rate. FTK Imager has same pass rate as AIR in most the common test cases. This hypothesis is in line with the author's speculation.

Table 5.2

Hypotheses Testing

Hypotheses	In Favour (Evidence)	Against (Evidence)
H1: FTK Imager will perform better than or equals to the other selected disk imaging tool in most of the common test cases.	**Perform better than others:** TC-07,TC-08 **Perform equals to:** TC-01 to TC-03, TC05 to TC08, TC-12(1), TC-13 to TC-14, TC-16, TC-17	
H2: Helix 3 Pro will perform better than or equals to AIR Imager in most of the common test cases.		TC-01 to TC-06, TC-08, TC-12 to TC-18
H3: AIR will perform better than the other two selected disk imaging tools in very few test cases		**Perform better than others:** TC-12(2), TC-15,TC-18 **Perform equals to:** TC-01 to TC-06, TC-12(1), TC-13 to TC-14, TC-16 to TC-17

Hypothesis H2 is not supported. Helix 3 Pro performed worse than AIR in most of the common test cases. In test case TC-12 where the tool required acquiring hidden partitions, Helix 3 Pro was not able to complete the entire imaging process. Helix 3 Pro only achieved 28.57% passed rate whereas AIR achieved 78.95%. Hence, Helix 3 Pro failed to provide complete information to the user. The incomplete information will lead to the inability of forensic investigator to gain full knowledge of the acquired data. In test case TC-16 where the tool required acquiring a GPT disk, Helix 3 Pro was not able to recognise the partition table. However, AIR acquired the GPT disk successfully and extracted accurate and complete image files. Apart from the two prominent test cases mentioned above, AIR also outperformed Helix 3 Pro in other common test cases. This hypothesis is not in line with author's speculation.

Hypothesis H3 is not supported. AIR was the best performer among the tested tools. AIR has achieved overall pass rate 90.81% whereas FTK Imager and Helix 3 Pro have achieved 88.73% and 73.62%, respectively. In test cases TC-12(2), TC-15 and TC-18, AIR has outperformed other two disk imaging tools. AIR was able to provide accurate and complete result in those test cases. The accuracy of the result is essential for disk imaging tools. Lawyers can challenge the validity of the disk imaging tools and dismiss the relevant evidence if the forensic investigator performed data acquisition by using an improperly validated tool. This hypothesis is not in line with author's speculation.

5.3 CONCLUSION

This Chapter discusses the findings based on the data collected from the evaluation of the disk imaging tools. Testing environment and procedures are discussed as two important elements of the disk imaging tools validation. These two elements have a direct impact on the quality and accuracy of the evaluation result. The significance of the test cases is discussed for each individual tool. The focus of the discussion of each tool is on the failed test cases. The analysis of possible reasons why the tool failed in the particular test cases provides key findings.

Research challenges are discussed with regards to various problem areas. The availability of the configuration tools for the testing environment was limited and it restricted the ability to run different types of test cases for the research. Wider range and types of test cases could improve the accuracy and completeness of the research. The discussion of the challenges posed by using the Linux Forensics Live CDs can alert other researchers if they intend to conduct similar type of research.

The findings of the tools testing imply that the testing requirements, configuration and the performance of the disk imaging tools are closely linked. The research found the performance of the disk imaging tools are vary from case to case. Hypotheses 2 and 3 are not in line with the author's original speculation. AIR is outperformed than other two disk imaging tools and Helix 3 Pro performed the worst among three tools. The author was speculating that Helix 3 pro would perform better because of its reputation and the rich functionalities provided. Apart from the research model depicted in Figure 3.7, the research also investigate the usability of the tools. Problems concerning the usability of the tools are discussed in sections from 5.1.3 to 5.1.5.

The research has made contribution to the tool evaluation research since the forensic industry has a strong demand for a set of configuration tools and a comprehensive evaluation methodology. Other researchers harbour the idea that the challenges and problems are inherent in the research. This research utilises the function mapping approach to uncover potential testing requirements. The study also has summarised the relevant literature related to evaluating disk imaging tools.

Chapter 6

Conclusion

6.0 INTRODUCTION

Chapter 1 identifies the research gaps in digital forensics research and outlines the expected outcome of this research. Digital evidence is generally identified, consolidated and presented by forensic practitioners using various digital forensic tools. The admissibility of the digital evidence extracted by invalidated digital forensics tools is questionable. Digital evidence is generally stored in a storage medium such as a hard disk. Disk imaging is employed to derive electronic information from the electronic devices and such information serve as potential evidence. Any problem that occurs in the process of evidence collection could potentially jeopardise the subsequent investigative processes. The performance of the disk imaging tools has become an issue of immediate concern in the digital forensic community. Chapter 2 has empirically reviewed the context and the development of the disk imaging tool evaluation, which is the research gap identified in Chapter 1.

Five relevant academic journal articles are analysed to find out how such studies were conducted. Research questions and hypotheses are defined to focus on the performance of the disk imaging tools in terms of accuracy and completeness of the extracted data. The functionality-driven approach is selected as a result of studying the relevant journal articles. Chapter 3 expounds the research model, evaluation requirements and specifications for testing the performance of the selected disk imaging tools. Following the specifications defined in Chapter 3, three selected disk imaging tools are evaluated and the research findings are reported in Chapter 4. Research findings are discussed and analysed in Chapter 5 to provide a clear summary of the outcomes of testing. Table 4.20 presented in Chapter 4 provides a definitive summary of the research findings.

The following sections are structured to conclude this research. The research findings are summarised in section 6.1, followed by competent answers to the research questions in section 6.2. Section 6.3 elaborates on the direction of possible follow-up studies before drawing a definitive conclusion.

6.1 SUMMARY OF THE RESEARCH FINDINGS

The findings of this research are pertinent to three areas: the testing environment, evaluation procedures and the performance of each tool. The main issue related to testing environment is the availability of tools used to configure the testing environment. The evaluation procedure involves the utilisation of forensically sound methods to evaluate these tools. The performance of each tool in each test case is compared and contrasted.

The research has found that the disk configuration tools available on the market are not adequate for conducting comprehensive evaluation tests on disk imaging tools. The prototypes of the tools used by this research are not the tools (Gavrila, 2005; Carrier, 2005) used in the CFTT and DFTT program. These tools have been developed exclusively for the evaluation of digital forensic tools. It is important to note that the tools used in this research are not special-built for digital forensic tool testing. What the tools actually do can be uncertain. Specialised tools must be developed to configure a proper testing environment. The limited availability of configuration tools has posed some constraints on the types of test cases that can be conducted for evaluating disk imaging tools. A set of forensically sound testing procedures are constructed. The test drive is wiped with forensically proven method before being used in a test case. Then the test drive is configured according to the test specifications for that particular test case. Once the drive is configured, data is acquired using the selected tools. Extra image files verification is executed again to ensure their integrity. Finally, the test drive is wiped and any effects from the configuration on the drive are removed to ensure that no data are left to affect the following test cases. The research also finds that HPA or DCO hidden areas can be overridden before the data can be acquired when these areas are connected to some of the forensic write blockers. In the test cases that involve hidden areas, no write blocker is used and only the visible data are hashed and verified after the data has been acquired.

The research has found that FTK Imager has no longer the problem that existed previously and was reported by NIST regarding version 2.5.3.14. It is also found that the actual report of the data acquired when scanning corrupted image files is inconsistent with what is stated in the user manual. FTK Imager cannot handle hidden areas (either HPA or DCO or the combination of both) when acquiring the entire test drive. FTK Imager provides no notification to the user about whether hidden areas are present or not. When the FTK Imager acquires a partition that has been partially hidden, it displays and logs that the error "Block Indexes Out of Bounds" instead of detecting and disclosing hidden areas. However, the acquisition of completely hidden partition is not successful and the software freezes at the stage "Preparing to Image". The program crashes as well when it attempts to create the directory listings for the hidden partition. Irregular configurations are not detected and notified by the FTK Imager.

Helix 3 Pro presents some noteworthy problems during the testing. The amount of data it has acquired is not reported as defined in the research specifications. Users must manually calculate the number and size of the generated image files. The tool should have captured at information during the testing. The size of the total acquired data is considered significant for disk imaging tools. Helix 3 Pro does not clearly state whether the image files have been verified when the test drive is transformed into EnCase image format. Extra verification measures may be required to verify the integrity of the image files again. Similarly to FTK Imager, Helix 3 Pro cannot handle HPA and/or DCO hidden areas. When acquiring partially and completely hidden partitions, Helix 3 Pro performs inconsistently. The disk imaging proceeds at a remarkably slow speed and the process has to be terminated because it does not finish within a reasonable timeframe. In the test case where UNC errors exist, Helix 3 Pro does not record types and locations of the errors and the inaccessible sectors are replaced by a pre-configured value without details being disclosed clearly in the log file and in the user manual. The network acquisition function of Helix 3 Pro is unstable in Windows environments. Unhandled software exceptions and program crashes are observed during the testing. Some usability problems of the program are also discerned, such as lethargic progress bar, no indication of overall imaging progress and of overall progress on the sender side of network acquisition. Finally, GUID partition type is not supported by the software.

AIR passes 7 out of 15 test cases with 100% success rate and the overall success rate is over 75%. A major problem found in AIR is that no appropriate error message is provided to the user or logged in the image log file, whenever the program encounters a problem. AIR does not support alternate image storage option and the user must have a single storage device that has equal or more storage spaces than the evidence drive (or the test drive in our case). The research has found that AIR does not support HPA and/or DCO detection and acquisition, in contrast to the other two evaluated tools. AIR cannot provide notification to the user when the source device has irregular configuration. AIR also presents some usability problems. Information such as the name of the examiner, case number and case description is not required of the user to enter. Such information should be properly classified and carefully documented. The information is important so it should be hoarded in a safe location for the legal or auditing purpose. The image log file is not saved automatically after the acquisition. A proper user manual is not provided by the AIR author due to the immensity of time and labour demanded for preparing such a manual.

6.2 ANSWER TO THE RESEARCH QUESTIONS

The main research question for this study is to evaluate the performance of the selected disk imaging tools during their evaluation tests. The usability of the disk imaging tools is also one of the research areas investigated to a limited extent in this research. According to the literature review, completeness and accuracy are the two important metrics to measure the performance of the disk imaging tools. The research sub-questions are related to whether the selected disk imaging tools are able to extract accurate and complete forensic data during the tool testing. To answer the SQ1 specified in section 3.2, multiple test scenarios are designed for testing whether the tools are extracting accurate and complete data. All the test cases are designed for testing either the accuracy or completeness or both. For example, test cases TC-09 and TC-10 are targeting the accuracy of the data. Test cases TC-12 and TC-13 are testing both the accuracy and completeness of the data extracted by the disk imaging tools. To answer the SQ2 specified in section 3.2, the disk imaging tools testing were followed a set of forensically sound approach. The test drive is reset to a clean state at the beginning of and the end of the disk imaging to ensure that no data from previous use is still remained. The mechanism used to reset the test drive is developed by Department of the Defense of America. Tableau Write Blocker is utilised consistently (where applied) to ensure no accidentally write attempt to the test drive. Every result is also verified again using EnCase to ensure the extracted data are identical to the source. To answer the SQ3 specified in section 3.2, this study has developed a way to rank the disk imaging tools according to their performance. Each disk imaging tool is undergoes a series of test cases and each test case composes a set of assertions. The assertions will be tested and marked either pass or fail. The pass rate is calculated by using the total number passed assertions to divide the total number of assertions in the test case. The tools are then ranked according to their overall pass rate in all test cases.

Section 5.2 describes and discusses the results of the hypotheses testing. To answer the main research question, the testing results indicate that AIR performed better than or equal to the other two disk imaging tools in most of the common test cases. Helix 3 Pro performed worse than other two disk imaging tools and Helix 3 Pro also presented many problems. It is recommended that the disk imaging tools must be fully validated and verified as extensively as possible. The tool testing must be conducted in different configurations and different execution environments.

6.3 AREAS OF FUTURE RESEARCH

Current digital forensic tools are unable to keep pace with the growing complexity and rapid evolution of technology in the contemporary digital environment (Roussev & Richard, 2004; Ayers, 2009). Building a systematic and scientifically proven methodology to validate the functions of the digital forensics tool is a demanding job. What has been achieved by CFTT, DFTT and other researchers can be used as stepping stone to building a comprehensive testing framework. The framework must be automated, tool-independent and future-proof. Disk imaging is an important constituent of the evidence collection in the digital forensics investigative process, according to DFRWS investigative process described in section 2.1.2. Activities such as examination, analysis and presentation are also crucial for the digital forensics investigation. Different test scenarios with different hardware types can be imposed on the test cases to create a more complete testing framework. For example, Apple Mac OS X partition scheme GUID and file system HFS or HFS+, configured in a 2TB or larger hard drive can be used to evaluate the responses of the disk imaging tools. Other file systems such as ZFS, ResierFS and HPFS are worth researching and test cases can be developed in association with them (Peterson, Shenoi, & Beebe, 2009). Some popular hardware interfaces were not tested in the evaluation due to the time limitation of the research. Hardware interfaces that are popular in consumer and commercial markets, such as USB, SAS and SCSI, can be incorporated into the testing framework to create a more comprehensive solution for digital forensic tool testing. In relation to this research, data acquisition of solid state storage is also a pressing research topic in digital forensics (Peterson et al., 2009). Solid State Disks (SSD) read data 20 times faster, consume less power and display a lower failure rate than traditional Magnetic hard disks. With the price dropping, Antonellis (2008, p.36) states that the increased use of SSD is on the horizon. However, despite the advantages of SSD, it presents forensics challenges that demand further research. Mitchell (2009) and Antonellis (2008) found that data recovery in SSD is extremely difficult and also impossible in some cases due to the fact that the implementations are non-standardised, controller technology is complicated and algorithms are proprietary and different from vendors to vendors. Highly sophisticated data carving technology is required even when the data recovery is possible.

6.4 CONCLUSION

The main objective of this research is to employ a systematic and forensically sound method to measure the performance of the disk imaging tools in different test scenarios. Peterson et al. (2009, p.29) points out that problems in the forensic tool development and the error rates of digital forensics tools are among the most important topics for research. With some improvements of the research methods employed in this research and further development of configuration tools, a comprehensive testing framework can be formed to evaluate different types of digital forensic tools across multi-platform environments. Thanks to the selected functionality-driven approach, many problems are identified in the evaluated disk imaging tools and discussed.

The major finding of the research has shown that the accuracy and completeness are two essential attributes of disk imaging tools. These two attributes have a positive impact on the validity of the disk imaging tools. Testing of disk imaging tools should steer the focus toward these two attributes. Creating test cases that focus on the accuracy and completeness of data extracted by disk imaging tools can assure that the evidence generated by the tools can withstand the scrutiny of courts.

This research enriches the body of knowledge of testing of digital forensics tools by building a standardised testing framework. The information provided in this research could be valuable for other researchers who conceive some novel research ideas in digital forensic tools testing, for law enforcement agents and other parties interested to understand the capabilities of the tools, for software developers to recognise the shortcomings and issues of their tools and to improve the tools for better use.

References

AccessData (2007). Forensic Toolkit Imager User Guide. 1-34. Retrieved from http://www.accessdata.com/downloads/media/en_us/print/manuals/ImagerUsersGuide.pdf

AccessData. (2009). *Forensic Toolkit 3 product features*. Retrieved 15th, Mar, 2010, from http://www.accessdata.com/forensictoolkit.html

AccessData. (n.d). FTK Imager 2.x Release Notes. Retrieved 18th, Mar, 2010, from http://www.accessdata.com/downloads/media/Imager_2.x_ReleaseNotes.pdf

Adams, C. W. (2008). *Legal issues pertaining to the development of digital forensic tools.* Paper presented at the Proceedings - SADFE 2008 3rd International Workshop on Systematic Approaches to Digital Forensic Engineering, Berkeley, CA.

Akhter, F. (2008). E-Commerce Security: The Categorical Role of Computers in Forensic Online Crime In *Intelligence and Security Informatics* (Vol. 5075). Berlin: Springer.

Al-Azhar, M. N. (2009). Forensically Sound Write Protect on Ubuntu *Forensic Cop Journal*, *1*(3).

Antonellis, C. J. (2008). Solid state disks and computer forensics. *Journal of Information Systems Security Association, 2008*(July), 36-38.

Ayers, D. (2009). A second generation computer forensic analysis system. *Digital Investigation*, *6*(Supplement 1), S34-S42.

Ayers, D. (2009a). Flaws found in 'EnCase®' computer forensic software. NZ Lawyer (111).

AtlanticLinux. (2009). *Ubuntu 9.04 Fake RAID problems*. Retrieved 10th Oct, 2010, from http://atlanticlinux.ie/blog/?tag=dmraid

Balzanto, T. (2010). Error: Can't Initialize Source. Retrieved 10th Oct, 2010, from http://www.e-fense.com/forums/showthread.php?t=346&highlight=source+initialise

Barbara, J. J. (2006). Digital Insider: Software Imaging/Analysis Tools, Part 1. *Forensic Magazine*.

Baryamureeba, V., & Tushabe, F. (2004). *The enhanced digital investigation process model.* Paper presented at the Digital Forensic Research Workshop.

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

Berghel, H. (2007). Hiding Data, forensics, and anti-forensics. *Communication of ACM, 50*(4), 15-20.

Black, P. E. (2005). *Software assurance metrics and tool evaluation.* Paper presented at the Proceedings of the 2005 International Conference on Software Engineering Research and Practice, Las Vegas, US.

Boulanger, A. (2005). Open-source versus proprietary software - Is one more reliable and secure than the other. *IBM Systems Journal*, *44*(2), 239-249.

Britz, M. T. (2008). *Computer Forensics and Cyber Crime: An Introduction* (2 ed.): Prentice Hall.

Brungs, A., & Jamieson, R. (2005). Identification of Legal Issues for Computer Forensics. *Information systems management, 22*(2), 57.

Bukhari, S., Yusof, I., & Abdullah, M. (2010). Performance evaluation of open-source disk imaging tools for collecting digital evidence Symposium conducted at the meeting of the Regional Conference on Knowledge Integration in ICT, Putrajaya, Malaysia.

Byers, D., & Shahmehri, N. (2008). Contagious errors: Understanding and avoiding issues with imaging drives containing faulty sectors. *Digital Investigation, 5*(1-2), 29-33.

Byers, D., & Shahmehri, N. (2009). A systematic evaluation of disk imaging in EnCase 6.8 and LinEn 6.1. *Digital Investigation, 6*(1-2), 61-70.

Byers, D., & Shahmehri, N. (2008a). Disk imaging evaluation: Encase 6.8/Linen 6.1. *12*(1). Retrieved from www.ep.liu.se/ea/cis/2009/001/cis09001.pdf

Caloyannides, M. A., Memon, N., & Venema, W. (2009). Digital forensics. *IEEE security and privacy, 7*(2), 16-17.

Carrier, B. (2002). Open Source Digital Forensics Tools: A legal argument. Retrieved 21st February 2010 from http://www.digital-evidence.org/papers/opensrc_legal.pdf

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2).

Carrier, B. (2005). *Digital forensics tool testing images*. Retrieved 13th Mar, 2010, from http://dftt.sourceforge.net.

Casey, E. (2000). *Digital Evidence and Computer Crime* (1 ed.). London: Academic Press.

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (Vol. 2). London: Academic Press.

Casey, E. (2006). Investigating sophisticated security breaches. *Communication of ACM, 49*(2), 48.

Ciardhuain, S. O. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence, 3*(1).

Cohen, F. B. (2010). Fundamentals of Digital Forensic Evidence. In *Handbook of Information and Communication Security* (pp. 789-808). Berlin Heidelberg: Springer.

Cohen, T., & Schroader, A. (2007). *Alternate data storage forensics*. Burlington: Syngress.

Comella-Dorda, S., Dean, J., Lewis, G., Morris, E., Oberndorf, P., & Harper, E. (2002). *A process for COTS software product evaluation.* Paper presented at the Proceedings of the First International Conference on COTS-Based Software Systems.

Dan, M., Anna, C., Steve, R., Alain, G., Matthew, K., & Jeremy, T. (2007). *Is the Open Way a Better Way? Digital Forensics Using Open Source Tools.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

DarkNet. (2006). *10 Best Security Live CD Distros*. Retrieved 23rd March, 2010, from http://www.darknet.org.uk/2006/03/10-best-security-live-cd-distros-pen-test-forensics-recovery/

Detective, D. (2010). *Introduction to Digital Detective's NetAnalysis v1.51*. Retrieved 1st Feb, 2010, from http://www.digital-detective.co.uk/netanalysis.asp

DIBS. (2010). *Computer forensics equipment*. Retrieved 20th, Mar, 2010, from http://www.computer-evidence.com/products/products.asp

Dixon, P. D. (2005). An overview of computer forensics. *IEEE Potentials, 24*(5), 7-10.

DFRWS. (2001). *A Road Map for Digital Forensic Research*. New York, U.S.A.

E-fence. (2009). *Helix3 pro*. Retrieved 1st, Feb, 2010, from http://www.e-fense.com/helix3pro.php

Erbacher, R. F. (2010). *Validation for digital forensics*. Paper presented at the meeting of the 2010 Seventh International Conference on New Generation Information Technology, Las Vegas, US.

Etter, B. (2001). The forensic challenges of e-crime Symposium conducted at the meeting of the 7th Indo-Pacific Congress on Legal Medicine and Forensic Sciences, Melbourne, Australia.

Farmer, D., & Venema, W. (1999). Computer forensics analysis class handouts. Retrieved 10th Mar, 2010, from http://www.fish.com/forensics/class.html

Freiling, F. C., & Schwittay, B. (2006). A Common Process Model for Incident Response and Computer Forensics. *Communications of the ACM*, *48*, 8.

ForensicsWiki. (2010). *iLook*. Retrieved 2nd Feb, 2010, from http://www.forensicswiki.org/wiki/ILook

Garfinkel, L. S. (2010). Digital forensics research: the next 10 years. *Digital Investigation*, *7*, S64-S73.

Gavrila, S. I. (2005). FS-TST 2.0: Forensic software Ttesting support tools, National Institute of Justice.

Gibson, S. (2010). *AIR - Automated Image and Restore*. Retrieved 21st March, 2010, from http://air-imager.sourceforge.net/

Gleason, B. (2009). *Alternatives to Helix3*. Retrieved 21st March, 2010, from http://www.forensicfocus.com/index.php?name=Content&pid=172&page=1

Goel, A. L. (1985). Software Reliability Models: Assumptions, Limitations, and Applicability. *IEEE Transactions on Software Engineering*, *SE-11*(12), 1411-1424.

Grossman, J. (2007). *Website Security Statistics Report*. Santa Clara. Retrieved 18th February 2010 from http://www.whitehatsec.com/home/assets/WPStatsreport_100107.pdf

GuidanceSoftware. (2010). *EnCase forensic version 6.17 user guide*. Pasadena, CA.

Guidance. (2010). EnCase forensic features and functionality. Retrieved from 22nd, Mar 2010 http://www.guidancesoftware.com/WorkArea/DownloadAsset.aspx?id=671

Guo, Y., & Slay, J. (2010). *A Function Oriented Methodology to Validate and Verify Forensic Copy Function of Digital Forensic Tools.* Paper presented at ARES 2010 International Conference on Availability, Reliability, and Security.

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic software tools - Searching Function. *Digital Investigation*, *6*, S12-S22.

Gupta, M. R., Hoeschele, M. D., & Rogers, M. K. (2006). Hidden disk areas: HPA and DCO. *International Journal of Digital Evidence, 5*(1).

Haase, N. (2001). Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000. Retrieved 18th February 2010 from http://www.sans.org/reading_room/whitepapers/incident/computer_forensics_introduction_to_incident_response_and_investigation_of_windows_nt/2000_647?show=647.php&cat=incident

Harbour, N. (2006). *Dcfldd*. Retrieved 4th May, 2010, from http://dcfldd.sourceforge.net/

IEEE. (1990). IEEE Standard Glossary of Software Engineering Terminology. *IEEE Std 610.12-1990*, 1.

Johnson, T. A. (2005). *Forensic computer crime investigation*. New York: CRC Press.

Kenneally, E. E. (2001). Gatekeeping Out Of The Box: Open Source Software As A Mechanism To Assess Reliability For Digital Evidence. *Virginia Journal of Law and Technology, 6*(3).

Kenneally, E. E., & Brown, C. L. T. (2005). Risk sensitive digital evidence collection. *Digital Investigation, 2*(2), 101-119.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response* (No. SP 800-86). Gaithersburg: National Institute of Standards and Technology.

Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., et al. (2007). Acquiring Data, Duplicating Data, and Recovering Deleted Files. In *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators*: Syngress Publishing.

Kohn, M., Eloff, J., & Olivier, M. (2006). *Framework for a Digital Forenisc Investigation.* Paper presented at the Proceedings of Information Security South Africa, South Africa.

Kontio, J. (1996). *A case study in applying a systematic method for COTS evaluation.* Paper presented at the Proceedings of the 18th international conference on software engineering, Berlin Germany.

Kornblum, J., & Medico, A. (2009). *dc3dd*. Retrieved 4th May, 2010, from http://dc3dd.sourceforge.net/

Kunda, D., & Brooks, L. (1999). *Applying social-technical approach for COTS selection.* Paper presented at the Proceedings of the 4th UKAIS conference, University of York, UK.

Lin, A. C., Lin, L. L., Lan, T. H., & Wu, T.-C. (2005). *Establishment of the Standards Operating Procedure for Gathering Digital Evidence.* Paper presented at the Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), Taibei, Taiwan.

Lyle, J. R. (2003). NIST CFTT: Testing disk imaging tools. *International Journal of Digital Evidence, 1*(4), 1-10.

Lyle, J. R., & Wozar, M. (2007). Issues with imaging drives containing faulty sectors. *Digital Investigation, 4*(Supplement 1), 13-15.

Malinowski, C., & Noble, R. (2007). Hashing and data integrity: Reliability of hashing and granularity size reduction. *Digital Investigation, 4,* 98-104.

Maiden, N. A. M., & Ncube, C. (1998). *Acquiring COTS software selection requirements.* Paper presented at the Requirements Engineering, 1998. Proceedings. 1998 Third International Conference on, Colorado Springs, CO.

Manes, G. W., & Downing, E. (2009). Overview of Licensing and Legal Issues for Digital Forensic Investigators. *Security & Privacy, IEEE, 7*(2), 45-48.

Maxim, S. (2009). *Linux for computer forensic investigators: «pitfalls» of mounting file systems*. Retrieved 9th Oct, 2010, from http://www.forensicfocus.com/linux-forensics-pitfalls-of-mounting-file-systems

Mercuri, R. (2005). Challenges in forensic computing. *Communication of ACM, 48*(12), 17-21.

Meyrick, K. (2006). *Host protected area - Creation of an HPA*. Retrieved 16th Apr, 2010, from http://en.wikipedia.org/wiki/File:Hpacreate.png

Mitchell, R. L. (2009). Solid-state disks offer 'fast erase' features. *Computerworld, 2009*(Feburary).

Mohay, G. (2005). *Technical challenges and directions for digital forensics.* Paper presented at the Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on.

Moll, R., Prokop, M., & Morgenstern, H. (2009). Digital discovery with bootable CDs Symposium conducted at the meeting of the 2009 IT Security Incident Management and IT Forensics Stuttgart, Germany.

Newsham, T., Palmer, C., Stamos, A., & Burns, J. (2007). Breaking forensics software: weaknesses in critical evidence collection. Retrieved 3rd, Mar 2010 from https://www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1_1.BH2007.pdf

US-CERT. (2007). *Vulnerabilitiy Note VU#310057*. Retrieved 9th, Mar, 2010, from http://www.kb.cert.org/vuls/id/310057

NFI. (2006). rdd forensic copy program. Retrieved 4th May, 2010, from http://sourceforge.net/projects/rdd/files/

NIJ. (2001). *Electronic crime scene investigation: a guide for first responders*. Washington, DC.

NIJ. (2008). *Electronic crime scene investigation: a guide for first responders*. 2ed. Washington, DC.

NIJ. (2008a). *Test Results for Digital Data Acquisition Tool: FTK Imager 2.5.3.14.* Washington, DC: National Institute of Standards and Technology. Retrieved from 21st January 2010 http://www.ojp.usdoj.gov/nij/pubs-sum/222982.pdf

Nikkel, B. J. (2009). Forensic analysis of GPT disks and GUID partition tables. *Digital Investigation, 6*, 39-47.

NIST. (2001). General test methodology for computer forensic tools. Retrieved from http://www.cftt.nist.gov/Test%20Methodology%207.doc

NIST. (2004). *Digital Data Acquisition Tool Specification (Draft 1 of Version 4.0)*. Washington, DC: NIST. Retrieved 21st January 2010 from http://www.cftt.nist.gov/Pub-Draft-1-DDA-Require.pdf

NIST. (2005). *Digital Data Acquisition Tool Test Assertions and Test Plan (Draft 1 of Version 1.0)*. Washington, DC: NIST. Retrieved from 21st January 2010 http://www.cftt.nist.gov/DA-ATP-pc-01.pdf

Noblett, M., Pollitt, M., & Presley, L. (2000). Recovering and Examining Computer Forensic Evidence. *Forensic science communications, 2*(4), 13.

Oliver, S. (2010). *Apple's new MacBook Airs predicted to sell 700K during holidays*. Retrieved 24th Oct, 2010, from http://www.appleinsider.com/articles/10/10/22/apples_new_macbook_air_predicted_to_sell_700k_during_holidays.html

Palmer, G. (2001). *A Road Map for Digital Forensic Research* (No. DTR - T001-01). New York.

Payne, C. (2002). On the Security of Open Source Software. *Information Systems Journal*, *12*, 61-78.

PCMag. (2002). *Event Monitoring*. Retrieved 2nd, Feb, 2010, from http://www.pcmag.com/print_article2/0,1217,a=28321,00.asp?hidPrint=true

Perrin, C. (2008). Not invented here has no place in open source development. Retrieved 18 March from http://blogs.techrepublic.com.com/security/?p=460

Peterson, G., Shenoi, S., & Beebe, N. (2009). Digital Forensic Research: The Good, the Bad and the Unaddressed. In *Advances in Digital Forensics V* (Vol. 306, pp. 17-36): Springer Boston.

Pollitt, M. (1995). *Computer Forensics: an Approach to Evidence in Cyberspace.* Paper presented at the Proceeding of the National Information Systems Security Conference.

Raymond, E. S. (2002). The cathedral and the bazaar. Retrieved 18 March from http://www.catb.org/~esr/writings/cathedral-bazaar/

Reichenkron, T. (2006). *Security Issues In Open Source Project.* Paper presented at the Open source Software Engineering, Berlin.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3).

Ridder, C. K. (2009). Evidentiary Implications of Potential Security Weaknesses in Forensic Software. *International Journal of Digital Crime and Forensics, 1*(3), 80-91.

Rohilla, V., & Malik, S. (2008). Software verification and validation Symposium conducted at the meeting of the Proceedings of the 2nd National Conference INDIACOM-2008, New Delhi, India.

Rogers, M. (2003). Computer forensics: science or fad. *Security Wire Digest, 5*(55).

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security, 23*(1), 12-16.

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). *Computer Forensics Field Triage Process Model.* Paper presented at the Proceedings of the Conference on Digital Forensics, Security and Law.

Roussev, V. and Richard III, G.G. (2006). Next-generation digital forensics. Communication of ACM, 49(2), 76-80.

Roussev, V. and Richard III, G.G. (2004). Breaking the performance wall: The case for distributed digital forensics. In *Proceedings of the 2004 Digital Forensics Research Workshop.*

Richardson, R. (2007). 2007 CSI Computer Crime and Security Survey. Retrieved 21st January 2010 from http://www.gocsi.com/forms/csi_survey.jhtml

Ryan, D. J., & Shpantzer, G. (2002). Legal aspects of digital forensics. Retrieved 21st January 2010 from http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf

SANS. (2009). *Forensics 508*. Retrieved 22nd March, 2010, from http://www.sans.org/security-training/computer-forensic-investigations-incident-response-98-mid

Sandstorm. (2009). *NetIntercept system summary*. Retrieved 1st, Jan, 2010, from http://www.sandstorm.net/products/netintercept/technical.php

Saudi, M. M. (2001). An overview of disk imaging tool in computer forensics. Retrieved 21st January 2010 from http://www.sans.org/reading_room/papers/?id=643&c=0eeabaf101ef050e3c66f79b71b24362

Schweitzer, D. (2003). *Incident response: computer forensics toolkit*. Indianapolis: Wiley Publishing, Inc.

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.

Sheng, J., & Wang, B. (2008). *Evaluating COTS components using gap analysis.* Paper presented at the The 9th International Conference for Young Computer Scientists, Zhang Jia Jie, Hunan.

Simson, G., Malan, D., Dubec, K-A., Stevens, C., & Pham, C. (2006). Advanced forensic format: An open, extensible format for disk imaging. *Springer.* Symposium conducted at the meeting of the Advances in Digital Forensics II: FIP International Conference on Digital Forensics, Orlando, Florida.

Sitaraman, S., & Venkatesan, S. (2006). Computer and Network Forensics. In *Digital Crime and Forensic Science* (pp. 68). London: Idea Group.

Smith, R. (2009). Make the most of large drives with GPT and Linux. Retrieved 9th Sep 2010 from http://www.ibm.com/developerworks/linux/library/l-gpt/

Sommer, P. (2010). Forensic science standards in fast-changing environments *Science and Justice*, *50*(1), 12-17.

Sourcefire. (2010). *What is Snort?* Retrieved 3rd, Mar, 2010, from http://www.snort.org/

Staarfanger. P. (2009). Helix3Pro Receiver Failures. Retrieved 1st Oct 2010 from http://www.e-fense.com/forums/showthread.php?t=350&highlight=source+initialise

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, *8*(2), 42-54.

SWGDE (2009). SWGDE and SWGIT Digital & Multimedia Evidence Glossary. Retrieved 21st March 2010 from http://www.swgde.org/documents/swgde2009/SWGDE_SWGITGlossaryV2.3.pdf

SWGDE (2009a). SWGDE Recommended Guidelines for Validation Testing. Retrieved 3rd March 2010 from http://www.swgde.org/documents/swgde2009/SWGDE%20Validation%20Guidelines%2001-09.pdf

Technical Committee T13. (2001). *AT Attachment with packet interface-6 (ATA/ATAPI-6)*. Retrieved 14th Apr, 2010, from http://www.t10.org/t13/project/d1410r3a-ATA-ATAPI-6.pdf

Thompson, E. (2005). MD5 collisions and the impact on computer forensics. *Digital Investigation*, *2*, 36-40.

Vatis, M. (2004). *Law enforcement tools and technologies for investigating cyber attacks: Gap analysis report*: Institute for security technology studies.

Viega, J. (2000). The Myth of Open Source Security. Retrieved 21st January 2010 from http://itmanagement.earthweb.com/secu/article.php/621851

Wallace, D. R., & Fujii, R. U. (1989). Software verification and validation: an overview. *IEEE Software*, *6*(3), 10-17.

Wang, X., Feng, D., Lai, X., & Yu, H. (2004). Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD*Springer*. Symposium conducted at the meeting of the Crypto 2004, Santa Barbara, California.

Wang, X., Lai, X., Feng, D., Chen, H., & Yu, X. (2005). Cryptanalysis of the Hash Functions MD4 and RIPEMD. In R. Cramer (Chair), *Springer*. Symposium conducted at the meeting of the Advances in Cryptology – EUROCRYPT 2005, Aarhus, Denmark.

Wang, Y., Cannady, J., & Rosenbluth, J. (2005). Foundations of computer forensics: A technology for the fight against computer crime. *Computer Law & Security Report*, *21*(2), 119-127.

Waring, T., & Maddocks, P. (2005). Open Source Software implementation in the UK public sector: Evidence from the field and implications for the future. *International Journal of Information Management*, *25*, 411-428.

Webber, D. (2009). *Helix forensics CD now payware*. Retrieved 23rd March, 2010, from http://advosys.ca/viewpoints/2009/03/helix-forensics-cd-now-payware/

Whitcroft, A. (2009). *Bug #380138 Do not disable HPA by default* Retrieved 10th Oct, 2010, from https://bugs.launchpad.net/ubuntu/+source/linux/+bug/380138

Wikipedia.org. (2010). XTree. Retrieved 3rd Mar, 2010 from http://en.wikipedia.org/wiki/XTree

Williams, J. (2006). Computer forensics: A practical guide to its use in corporate litigation. 1-4, from http://www.kpmg.ca/en/services/advisory/forensic/documents/computerforensics.pdf

Wilsdon, T., & Slay, J. (2006). *Validation of forensic computing software utilizing black box testing technique.* Paper presented at the Proceedings of 4th Australian Digital Forensics Conference, Perth, Australia.

Cases

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Federal Rules of Evidence, 901(a), 2007.

Frye v. United States, 293 F. 1013 (1923).

Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).

United States v. Liebert, 519 F. 2d 542, 547 (3rd Cir. 1975)

Williford v. State, 127 SW 3d 309 (Court of Appeals, Eastland 2004)

Appendix 1 – Definitions

Access Method (Major Scheme 1): The computer reads the physical devices through a set of commands or protocols. For example, the operating system reads the data from a SATA hard drive by ATA command sets.

Digital Source (Major Scheme 2): A container of digital data that can be acquired by a data acquisition tool (NIST, 2004, p.7). For example, physical hard drive, flash memory, USB storage device or logical drive (a partition). The digital source in this research could be a partition or the entire hard drive.

Data Destination (Major Scheme 3): location(s) that store the image files.

Execution Environment (Major Scheme 4): Software is a service that must be operating in an operating system. Disk imaging tool can be operate in Microsoft Windows or Linux operating system.

Hidden Data Sectors: data sectors in the current configuration of a drive that are not accessible by the disk imaging tool (NIST, 2004, p.7).

Hidden Areas (Major Scheme 5): the areas that hidden from the user and the operating system. These areas are usually being used to conceal information.

Partition Partially Hidden: A partition has start and sectors. Partially hidden partition means only certain part of the whole partition is accessible by read or write commands. For example, a typical partition starts from the sector 100 to the end sector 500. Partially hidden could means anything starts from the sector 101 to the end. See also Completely Hidden.

Partition Completely Hidden: Partition completely hidden means that the entire partition, starting from the first sector to the end, is not accessible by read and write commands.

Physical Interface (Major Scheme 6): A physical device connects to the computer through a physical interface. For example, a hard drive may connect to the computer through an ATA interface or USB interface.

Unresolved Error: The disk imaging tool sends multiple I/O requests to the disk drive but all return failure (NIST, 2004, p.7)..

Visible Data Sectors: data sectors in the current configuration of a drive that are accessible by the disk imaging tool (NIST, 2004, p.7).

Irregular Configurations: Digital source maybe configured some way outside the norm which may lead to the acquired data being corrupt or misinterpreted. In some extreme cases, it may lead to the data acquisition not viable (Byers & Shahmehri, 2008a).

Appendix 2 – Testing requirements

1. Fundamental Requirements (FR)

Requirement ID	Description	Corresponding NIST Requirements
TSP-FR-01	The tool shall be able to acquire a digital source using a supported physical interface	DI-RM-01
TSP-FR-02	The tool shall be able to create an image or clone of digital source	DI-RM-02
TSP-FR-03	The tool shall be able to function at least one execution environment	DI-RM-03
TSP-FR-04	All the visible sectors are acquired from the digital source	DI-RM-04
TSP-FR-05	All the hidden sectors are acquired from the digital source	DI-RM-05
TSP-FR-06	All the data sectors are accurately acquired from the digital source	DI-RM-06
TSP-FR-07	The tool shall report to the user of the error type and the location of the error if error occurred during the reading from a digital source.	DI-RM-07
TSP-FR-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.	DI-RM-08

2. Requirements for Optional Features

Image Creation (IC) Function

Requirement ID	Description	Corresponding NIST Requirements
TSP-RIC-01	If an image creation is selected the tool shall create the image in the selected format and destination with all the data acquired.	DI-RO-01
TSP-RIC-02	If error occurs during the image file creation, the tool shall report to the user of the condition	DI-RO-02
TSP-RIC-03	If space is insufficient on the selected image destination device during an image file creation, the tool shall report to the user of the condition	DI-RO-03
TSP-RIC-04	If multi-file image creation and the image file size is selected, the tool shall create a multi-file image with the requested size which contains all the data acquired	DI-RO-04
TSP-RIC-05	if the image file integrity check is selected, the tool shall report to the user whether the image file has been changed and if the image file has been changed the location should be reported	DI-RO-05
TSP-RIC-	If image format conversion is selected, the target image file	DI-RO-06

06	format should contain same data as the original image file	
TSP-RIC-07	The tool shall allow the user select an alternate destination device to continue image creation process if there is insufficient space in destination device and destination device switching function is supported. The multi-image file should represent the same data as acquired by the tool	DI-RO-07

Logging Function (LOG)

Requirement ID	**Description**	**Correspondent NIST Requirements**
TSP-RLOG-01	If the tool offers log file creation then the tool shall record at least one of the following information: tool version, tool settings, acquisition date and/or time, device size, device manufacturer, device model number, device serial number, partition table, amount of data acquired and user comments.	DI-RO-01
TSP-RLOG-02	The tool shall display correct information about the acquisition.	N/A
TSP-RLOG-03	The tool shall display correct information regarding to the acquisition to the user and consistent with the log file if the log file function is supported	N/A

Hidden Sector (HS)

Requirement ID	**Description**	**Correspondent (Byers & Shahmehri, 2009) Requirements**
TSP-RHS-01	The tool shall report to the user if it detects hidden sectors are contained in digital source	SKL-DI-05
TSP-RHS-02	The tool shall report to the user that hidden sectors may present but undetected if it cannot detect hidden sectors on the digital source	SKL-DI-06
TSP-RIC-03	The tool shall report to the user that hidden sectors will not be acquired if it cannot acquire hidden sectors on the digital source	SKL-DI-07

Appendix 3 – Test Scenarios

Test Cases	Description	Assertions for Testing
TC-01 (A11)	Acquire a hard drive using Access Interface (AI) and convert to an image file	**AFR01-05, AFR07,AIC01, AIC05, ALOG01-03**
TC-02 (A11)	Acquire a digital source that supported by the tools to an image file	**AFR01-05, AFR07,AIC01, AIC05, ALOG01-03**
TC-03 (A18)	Acquire a hard drive with hidden sectors to an image file	**AFR01-07, AIC01-02, AIC05-08, ALOG01-03, AHS01-03**
TC-04 (A12)	Acquire a digital source that has at least one faulty data sector	**AFR01-05, AFR07-09, AIC01-03, AIC05-08, ALOG01-03**
TC-05 (A12)	Acquire a digital source to an image file in an alternate supported format	**AFR01-05, AFR07, AIC01-02, ALOG01-03**
TC-06 (A12)	Simulate an unresolved read error scenario and check whether the tool notifies and/or try to recover the error sectors when writing an image file	**AFR01-04, AFR05, AFR07-09, AIC01-03, ALOG01-03**
TC-07 (A08)	Attempt to create an image file where destination device has insufficient storage space	**AFR01-04, AIC04, ALOG01-03**
TC-08 (A13)	Attempt to create an image file where destination device has insufficient storage space, and see whether the tool notifies the user and offer another destination device to continue	**AFR01-05, AFR07, AIC01-02, AIC04-05, AIC10, ALOG01-03**
TC-09 (A05)	Verify a correct image	**AFR03, AIC06, ALOG01-03**
TC-10 (A06)	Try verifying a corrupted image	**AFR03, AIC06-08, ALOG01-03**
TC-11 (A05)	Convert an existing image file to another supported image file format	**AFR03, AFR09, ALOG01-03**
TC-12 (A18)	Acquire a partition that is partially or completely hidden by HPA or DCO	**AFR01-07,AIC01-02,AIC05-08, ALOG01-03, AHS01-03**
TC-13 (A12)	Acquire a partition that is overlapping with another partition. The end sector of a partition is ended beyond the starting sector of the next partition.	**AFR01-05,AFR07, AIC01-02, AIC11, ALOG01-03**
TC-14 (A12)	Acquire a hard disk with a partition's end address ended outside the physical disk boundary.	**AFR01-05,AFR07, AIC01-02, AIC11, ALOG01-03**
TC-15 (A19)	Acquire a hard disk with an unreadable MBR	**AFR01-05,AFR07-09, AIC01-03, AIC05-08, AIC11, ALOG01-03**
TC-16 (A15)	Acquire a single GPT partition.	**AFR01-05, AFR07,AIC01-02, AIC05-08, ALOG01-03**
TC-17 (A19)	Acquire a GPT partition that is partially hidden by HPA	**AFR01-06,AFR07, AIC01-02, AIC05-08, ALOG01-03, AHS01-03**
TC-18 (A18)	Verify the network image acquisition function provided by the tool	**AFR01-05,AFR07, AIC01-02, AIC05-08, ALOG01-03**

Appendix 4 – Test Assertions

Assertions for Fundamental Requirements

Assertion ID	Assertion Description	Correspondent NIST Assertion
TSP-AFR-01	The tool accesses the digital source with a supported access interface	DA-AM-01
TSP-AFR-02	The tool acquires a digital source	DA-AM-02
TSP-AFR-03	The tool operates in an execution environment	DA-AM-03
TSP-AFR-04	The tool creates an image file of the digital source	DA-AM-05
TSP-AFR-05	The tool acquires all the visible data sectors from the digital source	DA-AM-06
TSP-AFR-06	The tool acquires all the hidden data sectors from the digital source	DA-AM-07
TSP-AFR-07	All data sectors acquired from the digital source are acquired accurately.	DA-AM-08
TSP-AFR-08	The tool reports to the user of the error type and the location of the error if error occurred during the reading from a digital source.	DA-AM-09
TSP-AFR-09	If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.	DA-AM-10

Assertions for Optional Features - Logging Function (LOG)

Assertion ID	Assertion Description	Correspondent NIST Assertion
TSP-ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.	DA-AO-23
TSP-ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device name & serial, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.	SKL-DIA-25
TSP-ALOG-03	The acquisition information displayed to the user is consistent with the log file if the log file function is supported	N/A

Assertions for Optional Features - Hidden Sector (HS)

Assertion ID	**Assertion Description**	**Correspondent Assertion (Byers & Shahmehri, 2009)**
TSP-AHS-01	The tool reports to the user if any hidden sectors are found	SKL-DIA-08
TSP-AHS-02	The tool reports to the user that digital source may contain hidden sector but unable to detect it due to incompatible execution environment and/or access interface.	SKL-DIA-09 SKL-DIA-10
TSP-AHS-03	The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment and/or access method.	SKL-DIA-11 SKL-DIA-12

Assertions for Optional Features - Image Creation (IC) Function

Assertion ID	**Assertion Description**	**Correspondent NIST Assertion**
TSP-AIC-01	The data represented by an image file is the same as the data acquired by the tool	DA-AO-01
TSP-AIC-02	The tool creates an image file according to the file format the user specified.	DA-AO-02
TSP-AIC-03	The tool reports to the user if an error occurs during the image creation process.	DA-AO-03
TSP-AIC-04	The tool reports to the user if insufficient space in the destination device during the image creation process.	DA-AO-04
TSP-AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller	DA-AO-05
TSP-AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.	DA-AO-06
TSP-AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.	DA-AO-07
TSP-AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.	DA-AO-08
TSP-AIC-09	If image format conversion is selected, the target	DA-AO-09

	image file format contains the same data as the original image file	
TSP-AIC-10	The tool reports to the user if insufficient space in the destination device to contain the multi-image file creation and if destination device switching function is supported, the image is continue on the selected destination device.	DA-AO-10
TSP-AIC-11	The tool reports to the user if any irregularities found in the digital source.	SKL-DIA-24

Appendix 5 – Configuration Procedures

4.1 Drive Reset (Common in most Test Scenarios)

This procedure is to removes any partitions, data in the hard drive. Each test case will require drive reset to make the hard drive ready for the next test case.

1. Connect the test hard drive to the machine
    - 1.1 Boot the computer to the HDAT2 CD if HPA and/or DCO are existed
    - 1.2 Choose the test hard drive in the device list
    - 1.3 Navigate to the Device Information Menu to detect HPA and/or DCO
    - 1.4 Navigate to the SET MAX (HPA) Menu if HPA is existed or Navigate to Device Configuration Overlay (DCO) menu if DCO is existed
    - 1.5 Choose “Auto Remove HPA Area” for HPA or “Restore” for DCO
2. Boot the computer to the Darik's Boot and Nuke CD
3. Choose the test hard drive to wipe
4. Select DoD Short method
5. Wait for the drive reset completed

4.2 Partitioning Test Drive (Common in most Test Scenarios)

Linux Environment

1. Start Gparted and select the test drive on the top right corner.
2. Create new Partition then input the size of the partition and choose whether its primary or extended partition.
3. Choose file system
4. Finish and click add

Windows Environment

1. Right click Computer on the desktop and select manage.
2. Select the test drive and right click the drive and select simple volume
3. Right click the test drive and select convert to GPT disk if GUID partition table is required.

4.3 Detect HPA and/or DCO in the hard drive

1. Open Terminal program
2. Input the command: hdparm –N /dev/xxx (xxx is the device use command fdisk –l to check)
3. Or input the command: disk_stat /dev/xxx (xxx is the device use command fdisk –l to check)
    a) Disk_stat command is only available in Linux environment and it can only detects HPA

4.4 Implement HPA and/or DCO in the hard drive

1. Boot from the HDAT2 CD
2. Choose the test hard drive in the device list
3. Navigate to the SET MAX (HPA) Menu to implement HPA
    a) Select Set Max Address and Input the LBA sector for the new hidden area
    b) Choose Volatile mode as hard setting and Press S to confirm the new HPA
4. Navigate to the DCO Menu to implement DCO
    a) Select Modify option and change the Maximum LBA sectors to the desired value
    b) Press S to confirm the new DCO

4.5 Implement UNC Errors

1. Boot from the MHDD floppy
2. Select the test hard drive in the device list
3. Type “makebad” command in the command line (Use this command as caution)
4. Click Esc to stop program after 1 second (run this program more 3 second the hard drive may not readable due to excessive amount of errors)

4.6 Acquisition – FTK Imager (Common in most Test Scenarios)

This procedure outlines the process of a disk imaging acquisition of the tool FTK Imager.

4.5.1 Prerequisites

1. Windows XP Professional with Service Pack 3 is installed in the system or Windows 7 with latest system updates installed
2. Minimum data storage requirement for the program is met

4.5.2 Acquisition – FTK Imager (Windows Version - Common in most Test Scenarios)

1. Connect the test hard drive to the Windows machine using the specified physical interface. Connect to the hardware writeblocker if the test case is required.
2. Log on the computer with administrator privilege.
3. Start FTK Imager (Under Windows 7, run the program as administrator)
4. Click “Add Evidence Item” and select physical drive
5. Choose the test drive and click Finish
6. Acquire Entire drive or single partition
    a) Right click the physical drive and select “Export disk image”
    b) Right click the partition that need to be acquired and select “Export disk image”
7. Select verify image, precalculate progress and create directory listings and Add image and choose image type either dd, E01 or Smart.
8. Input Case Number, Evidence Number, Description, Examiner and Notes.
9. Choose destination folder and input the desired image filename. Change Image fragment size if necessary.
10. Then click finish to start disk acquisition.
11. Wait until FTK Imager indicates the acquisition progress is completed.

4.1 Acquisition – AIR

This procedure outlines the process of the disk imaging acquisition of the tool AIR.

4.6.1 Prerequisites

1. Uudecode program must be installed (use command “which uudecode” to verify whether uudecode is installed)

2. Linux distributions Ubuntu and Gentoo are required for better stability. (the project used Ubuntu based Linux Distribution)
3. Perl/Tk must be installed. If Perl/Tk is not installed on your system, install-air will attempt to download it itself.
4. Install program autoconf-1.10.1 and gperf
5. Install dc3dd (x.xx.x indicates the version of dc3dd. Our project used version 6.12.4)
    a) Unpack the installation file:
    ```
    $ tar zxvf dc3dd.x.xx.x.tar.gz
    ```
    b) Navigate to the unpacked file directory and install:
    ```
    $ ./configure
    $ make
    $ sudo make install
    ```
6. Installation of AIR (x.x.x indicates the version of AIR. Our project used version 2.0.0)
    a) Unzip the installation file:
    ```
    $ sudo gunzip install-air-x.x.x.gz
    ```
    b) Change the ownership of the installation file
    ```
    $ chmod +x install-air-x.x.x
    $ sudo ./install-air-x.x.x
    ```

4.6.2 Acquisition – AIR (Common in most Test Scenarios)

1. Connect the test hard drive to the Windows machine using the specified physical interface. Connect to the hardware writeblocker if the test case is required.
2. Open the Terminal and type in the command “sudo air” to run AIR.
3. In the field source device type in source drive (Use command “fdisk -l” to verify). Partition can also be specified in here.
4. In the field destination device type in destination drive (Mount the destination drive in the system)
5. Choose md5 as Hash 1 and sha1 as Hash 2. Choose Verify as Yes.
6. Select Use DC3DD and Split Image to 2047 Mbytes

7. Keep setting “noerror, sync” as Conversion.
8. Click start to start the acquisition
9. Wait until AIR indicates the acquisition progress is completed.
10. Save the Log file to an external drive as backup.

4.2 Acquisition – Helix 3 Pro

This procedure outlines the process of a disk imaging acquisition of the tool Helix 3 Pro.

4.7.1 Prerequisites

1. CD/DVD drive is properly setup and ready to use
2. Windows XP Professional with Service Pack 3 is installed in the system or Windows 7 with latest system updates installed
3. Minimum data storage requirement for the program is met

4.7.2 Acquisition – Helix 3 Pro (Common in most Test Scenarios)

1. Connect the test hard drive to the Windows machine using the specified physical interface. Connect to the hardware writeblocker if the test case is required.
2. Boot from the Helix 3 Pro Live CD or start Helix 3 from the Windows environment
3. Run Helix 3
4. Choose the Source drive or partition from the device list.
5. Click Acquire tab
    a) Select the output type (Usually is RAW format but EnCase format is used in certain test cases)
    b) Input Case name, Examiner, Case Number, Item number, Description and Notes
    c) Choose 2GB default segmentation and Read Size 32768
    d) Select MD5 and SHA1 as hash protocol
    e) Select destination drive
    f) Start the acquisition
    g) Wait until Helix 3 Pro indicates the acquisition progress is completed.

4.3 Verification of Acquired Image (Common in most Test Scenarios)

The acquired images from each test case will input to EnCase to verify the hash values and ensure the values are matched from the output of the disk imaging tool that is being tested. However, sometimes extra verification method may require. Hex editor may also be used as verification tool to check the hex value of the data.

Appendix 6 – Gap Analysis Matrix

Fundamental Requirements (FR)

Requirement ID	Description	FTK Imager	Helix 3 Pro	AIR
TSP-FR-01	The tool shall be able to acquire a digital source using a supported physical interface	✓	✗	✓
TSP-FR-02	The tool shall be able to create an image or clone of digital source	✓	✓	✓
TSP-FR-03	The tool shall be able to function at least one execution environment	✓	✓	✓
TSP-FR-04	All the visible sectors are acquired from the digital source	✗	✗	✓
TSP-FR-05	All the hidden sectors are acquired from the digital source	✗	✗	✗
TSP-FR-06	All the data sectors are accurately acquired from the digital source	✓	✓	✓
TSP-FR-07	The tool shall report to the user of the error type and the location of the error if error occurred during the reading from a digital source.	✓	✓	✓
TSP-FR-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.	✓	✓	✓

Image Creation (IC) Function

Requirement ID	Description	FTK Imager	Helix 3 Pro	AIR
TSP-RIC-01	If an image creation is selected the tool shall create the image in the selected format and destination with all the data acquired.	✓	✓	✓
TSP-RIC-02	If error occurs during the image file creation, the tool shall report to the user of the condition	✓	✗	✗
TSP-RIC-03	If space is insufficient on the selected image destination device during an image file creation, the tool shall report to the user of the condition	✓	✓	✗
TSP-RIC-04	If multi-file image creation and the image file size is selected, the tool shall create a multi-file image with the requested size which contains all the data acquired	✓	✓	✓
TSP-RIC-05	if the image file integrity check is selected, the tool shall report to the user whether the image file has been changed and if the image file has been changed the location should be reported	✗	N/A	N/A
TSP-RIC-06	If image format conversion is selected, the target image file format should contain same data as the original image file	✓	✓	✓
TSP-RIC-07	The tool shall allow the user select an alternate destination device to continue image creation process if there is insufficient space in destination device and destination device switching function is supported. The multi-image file should represent the same data as acquired by the tool	✓	✓	✗
TSP-RIC-08	The tool shall notify the user of any irregularities in the configuration of the digital source.	✗	✗	✗

Logging Function (LOG)

Requirement ID	Description	FTK Imager	Helix 3 Pro	AIR
TSP-RLOG-01	If the tool offers log file creation then the tool shall record at least one of the following information: tool version, tool settings, acquisition date and/or time, device size, device manufacturer, device model number, device serial number, partition table, amount of data acquired and user comments.	✓	✓	✓
TSP-RLOG-02	The tool shall display correct information about the acquisition. The essential information must display to the user.	✗	✗	✓
TSP-RLOG-03	The tool shall display correct information regarding to the acquisition to the user and consistent with the log file if the log file function is supported	✓	✓	✓

Hidden Sector (HS)

Requirement ID	Description	FTK Imager	Helix 3 Pro	AIR
TSP-RHS-01	The tool shall report to the user if it detects hidden sectors are contained in digital source	✗	✗	✗
TSP-RHS-02	The tool shall report to the user that hidden sectors may present but undetected if it cannot detect hidden sectors on the digital source	✗	✗	✗
TSP-RIC-03	The tool shall report to the user that hidden sectors will not be acquired if it cannot acquire hidden sectors on the digital source	✗	✗	✗

Appendix 7 – Disk Imaging Tools Test Results

Testing Environment, Support Software and Test Report Key

Testing Environment:

Test Station 1 Windows Environment	Test Station 2 Linux Environment
Intel® Core(TM) i5 CPU 750 @2.67GHz	Intel® Core2(TM) CPU 6300 @1.86GHz
Gigabyte Motherboard GA-P55A-UD4	EPox 5P965 Motherboard
BIOS version F6	
On board USB 2.0, USB3.0, Ethernet, SATA and PATA controllers	On board USB 2.0, Ethernet, SATA and PATA controllers
Texas Instruments 1394 OHCI Host controller	1.44 MB floppy drive
4GB Ram	3GB Ram
ASUS DVD-RW DRW-24B1ST ATA Device	Pioneer DVD-RW DVR-111D ATA device
SAMSUNG HD103SJ SATA drive 1TB	Seagate ST3250823AS SATA drive 250Gb
Windows 7, Windows XP SP3 with latest system updates or Virtualised Windows XP SP3	Ubuntu 9.04 LTS

Support Software:

Software	Version	Description
MHDD	4.5	Low-level HDD Diagnostics Software
UltraEdit	16.10.0.1036	Hex Editor
Darik's Boot and Nuke	2.2.6	Used to securely wipe the test drive
Hdparm	9.29	Linux Hard drive tool, used to check and change parameter of the test hard drive
Gparted	0.6.2	Linux hard drive partitioning tool
Disk Management Tool	1.0.0	Windows hard disk partitioning tool (Supports GPT partition style)
Disk_stat	3.1.2	Used to check the existence of Host protected areas
EnCase	6.16.1	Used to verify the hash value of the acquired images
WinHex	15.6	Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor from X-Ways Software

Test Results Report Key:

Heading	Description
Test & Case Summary:	Test ID, Test Date, Case name and summary of the test case.
Assertion	The test assertion that applicable to the test case stated above. Assertions are selected from the test assertion in Appendix 3.
Source Drive:	Name, model, capacity and Serial Number.
Drive Setup:	Configuration of the source drive.
Log highlights:	The information extracted from log files that highlight the importance of the test.
Results by assertion:	Expected and actual result for each assertion tested. Result will be indicated as Pass/fail per assertion tested.
Analysis:	Indicate whether the expected results achieved and provide simple analysis of the results.

Test Results – FTK Imager

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

1.1 TC-01-FW

Test Case TC-01-FW **(FTK Imager 2.9.0.1385)**	
Test & Case Summary:	TC-01 Acquire a hard drive using Access Interface (AI) and convert to an image file
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	Source hashes MD5 checksum: 436a043c1766f46f3945e605144f22eb SHA1 checksum: 82d4b6226995d11b82979db901e809a06b1574e8 /dev/sda: current max LBA: 156,296,385 /dev/sda: native max LBA: 156,296,385 /dev/sda: physical max LBA: 156,296,385 /dev/sda: HPA not set /dev/sda: DCO not set
Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Source data size: 76319 MB Sector count: 156301488 MD5 checksum: 436a043c1766f46f3945e605144f22eb SHA1 checksum: 82d4b6226995d11b82979db901e809a06b1574e8 Acquisition started: Mon Jun 28 00:16:23 2010 Acquisition finished: Mon Jun 28 01:07:57 2010 Verification started: Mon Jun 28 01:07:57 2010 Verification finished: Mon Jun 28 01:24:05 2010 MD5 checksum: 436a043c1766f46f3945e605144f22eb : verified

	SHA1 checksum: 82d4b6226995d11b82979db901e809a06b1574e8 : verified
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

1.2 TC-01-USB

Test Case TC-01-USB (FTK Imager 2.9.0.1385)	
Test & Case Summary:	TC-01 Acquire a hard drive using Access Interface (AI) and convert to an image file
Assertions:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: USB 2.0 Drive (4GB) Serial Number: N/A Sector count: 7,987,200 Write blocker: N/A
Drive Setup:	Source hashes MD5 checksum: fcf954774adec1eefb4b873b3c8f3612 SHA1 checksum: 033772e928aea0c52827574cfb2c7f020062aa84 /dev/sda: current max LBA: 7,987,200 /dev/sda: native max LBA: 7,987,200 /dev/sda: physical max LBA: 7,987,200

	/dev/sda: HPA not set /dev/sda: DCO not set
Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Cylinders: 497 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 7,987,200 Drive Model: USB2.0 Flash Disk USB Device **Drive Serial Number:** Drive Interface Type: USB Source data size: 3900 MB Sector count: 7987200 MD5 checksum: fcf954774adec1eefb4b873b3c8f3612 SHA1 checksum: 033772e928aea0c52827574cfb2c7f020062aa84 Acquisition started: Tue Sep 21 07:57:03 2010 Acquisition finished: Tue Sep 21 08:02:59 2010 Image Verification Results: Verification started: Tue Sep 21 08:03:00 2010 Verification finished: Tue Sep 21 08:04:23 2010 MD5 checksum: fcf954774adec1eefb4b873b3c8f3612 : verified SHA1 checksum: 033772e928aea0c52827574cfb2c7f020062aa84 : verified
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 PASSED AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

1.3 TC-02-NTFS

Test Case TC-02-NTFS (FTK Imager 2.9.0.1385)	
Test & Case Summary:	TC-02-NTFS Acquire a digital source that supported by the tools to an image file
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is

	selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	Source hashes MD5 checksum: 436a043c1766f46f3945e605144f22eb SHA1 checksum: 82d4b6226995d11b82979db901e809a06b1574e8 /dev/sda: current max LBA: 156,301,488 /dev/sda: native max LBA: 156,301,488 /dev/sda: physical max LBA: 156,301,488 /dev/sda: HPA not set /dev/sda: DCO not set
Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Source data size: 76319 MB Sector count: 156301488 MD5 checksum: 436a043c1766f46f3945e605144f22eb SHA1 checksum: 82d4b6226995d11b82979db901e809a06b1574e8 Acquisition started: Mon Jun 28 00:16:23 2010 Acquisition finished: Mon Jun 28 01:07:57 2010 Verification started: Mon Jun 28 01:07:57 2010 Verification finished: Mon Jun 28 01:24:05 2010 MD5 checksum: 436a043c1766f46f3945e605144f22eb : verified SHA1 checksum: 82d4b6226995d11b82979db901e809a06b1574e8 : verified
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 PASSED AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

1.4 TC-02-Ext2

<table>
<tr><td colspan="2">Test Case TC-02-Ext2 (FTK Imager 2.9.0.1385)</td></tr>
<tr><td>Test & Case Summary:</td><td>TC-02 Acquire a digital source that supported by the tools to an image file

Notes: Acquire Ext2 only in a multi-partitioned HD (with WriteBlocker, Partition size 2047MB)</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: b5c637ffdd3c94d855be01391ada64fe
SHA1 checksum: 4e681e1197929248a1e968943190d0886482c90b
/dev/sdb: current max LBA: 156,296,385
/dev/sdb: native max LBA: 156,296,385
/dev/sdb: physical max LBA: 156,296,385
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>6297479</td><td>6297417</td><td>NTFS</td><td>3Gb</td></tr>
<tr><td>/dev/sdb2</td><td>6297543</td><td>10490444</td><td>4192902</td><td>Ext2</td><td>2Gb</td></tr>
<tr><td>/dev/sdb3</td><td>10490508</td><td>14683409</td><td>4192902</td><td>Ext3</td><td>2Gb</td></tr>
<tr><td>/dev/sdb4</td><td>14683473</td><td>16787924</td><td>2104452</td><td>FAT16</td><td>1Gb</td></tr>
<tr><td>/deb/sdb5</td><td>18892503</td><td>20996954</td><td>2104452</td><td>Swap</td><td>1Gb</td></tr>
</table>
</td></tr>
</table>

Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Starting Sector: 6,297,543 Sector Count: 4,192,902 Source data size: 2047 MB MD5 checksum: b5c637ffdd3c94d855be01391ada64fe SHA1 checksum: 4e681e1197929248a1e968943190d0886482c90b Acquisition started: Tue Jul 27 01:51:51 2010 Acquisition finished: Tue Jul 27 01:53:11 2010 Verification started: Tue Jul 27 01:53:11 2010 Verification finished: Tue Jul 27 01:53:43 2010 MD5 checksum: b5c637ffdd3c94d855be01391ada64fe : verified SHA1 checksum: 4e681e1197929248a1e968943190d0886482c90b : verified
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 PASSED AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

1.5 TC-02-Ext3

Test Case TC-02-Ext3 **(FTK Imager 2.9.0.1385)**	
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire Ext3 only in a multi-partitioned HD (with WriteBlocker, Partition size 2047MB)
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

<table>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: dd010be4950db17ebe05b213cd57f6c4
SHA1 checksum: c4069f4a8681ef7e4cfed734f4b8794646039fc5
/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>6297479</td><td>6297417</td><td>NTFS</td><td>3Gb</td></tr>
<tr><td>/dev/sdb2</td><td>6297543</td><td>10490444</td><td>4192902</td><td>Ext2</td><td>2Gb</td></tr>
<tr><td>/dev/sdb3</td><td>10490508</td><td>14683409</td><td>4192902</td><td>Ext3</td><td>2Gb</td></tr>
<tr><td>/dev/sdb4</td><td>14683473</td><td>16787924</td><td>2104452</td><td>FAT16</td><td>1Gb</td></tr>
<tr><td>/deb/sdb5</td><td>18892503</td><td>20996954</td><td>2104452</td><td>Swap</td><td>1Gb</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
Starting Sector: 10,490,508
Sector Count: 4,192,902
Source data size: 2047 MB
MD5 checksum: dd010be4950db17ebe05b213cd57f6c4
SHA1 checksum: c4069f4a8681ef7e4cfed734f4b8794646039fc5
Acquisition started: Tue Jul 27 01:56:23 2010
Acquisition finished: Tue Jul 27 01:57:43 2010
Verification started: Tue Jul 27 01:57:43 2010
Verification finished: Tue Jul 27 01:58:18 2010
MD5 checksum: dd010be4950db17ebe05b213cd57f6c4 : verified
SHA1 checksum: c4069f4a8681ef7e4cfed734f4b8794646039fc5 : verified</td></tr>
<tr><td>Results by assertion:</td><td>AFR-01 PASSED
AFR-02 PASSED
AFR-03 PASSED
AFR-04 PASSED
AFR-05 PASSED
AFR-07 PASSED</td><td>AIC-01 PASSED
AIC-05 PASSED
ALOG-01 PASSED
ALOG-02 PASSED
ALOG-03 PASSED</td></tr>
<tr><td>Analysis:</td><td>Test achieved the expected Result. Source hashes match verification hashes.</td></tr>
</table>

1.6 TC-02-FAT16

<table>
<tr><td colspan="2">Test Case TC-02-FAT16 (FTK Imager 2.9.0.1385)</td></tr>
<tr><td>Test & Case Summary:</td><td>TC-02 Acquire a digital source that supported by the tools to an image file

Notes: Acquire FAT16 only in a multi-partitioned HD (with WriteBlocker, Partition size 1027MB)</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: b446594538d0f400fb80f54f6c78c481
SHA1 checksum: 1a647d852f8ae609111a601b88091596ab2e8d92
/dev/sdb: current max LBA: 156,296,385
/dev/sdb: native max LBA: 156,296,385
/dev/sdb: physical max LBA: 156,296,385
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>6297479</td><td>6297417</td><td>NTFS</td><td>3Gb</td></tr>
<tr><td>/dev/sdb2</td><td>6297543</td><td>10490444</td><td>4192902</td><td>Ext2</td><td>2Gb</td></tr>
<tr><td>/dev/sdb3</td><td>10490508</td><td>14683409</td><td>4192902</td><td>Ext3</td><td>2Gb</td></tr>
<tr><td>/dev/sdb4</td><td>14683473</td><td>16787924</td><td>2104452</td><td>FAT16</td><td>1Gb</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>20996954</td><td>2104452</td><td>Swap</td><td>1Gb</td></tr>
</table></td></tr>
</table>

Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Starting Sector: 14,683,473 Sector Count: 2,104,452 Source data size: 1027 MB MD5 checksum: b446594538d0f400fb80f54f6c78c481 SHA1 checksum: 1a647d852f8ae609111a601b88091596ab2e8d92 Acquisition started: Tue Jul 27 01:58:03 2010 Acquisition finished: Tue Jul 27 01:58:43 2010 Verification started: Tue Jul 27 01:58:43 2010 Verification finished: Tue Jul 27 01:58:50 2010 MD5 checksum: b446594538d0f400fb80f54f6c78c481 : verified SHA1 checksum: 1a647d852f8ae609111a601b88091596ab2e8d92 : verified
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 PASSED AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

1.7 TC-02-FAT32

Test Case TC-02-FAT32 (FTK Imager 2.9.0.1385)	
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire FAT32 only in a multi-partitioned HD (with WriteBlocker, Partition size 1027MB) Sector first from 4193028 to 6297479. total: 2104452
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user.

<table>
<tr><td></td><td>ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: 2c22fded78dc8ccc2c935944883a2e1b
SHA1 checksum: 10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5
/dev/sdb: current max LBA: 156,296,385
/dev/sdb: native max LBA: 156,296,385
/dev/sdb: physical max LBA: 156,296,385
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>4192964</td><td>4192902</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sdb3</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sdb4</td><td>10490508</td><td>12594959</td><td>2104452</td><td>Ext2</td></tr>
<tr><td>/dev/sdb5</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
Starting Sector: 4,193,028
Sector Count: 2,104,452
Source data size: 1027 MB
MD5 checksum: 2c22fded78dc8ccc2c935944883a2e1b
SHA1 checksum: 10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5
Acquisition started: Tue Jul 27 07:07:32 2010
Acquisition finished: Tue Jul 27 07:08:15 2010
Verification started: Tue Jul 27 07:08:15 2010
Verification finished: Tue Jul 27 07:08:20 2010
MD5 checksum: 2c22fded78dc8ccc2c935944883a2e1b : verified
SHA1 checksum: 10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5 : verified</td></tr>
<tr><td>Results by assertion:</td><td>
<table>
<tr><td>AFR-01 PASSED</td><td>AIC-01 PASSED</td></tr>
<tr><td>AFR-02 PASSED</td><td>AIC-05 PASSED</td></tr>
<tr><td>AFR-03 PASSED</td><td>ALOG-01 PASSED</td></tr>
<tr><td>AFR-04 PASSED</td><td>ALOG-02 PASSED</td></tr>
<tr><td>AFR-05 PASSED</td><td>ALOG-03 PASSED</td></tr>
<tr><td>AFR-07 PASSED</td><td></td></tr>
</table>
</td></tr>
<tr><td>Analysis:</td><td>Test achieved the expected Result. Source hashes match verification hashes.</td></tr>
</table>

1.8 TC-02-SWAP

<table>
<tr><td colspan="2">Test Case TC-02-SWAP (FTK Imager 2.9.0.1385)</td></tr>
<tr><td>Test & Case Summary:</td><td>TC-02 Acquire a digital source that supported by the tools to an image file
Notes: Acquire SWAP partition only in a multi-partitioned HD (with Write blocker, Partition size 1027MB)</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: 4e1e7f58383e4d89b6357293005cd1b3
SHA1 checksum: 8ff9faac1941b857c945c275c21bbc1ab7e0c399
/dev/sdb: current max LBA: 156,296,385
/dev/sdb: native max LBA: 156,296,385
/dev/sdb: physical max LBA: 156,296,385
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>4192964</td><td>4192902</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sdb3</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sdb4</td><td>10490508</td><td>12594959</td><td>2104452</td><td>Ext2</td></tr>
<tr><td>/dev/sdb5</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
</table>
</td></tr>
</table>

Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Starting Sector: 18,892,503 Sector Count: 2,104,452 Source data size: 1027 MB MD5 checksum: 4e1e7f58383e4d89b6357293005cd1b3 SHA1 checksum: 8ff9faac1941b857c945c275c21bbc1ab7e0c399 Acquisition started: Tue Jul 27 02:02:20 2010 Acquisition finished: Tue Jul 27 02:03:00 2010 Verification started: Tue Jul 27 02:03:00 2010 Verification finished: Tue Jul 27 02:03:06 2010 MD5 checksum: 4e1e7f58383e4d89b6357293005cd1b3 : verified SHA1 checksum: 8ff9faac1941b857c945c275c21bbc1ab7e0c399 : verified
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

1.9 TC-02-HFS

Test Case TC-02-HFS (FTK Imager 2.9.0.1385)		
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire Mac partition type HFS partition only	
Assertion:	AFR-01	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

<table>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
md5: d8235a6c57ddf91c902d42f0e39cb7d5
sha1: b91e9115388276b961e6a94a6322337048734d6c
/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>4096</td><td>4198399</td><td>4194304</td><td>HFS</td><td>2Gb</td></tr>
<tr><td>/dev/sdb2</td><td>4198400</td><td>14999551</td><td>10801152</td><td>HFS+</td><td>5Gb</td></tr>
<tr><td>Unallocated</td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
Starting Sector: 4,096
 Sector Count: 4,194,304
 Source data size: 2048 MB
 Sector count: 4194304
[Computed Hashes]
 MD5 checksum: d8235a6c57ddf91c902d42f0e39cb7d5
 SHA1 checksum: b91e9115388276b961e6a94a6322337048734d6c
Segment list:
  E:\Image\FTK_HFS.001
  E:\Image\FTK_HFS.002
Acquisition started: Sun Oct 03 10:18:17 2010
Acquisition finished: Sun Oct 03 10:19:38 2010
Verification started: Sun Oct 03 10:19:38 2010
Verification finished: Sun Oct 03 10:20:07 2010
MD5 checksum: d8235a6c57ddf91c902d42f0e39cb7d5 : verified
SHA1 checksum: b91e9115388276b961e6a94a6322337048734d6c : verified</td></tr>
<tr><td>Results by assertion:</td><td>AFR-01 PASSED   AIC-01 PASSED
AFR-02 PASSED   AIC-05 PASSED
AFR-03 PASSED   ALOG-01 PASSED
AFR-04 PASSED   ALOG-02 PASSED
AFR-05 PASSED   ALOG-03 PASSED
AFR-07 PASSED</td></tr>
<tr><td>Analysis:</td><td>Test achieved the expected Result. Source hashes match verification hashes.</td></tr>
</table>

1.10 TC-02-HFS+

Test Case TC-02-HFS+ (FTK Imager 2.9.0.1385)	
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire Apple Mac partition type HFS+ partition only
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	Source hashes md5: 5781d0f597685d4eff4cc3423900d73a sha1: e878400c062b1690b586be41523d303edf3eae52 /dev/sda: current max LBA: 156,301,488 /dev/sda: native max LBA: 156,301,488 /dev/sda: physical max LBA: 156,301,488 /dev/sda: HPA not set /dev/sda: DCO not set
Partition Table:	**Device** **Start** **End** **#sectors** **File System** **Size** /dev/sdb1 4096 4198399 4194304 HFS 2Gb **/dev/sdb2** **4198400** **14999551** **10801152** **HFS+** **5Gb** Unallocated
Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Starting Sector: 4,198,400 Sector Count: 10,801,152 Source data size: 5274 MB Sector count: 10801152 MD5 checksum: 5781d0f597685d4eff4cc3423900d73a SHA1 checksum: e878400c062b1690b586be41523d303edf3eae52

	Acquisition started: Fri Oct 01 15:26:57 2010 Acquisition finished: Fri Oct 01 15:30:29 2010 Segment list: E:\Image\FTK_Acquire_HFSplus.001 ………………………… E:\Image\FTK_Acquire_HFSplus.004 Verification started: Fri Oct 01 15:30:30 2010 Verification finished: Fri Oct 01 15:36:48 2010 MD5 checksum: 5781d0f597685d4eff4cc3423900d73a : verified SHA1 checksum: e878400c062b1690b586be41523d303edf3eae52 : verified
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 PASSED AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

1.11 TC-03-HPA

Test Case TC-03-HPA **(FTK Imager 2.9.0.1385)**		
Test & Case Summary:	TC-03 Acquire a hard drive with hidden sectors to an image file Notes: HPA active	
Assertion:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-06	The tool acquires all the hidden data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
	AHS-01	The tool reports to the user if any hidden sectors are found

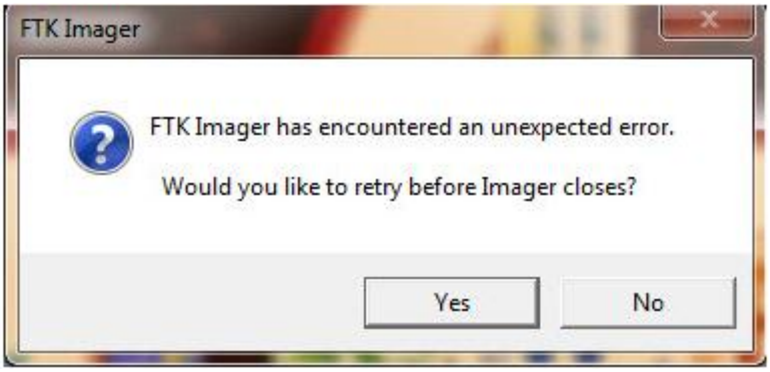
FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

	AHS-02 The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment **AHS-03** The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: N/A
Drive Setup:	Source hashes MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 /dev/sdb: current max LBA: **94,863,827** /dev/sdb: native max LBA: 94,863,827 /dev/sdb: physical max LBA: **156,301,487** /dev/sdb: **HPA set from sector 94,863,828 to 156,301,487** /dev/sdb: DCO not set
Partition Table:	**Device** **Start** **End** **#sectors** **File System** /dev/sdb1 63 41945714 41945652 NTFS /dev/sdb2 41945715 94863824 52918110 Ext3 /dev/sdb3 94863825 156296384 61432560 NTFS **(HPA)**
Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Cylinders: 5,905 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: **94,868,928** Drive Model: ST380817AS ATA Device Drive Serial Number: 5MR18V18 Drive Interface Type: IDE Source data size: **46322 MB** Sector count: **94,868,928** MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 Acquisition started: Thu Jul 22 12:22:59 2010 Acquisition finished: Thu Jul 22 12:42:25 2010 E:\Image\test003_HPA_ST380817AS.001 …………………….. E:\Image\test003_HPA_ST380817AS.031 Verification started: Thu Jul 22 12:50:44 2010 Verification finished: Thu Jul 22 12:59:01 2010 MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd : verified SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 : verified

	 FTK Imager has encountered an unexpected error. Would you like to retry before Imager closes?
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. FTK Imager failed to detect and acquire the hidden areas in the hard drive. FTK Imager encountered an unexpected error when creating the list of directories of the acquired data. However, all the data is still acquired accurately and correctly.

1.12 TC-03-DCO

Test Case TC-03-DCO (FTK Imager 2.9.0.1385)	
Test & Case Summary:	TC-03 Acquire a hard drive with hidden sectors to an image file Notes: DCO actived
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-06** The tool acquires all the hidden data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported **AHS-01** The tool reports to the user if any hidden sectors are found **AHS-02** The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment **AHS-03** The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,487 Write blocker: N/A
Drive Setup:	Source hashes MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 /dev/sdb: current max LBA: **94,863,827** /dev/sdb: native max LBA: 94,863,827 /dev/sdb: physical max LBA: **156,301,487** /dev/sdb: HPA not set /dev/sdb: **DCO set from sector 94,863,828 to 156,301,487**
Partition Table:	**Device** **Start** **End** **#sectors** **File System** /dev/sdb1 63 41945714 41945652 NTFS /dev/sdb2 41945715 94863824 52918110 Ext3

	/dev/sdb3 94863825 156296384 61432560 NTFS **(DCO)**
Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Cylinders: 5,905 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: **94,868,928** Drive Model: ST380817AS ATA Device Drive Serial Number: 5MR18V18 Drive Interface Type: IDE Source data size: **46322 MB** Sector count: **94868928** MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 Acquisition started: Mon Jul 26 20:00:03 2010 Acquisition finished: Mon Jul 26 20:16:17 2010 Segment list: H:\new\FTK_test003_DCO_ST380817AS.001 H:\new\FTK_test003_DCO_ST380817AS.002 …………………………… H:\new\FTK_test003_DCO_ST380817AS.031 Verification started: Mon Jul 26 20:16:17 2010 Verification finished: Mon Jul 26 20:23:58 2010 MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd : verified SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 : verified  FTK Imager has encountered an unexpected error. Would you like to retry before Imager closes?
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. FTK Imager failed to detect and acquire the hidden areas in the hard drive. During the acquisition process, FTK Imager encountered an unexpected error twice and the debugging information is also provided by FTK Imager.

1.13 TC-05-DD

<table>
<tr><th colspan="2">Test Case TC-05-DD (FTK Imager 2.9.0.1385)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a digital source to an image file in an alternate supported format
Notes: Acquire image to DD image format</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool.
AIC-02 The tool creates an image file according to the file format the user specified.
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes:
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Total sectors: 2104452 (1024MB)
/dev/sdb: current max LBA: 156,296,385
/dev/sdb: native max LBA: 156,296,385
/dev/sdb: physical max LBA: 156,296,385
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
</table>

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Starting Sector: 12,595,023 Sector Count: 2,104,452 Source data size: 1027 MB Sector count: 2104452 MD5 checksum: f7c2c38630b0c995732a87cce003dcca SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed Acquisition started: Wed Aug 11 03:34:53 2010 Acquisition finished: Wed Aug 11 03:35:36 2010 Verification started: Wed Aug 11 03:35:36 2010 Verification finished: Wed Aug 11 03:35:42 2010 MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes and the hash of the original DD image.

1.14 TC-05-Smart

<table>
<tr><td colspan="2">Test Case TC-05-Smart (FTK Imager 2.9.0.1385)</td></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a digital source to an image file in an alternate supported format
Notes: Acquire image to Smart image format</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool.
AIC-02 The tool creates an image file according to the file format the user specified.
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Total sectors: 2104452 (1024MB)
/dev/sda: current max LBA: 156,296,385
/dev/sda: native max LBA: 156,296,385
/dev/sda: physical max LBA: 156,296,385
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table></td></tr>
</table>

Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Starting Sector: 12,595,023 Sector Count: 2,104,452 Source data size: 1027 MB Sector count: 2104452 MD5 checksum: f7c2c38630b0c995732a87cce003dcca SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed Acquisition started: Wed Aug 11 03:37:58 2010 Acquisition finished: Wed Aug 11 03:38:41 2010 Verification started: Wed Aug 11 03:38:41 2010 Verification finished: Wed Aug 11 03:38:58 2010 MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-02 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 PASSED AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes and the hash of the original DD image.

1.15 TC-05-E01

Test Case TC-05-E01 (FTK Imager 2.9.0.1385)	
Test & Case Summary:	Acquire a digital source to an image file in an alternate supported format Notes: Acquire image to E01 format image format
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool. AIC-02 The tool creates an image file according to the file format the user specified. ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user.

<table>
<tr><td></td><td>ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Total sectors: 2104452 (1024MB)
/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
Starting Sector: 12,595,023
Sector Count: 2,104,452
Source data size: 1027 MB
Sector count: 2104452
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Acquisition started: Wed Aug 11 03:40:11 2010
Acquisition finished: Wed Aug 11 03:40:57 2010
Verification started: Wed Aug 11 03:40:57 2010
Verification finished: Wed Aug 11 03:41:18 2010
MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified</td></tr>
</table>

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes and the hash of the original DD image.

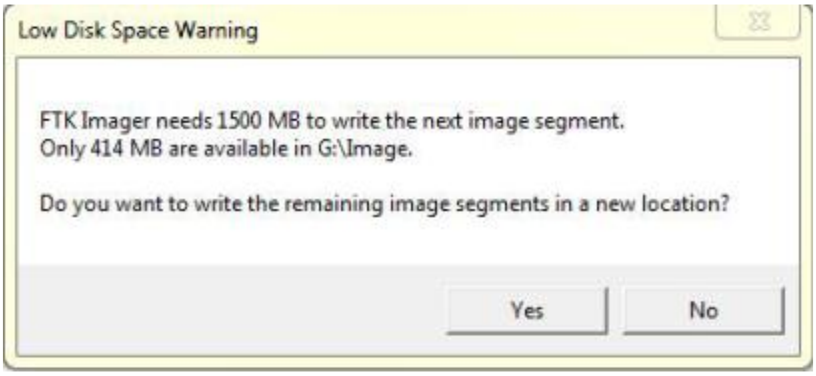
1.16 TC-06-UNC

Test Case TC-06-UNC (FTK Imager 2.9.0.1385)		
Test & Case Summary:	Acquire a digital source that has at least one faulty data sector Notes: 15 UNC errors existed	
Assertion:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AFR-08	The tool report to the user of the error type and the location of the error if error occurred during the reading from a digital source.
	AFR-09	If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-03	The tool reports to the user if an error occurs during the image creation process.
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device	

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

Drive Setup:	/dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA not set /dev/sdb: DCO not set Faulty sectors marked: 5161564, 12135645, 16429701, 28210195, 33486075, 40694940, 40828560, 57691700, 90179820, 91800252, 92763320, 104129017, 109477200, 118026966, 140386491
Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Cylinders: 9,729 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 156,301,488 Drive Serial Number: 02cc0e0010903500 Drive Interface Type: 1394 Source data size: 76319 MB Sector count: 156301488 **ATTENTION:** The following sector(s) on the source drive could not be read: 5161564, 12135645, 16429701, 28210195, 33486075, 40694940, 40828560, 57691700, 90179820, 91800252, 92763320, 104129017, 109477200, 118026966, 140386491 **The contents of these sectors were replaced with zeros in the image.** Checked - Zero filled into the 15 sectors that FTK imager could not read. MD5 checksum: 1b26c0e62b79f528793199a3d2de4034 SHA1 checksum: 52bafa6d754870b33cb85089ae89538c9355844c Acquisition started: Thu Aug 05 23:50:45 2010 Acquisition finished: Fri Aug 06 00:44:31 2010 Segment list: E:\Image\Test-UNC-Errors.001 E:\Image\Test-UNC-Errors.002 ……………………. E:\Image\Test-UNC-Errors.051 Verification started: Fri Aug 06 00:44:33 2010 Verification finished: Fri Aug 06 01:04:12 2010 MD5 checksum: 1b26c0e62b79f528793199a3d2de4034 : verified SHA1 checksum: 52bafa6d754870b33cb85089ae89538c9355844c : verified
Results by assertion:	AFR-01 PASSED AIC-01 PASSED ALOG-01 PASSED AFR-02 PASSED AIC-02 PASSED ALOG-02 PASSED AFR-03 PASSED AIC-03 PASSED ALOG-03 PASSED AFR-04 PASSED AFR-05 PASSED AIC-06 PASSED AFR-07 PASSED AIC-07 PASSED AFR-08 PASSED AIC-08 PASSED AFR-09 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

1.17 TC-07- Insufficient space & TC-08

Test Case TC-07-Insufficient space & TC-08 (FTK Imager 2.9.0.1385)	
Test & Case Summary:	Attempt to create an image file where destination device has insufficient space , and see whether the tool notifies the user and offer another destination device to continue
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-04** The tool reports to the user if insufficient space in the destination device during the image creation process. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-10** The tool reports to the user if insufficient space in the destination device to contain the multi-image file creation and if destination device switching function is supported, the image is continue on the selected destination device. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdc: current max LBA: 156,296,385 /dev/sdc: native max LBA: 156,296,385 /dev/sdc: physical max LBA: 156,296,385 /dev/sdc: HPA not set /dev/sdc: DCO not set
Partition Table:	**Device** **Start** **End** **#sectors** **System** unallocated 0 156296384 156296385 Empty
Log highlights:	 FTK Imager needs 1500 MB to write the next image segment. Only 414 MB are available in G:\Image. Do you want to write the remaining image segments in a new location?

Results by assertion:	**TC-07** AFR-01 PASSED ALOG-01 PASSED AFR-02 PASSED ALOG-02 PASSED AFR-03 PASSED ALOG-03 PASSED AFR-04 PASSED AIC-04 PASSED **TC-08** AFR-01 PASSED AIC-04 PASSED ALOG-01 PASSED AFR-02 PASSED AIC-05 PASSED ALOG-02 PASSED AFR-03 PASSED AIC-10 PASSED ALOG-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED
Analysis:	Test result **PASSED**. Notification has provided to the user that the destination device does not have enough free space to store the full image. Space checking is not done prior to the image acquisition.

1.18 TC-09-VerifyImage

Test Case TC-09-VerifyImage (FTK Imager 2.9.0.1385)	
Test & Case Summary:	Verify a correct image Notes: The image of FAT16 partition.
Assertion:	AFR-03 The tool operates in an execution environment AIC-06 If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,301,488 Write blocker: N/A
Drive Setup:	**Source image hashes** MD5 checksum: cbf8f802e41c7ddbfb0afeaa5c7d0de0 SHA1 checksum: fa59e48af260bcd9e874286b0e1026f03b461220 Total sectors: 4192902 (2047MB) /dev/sda: current max LBA: 156,301,488 /dev/sda: native max LBA: 156,301,488 /dev/sda: physical max LBA: 156,301,488 /dev/sda: HPA not set

<table>
<tr><td></td><td>/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
Bytes per Sector: 512
Sector Count: 4,192,902
Source data size: 2047 MB
Sector count: 4192902
MD5 checksum: cbf8f802e41c7ddbfb0afeaa5c7d0de0
SHA1 checksum: fa59e48af260bcd9e874286b0e1026f03b461220
Acquisition started: Tue Aug 03 00:18:22 2010
Acquisition finished: Tue Aug 03 00:19:53 2010
Segment list:
  D:\Images\Test009-Verify_Image_Fat16.001
  D:\Images\Test009-Verify_Image_Fat16.002
Verification started: Tue Aug 03 00:19:56 2010
Verification finished: Tue Aug 03 00:20:53 2010
MD5 checksum: cbf8f802e41c7ddbfb0afeaa5c7d0de0 : verified
SHA1 checksum: fa59e48af260bcd9e874286b0e1026f03b461220 : verified</td></tr>
<tr><td>Results by assertion:</td><td>AFR-03 PASSED   ALOG-01 PASSED
AIC-06   PASSED   ALOG-02 PASSED
ALOG-03 PASSED</td></tr>
<tr><td>Analysis:</td><td>Test achieved the expected Result. Source hashes match verification hashes.</td></tr>
</table>

1.19 TC-10-CorruptImage

<table>
<tr><td colspan="2">Test Case TC-10-CorruptImage (FTK Imager 2.9.0.1385)</td></tr>
<tr><td>Test & Case Summary:</td><td>Try verifying a corrupted image
Notes: The image of FAT32 partition.</td></tr>
<tr><td>Assertion:</td><td>AFR-03 The tool operates in an execution environment
AIC-06 If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
AIC-07 If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
AIC-08 If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td>Source image hashes
MD5 checksum: 2c22fded78dc8ccc2c935944883a2e1b
SHA1 checksum: 10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5
Total sectors: 2104452 (1027MB)
Address: Offset 35df5f70h Column 8 change byte from 43 to 42
/dev/sda: current max LBA: 156,296,385
/dev/sda: native max LBA: 156,296,385
/dev/sda: physical max LBA: 156,296,385
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
Notes: Acquire FAT32 partition only (sector first from 4193028 to 6297479. total: 2104452).</td></tr>
</table>

```
Starting Sector: 4,193,028
Sector Count: 2,104,452
Source data size: 1027 MB
Sector count:    2104452
MD5 checksum:    2c22fded78dc8ccc2c935944883a2e1b
SHA1 checksum:   10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5
Acquisition started:   Tue Jul 27 07:07:32 2010
Acquisition finished:  Tue Jul 27 07:08:15 2010
Segment list:
  E:\Image\Test002-FTK-FAT32.001
Verification started:  Tue Jul 27 07:08:15 2010
Verification finished: Tue Jul 27 07:08:20 2010
MD5 checksum:    2c22fded78dc8ccc2c935944883a2e1b : verified
SHA1 checksum:   10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5 :
verified
Verification started:  Mon Aug 02 23:50:02 2010
Verification finished: Mon Aug 02 23:50:13 2010
MD5 checksum:    2c22fded78dc8ccc2c935944883a2e1b : verified
SHA1 checksum:   10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5 :
verified
```

Verify an image that had one byte changed from the source image file:

```
Created By AccessData® FTK® Imager 2.9.0.1385 100406
Notes: Acquire FAT32 partition only (sector first from 4193028 to
6297479. total: 2104452). writeblocker used
Starting Sector: 4,193,028
Sector Count: 2,104,452
Source data size: 1027 MB
Sector count:    2104452
MD5 checksum:    2c22fded78dc8ccc2c935944883a2e1b
SHA1 checksum:   10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5
Acquisition started:   Tue Jul 27 07:07:32 2010
Acquisition finished:  Tue Jul 27 07:08:15 2010
Segment list:
  E:\Image\Test002-FTK-FAT32.001

Verification started:  Tue Jul 27 07:08:15 2010
Verification finished: Tue Jul 27 07:08:20 2010
MD5 checksum:    2c22fded78dc8ccc2c935944883a2e1b : verified
SHA1 checksum:   10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5 :
verified

Verification started:  Mon Aug 02 23:50:02 2010
Verification finished: Mon Aug 02 23:50:13 2010
MD5 checksum:    2c22fded78dc8ccc2c935944883a2e1b : verified
SHA1 checksum:   10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5 :
verified

Verification started:  Tue Aug 03 00:03:18 2010
Verification finished: Tue Aug 03 00:03:24 2010
```

	MD5 checksum: 771c7d34ed7a9b12e1419d8783b0f3e7 : **FAILED** SHA1 checksum: b9929b149d49658e418138eefa1aa9e49fc97710 : **FAILED**
Results by assertion:	AFR-03 PASSED ALOG-01 PASSED AIC-06 PASSED ALOG-02 PASSED AIC-07 PASSED ALOG-03 PASSED AIC-08 **FAILED**
Analysis:	Test **FAILED** to achieve the expected Result. FTK Imager detected the image has corrupted. However, the location of the corrupted data is not reported to the user.

1.20 TC-11-E01_DD

Test Case TC-11-E01_DD **(FTK Imager 2.9.0.1385)**	
Test & Case Summary:	Convert an existing image file to another image file format Notes: Convert image from E01 to DD format
Assertion:	AFR-03 The tool operates in an execution environment AFR-09 If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data. ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: N/A Image: Original E01 Image.
Drive Setup:	Source E01 image hashes MD5 checksum: f7c2c38630b0c995732a87cce003dcca SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed Total sectors: 2104452 (1024MB) /dev/sda: current max LBA: 156,296,385 /dev/sda: native max LBA: 156,296,385 /dev/sda: physical max LBA: 156,296,385 /dev/sda: HPA not set /dev/sda: DCO not set

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

<table>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
MD5 verification hash: f7c2c38630b0c995732a87cce003dcca
SHA1 verification hash: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Bytes per Sector: 512
Sector Count: 2,104,452
Acquired on OS: Windows 200x
Acquired using: ADI2.9.0.13
Acquire date: 8/10/2010 3:40:11 PM
System date: 8/10/2010 3:40:11 PM
Unique description: untitled
Source data size: 1027 MB
Sector count: 2104452
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Acquisition started: Wed Aug 11 03:46:55 2010
Acquisition finished: Wed Aug 11 03:47:31 2010
Segment list:
G:\new\Test005-AltFor-FTK\Test005-FTK-E01toDD.001
Verification started: Wed Aug 11 03:47:31 2010
Verification finished: Wed Aug 11 03:47:38 2010
MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified</td></tr>
<tr><td>Results by assertion:</td><td>AFR-03 PASSED
AFR-09 PASSED
ALOG-01 PASSED
ALOG-02 PASSED
ALOG-03 PASSED</td></tr>
<tr><td>Analysis:</td><td>Test achieved the expected Result. Source hashes match verification hashes and the hash of the original EnCase E01 image.</td></tr>
</table>

1.21 TC-11-E01_Smart

<table>
<tr><td colspan="2">Test Case TC-11-E01_Smart (FTK Imager 2.9.0.1385)</td></tr>
<tr><td>Test & Case Summary:</td><td>Convert an existing image file to another image file format
Notes: Convert image from E01 to Smart format</td></tr>
<tr><td>Assertion:</td><td>
<table>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-09</td><td>If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table>
</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: N/A
Image: Original E01 Image.</td></tr>
<tr><td>Drive Setup:</td><td>Source E01 image hashes
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Total sectors: 2104452 (1024MB)
/dev/sda: current max LBA: 156,296,385
/dev/sda: native max LBA: 156,296,385
/dev/sda: physical max LBA: 156,296,385
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
</table>

Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 MD5 verification hash: f7c2c38630b0c995732a87cce003dcca SHA1 verification hash: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed Bytes per Sector: 512 Sector Count: 2,104,452 Image Type: E01 Acquired on OS: Windows 200x Acquired using: ADI2.9.0.13 Acquire date: 8/10/2010 3:40:11 PM System date: 8/10/2010 3:40:11 PM Unique description: untitled Source data size: 1027 MB Sector count: 2104452 MD5 checksum: f7c2c38630b0c995732a87cce003dcca SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed Acquisition started: Wed Aug 11 03:48:23 2010 Acquisition finished: Wed Aug 11 03:48:55 2010 Segment list: G:\new\Test005-AltFor-FTK\Test005-FTK-E01toSmart.s01 Verification started: Wed Aug 11 03:48:55 2010 Verification finished: Wed Aug 11 03:49:14 2010 MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified
Results by assertion:	AFR-03 PASSED AFR-09 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes and the hash of the original EnCase E01 image.

1.22 TC-11-DD_E01

Test Case TC-11-DD_E01 **(FTK Imager 2.9.0.1385)**		
Test & Case Summary:	Convert an existing image file to another image file format Notes: Convert image from DD to E01 format	
Assertion:	AFR-03	The tool operates in an execution environment
	AFR-09	If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is

<table>
<tr><td></td><td>supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: N/A
Image: Original DD Image.</td></tr>
<tr><td>Drive Setup:</td><td>Source DD image hashes
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Total sectors: 2104452 (1024MB)
/dev/sda: current max LBA: 156,296,385
/dev/sda: native max LBA: 156,296,385
/dev/sda: physical max LBA: 156,296,385
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
Bytes per Sector: 512
Sector Count: 2,104,452
Image Type: Raw (dd)
Source data size: 1027 MB
Sector count: 2104452
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Acquisition started: Wed Aug 11 03:43:49 2010
Acquisition finished: Wed Aug 11 03:44:17 2010
Segment list:
G:\new\Test005-AltFor-FTK\Test005-FTK-DDtoE01.E01
Verification started: Wed Aug 11 03:44:17 2010
Verification finished: Wed Aug 11 03:44:35 2010
MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified</td></tr>
<tr><td>Results by assertion:</td><td>
<table>
<tr><td>AFR-03 PASSED</td><td>ALOG-01 PASSED</td></tr>
<tr><td>AFR-09 PASSED</td><td>ALOG-02 PASSED</td></tr>
<tr><td></td><td>ALOG-03 PASSED</td></tr>
</table>
</td></tr>
<tr><td>Analysis:</td><td>Test achieved the expected Result. Source hashes match verification hashes and the hash of the original DD image.</td></tr>
</table>

1.23 TC-11-DD_Smart

<table>
<tr><td colspan="2">Test Case TC-11-DD_Smart (FTK Imager 2.9.0.1385)</td></tr>
<tr><td>Test & Case Summary:</td><td>Convert an existing image file to another image file format
Notes: Convert image from DD to Smart format</td></tr>
<tr><td>Assertion:</td><td><table>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-09</td><td>If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table></td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: N/A
Image: Original DD Image.</td></tr>
<tr><td>Drive Setup:</td><td>Source DD image hashes
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Total sectors: 2104452 (1024MB)
/dev/sda: current max LBA: 156,296,385
/dev/sda: native max LBA: 156,296,385
/dev/sda: physical max LBA: 156,296,385
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table></td></tr>
</table>

Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Bytes per Sector: 512 Sector Count: 2,104,452 Image Type: Raw (dd) Source data size: 1027 MB Sector count: 2104452 MD5 checksum: f7c2c38630b0c995732a87cce003dcca SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed Acquisition started: Wed Aug 11 03:42:28 2010 Acquisition finished: Wed Aug 11 03:42:54 2010 Segment list: G:\new\Test005-AltFor-FTK\Test005-FTK-DDtoSmart.s01 Verification started: Wed Aug 11 03:42:54 2010 Verification finished: Wed Aug 11 03:43:10 2010 MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified
Results by assertion:	AFR-03 PASSED AFR-09 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes and the hash of the original DD image.

1.24 TC-11-Smart_DD

Test Case TC-11-Smart_DD **(FTK Imager 2.9.0.1385)**		
Test & Case Summary:	Convert an existing image file to another image file format Notes: Convert image from Smart to DD format	
Assertion:	AFR-03	The tool operates in an execution environment
	AFR-09	If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: N/A Image: Original Smart Image.	

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

<table>
<tr><td>Drive Setup:</td><td>Source Smart image hashes
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Total sectors: 2104452 (1024MB)
/dev/sda: current max LBA: 156,296,385
/dev/sda: native max LBA: 156,296,385
/dev/sda: physical max LBA: 156,296,385
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
MD5 verification hash: f7c2c38630b0c995732a87cce003dcca
SHA1 verification hash: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Bytes per Sector: 512
Sector Count: 2,104,452
Image Type: SMART ew-compressed
Acquired on OS: Windows 200x
Acquired using: ADI2.9.0.13
Acquire date: 8/10/2010 3:37:58 PM
System date: 8/10/2010 3:37:58 PM
Source data size: 1027 MB
Sector count: 2104452
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Acquisition started: Wed Aug 11 03:50:31 2010
Acquisition finished: Wed Aug 11 03:50:58 2010
Segment list:
  G:\new\Test005-AltFor-FTK\Test005-FTK-SmartToDD.001
Verification started: Wed Aug 11 03:50:58 2010
Verification finished: Wed Aug 11 03:51:04 2010
 MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified
 SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified</td></tr>
<tr><td>Results by assertion:</td><td>AFR-03 PASSED   ALOG-01 PASSED
AFR-09 PASSED   ALOG-02 PASSED
ALOG-03 PASSED</td></tr>
<tr><td>Analysis:</td><td>Test achieved the expected Result. Source hashes match verification hashes and the hash of the original Smart image.</td></tr>
</table>

1.25 TC-11-Smart_E01

<table>
<tr><td colspan="2">Test Case TC-11-Smart_E01 (FTK Imager 2.9.0.1385)</td></tr>
<tr><td>Test & Case Summary:</td><td>Convert an existing image file to another image file format
Notes: Convert image from Smart to EnCase E01 format</td></tr>
<tr><td>Assertion:</td><td>AFR-03 The tool operates in an execution environment
AFR-09 If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: N/A
Image: Original Smart Image.</td></tr>
<tr><td>Drive Setup:</td><td>Source Smart image hashes
MD5 checksum: f7c2c38630b0c995732a87cce003dcca
SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Total sectors: 2104452 (1024MB)
/dev/sda: current max LBA: 156,296,385
/dev/sda: native max LBA: 156,296,385
/dev/sda: physical max LBA: 156,296,385
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Setup:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th></tr>
<tr><td>/dev/sda1</td><td>63</td><td>41945714</td><td>41945652</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda2</td><td>4192965</td><td>156296384</td><td>152103420</td><td>Extended</td></tr>
<tr><td>/dev/sda5</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sda6</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sda7</td><td>10490508</td><td>12594959</td><td>1052226</td><td>Ext2</td></tr>
<tr><td>/dev/sda8</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/dev/sda9</td><td>14699538</td><td>18892439</td><td>4192902</td><td>HPFS/NTFS</td></tr>
<tr><td>/dev/sda10</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
MD5 verification hash: f7c2c38630b0c995732a87cce003dcca
SHA1 verification hash: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed
Bytes per Sector: 512
Sector Count: 2,104,452
Image Type: SMART ew-compressed
Acquired on OS: Windows 200x
Acquired using: ADI2.9.0.13
Acquire date: 8/10/2010 3:37:58 PM</td></tr>
</table>

	System date: 8/10/2010 3:37:58 PM Source data size: 1027 MB Sector count: 2104452 MD5 checksum: f7c2c38630b0c995732a87cce003dcca SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed Acquisition started: Wed Aug 11 03:51:17 2010 Acquisition finished: Wed Aug 11 03:51:44 2010 Segment list: G:\new\Test005-AltFor-FTK\Test005-FTK-SmartToE01.E01 Verification started: Wed Aug 11 03:51:44 2010 Verification finished: Wed Aug 11 03:52:03 2010 MD5 checksum: f7c2c38630b0c995732a87cce003dcca : verified SHA1 checksum: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed : verified
Results by assertion:	AFR-03 PASSED ALOG-01 PASSED AFR-09 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes and the hash of the original Smart image.

1.26 TC-12-01 Partially Hidden by HPA

Test Case TC-12-01 Partially Hidden by HPA (FTK Imager 2.9.0.1385)		
Test & Case Summary:	Acquire a partition that is partially or completely hidden by HPA or DCO **Notes**: FAT32 partition has been partially hidden by HPA from 150301488 to 156301487.	
Assertion:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-06	The tool acquires all the hidden data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start

	sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported **AHS-01** The tool reports to the user if any hidden sectors are found **AHS-02** The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment **AHS-03** The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: N/A
Drive Setup:	Source hashes MD5 checksum: 554357b44e0334f254e80ab537a299c7 SHA1 checksum: aa314705b7addb0bf230974b30967fa74082f490 /dev/sdb: current max LBA: 150,301,484 /dev/sdb: native max LBA: 150,301,484 /dev/sdb: physical max LBA: **156,301,488** /dev/sdb: **HPA set from sector 150,301,488 to 156,301,487 (Total 5,999,999 sectors)**

Partition Table:

Device	Start	End	#sectors	File System
/dev/sdb1	63	2104514	2104452	NTFS
/dev/sdb2	2104515	149565149	145460535	Ext3
/dev/sdb3	149565150	156296384	6731235	FAT32 **(Partially HPA)**

Log highlights:

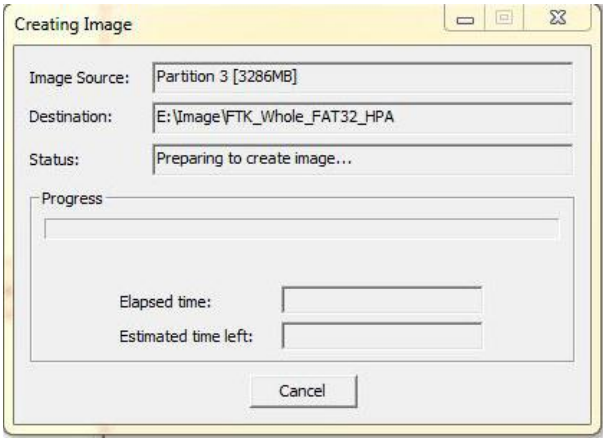
```
NOTICE: Imaging failed with the following error:
block index out of bounds
This image is incomplete!

Created By AccessData® FTK® Imager 2.9.0.1385 100406
Case Information:
Case Number: FAT32 Partition partically hidden
Evidence Number:
Unique Description:
Examiner: James Liang
Notes:
--------------------------------------------------------------
Information for E:\Image\FAT32_Part_Hidden:
Physical Evidentiary Item (Source) Information:
[Partition Information]
 Starting Sector: 149,565,150
 Sector Count: 6,731,235
 Source data size: 3286 MB
 Sector count:    6731235
[Computed Hashes]
 MD5 checksum:    397a300fac799fd8c78bd5951c1a626e
 SHA1 checksum:   3c91b102f596f0e29bf63ccb007996c80d484a7c
Image Information:
```

	Acquisition started: Tue Aug 31 23:11:04 2010 Acquisition finished: Tue Aug 31 23:11:14 2010
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 **FAILED** AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. FTK detects the partition information correctly. However, FTK reports the block index out of bounds instead of the partition is partially hidden.

1.27 TC-12-02 Completely Hidden by HPA

Test Case TC-12-02 Completely Hidden by HPA (FTK Imager 2.9.0.1385)		
Test & Case Summary:	Acquire a partition that is partially or completely hidden by HPA or DCO **Notes**: FAT32 partition has been completely hidden by HPA from 149565150 to 156301487.	
Assertion:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-06	The tool acquires all the hidden data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
	AHS-01	The tool reports to the user if any hidden sectors are found
	AHS-02	The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

<table>
<tr><td></td><td>AHS-03 The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td>/dev/sdb: current max LBA: 149,565,150
/dev/sdb: native max LBA: 149,565,150
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA set from sector 149,565,150 to 156,301,487 (Total 6,736,337 sectors)</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>2104514</td><td>2104452</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>2104515</td><td>149565149</td><td>145460535</td><td>Ext3</td></tr>
<tr><td>/dev/sdb3</td><td>149565150</td><td>156296384</td><td>6731234</td><td>FAT32 (Entire HPA)</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>


Creating Image

Image Source: Partition 3 [3286MB]

Destination: E:\Image\FTK_Whole_FAT32_HPA

Status: Preparing to create image...

Elapsed time:

Estimated time left:

</td></tr>
<tr><td>Results by assertion:</td><td>AFR-01 PASSED
AFR-02 PASSED
AFR-03 PASSED
AFR-04 FAILED
AFR-05 FAILED
AFR-06 FAILED
AFR-07 FAILED
AIC-01 FAILED
AIC-02 FAILED
AIC-05 FAILED
AIC-06 FAILED
AIC-07 FAILED
AIC-08 FAILED
AHS-01 FAILED
AHS-02 FAILED
AHS-03 FAILED
ALOG-01 FAILED
ALOG-02 FAILED
ALOG-03 FAILED</td></tr>
<tr><td>Analysis:</td><td>Test FAILED to achieve the expected Result. FTK Imager is able to detect the partition information correctly. However, FTK Imager freezes at the preparing to create image.</td></tr>
</table>

1.28 TC-13 Overlapping Partitions

<table>
<tr><th colspan="2">Test Case TC-13 Overlapping Partitions (FTK Imager 2.9.0.1385)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a partition that is overlapping with another partition
Notes: Partitions are overlapped. The last NTFS partition started before the end of the last partition. Starting sector changed from 79,168,320 to 79,100,000.</td></tr>
<tr><td>Assertions:</td><td>
<table>
<tr><td>AFR-01</td><td>The tool accesses the digital source with a supported access interface</td></tr>
<tr><td>AFR-02</td><td>The tool acquires a digital source</td></tr>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-04</td><td>The tool creates an image file of the digital source</td></tr>
<tr><td>AFR-05</td><td>The tool acquires all the visible data sectors from the digital source</td></tr>
<tr><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-01</td><td>The data represented by an image file is the same as the data acquired by the tool</td></tr>
<tr><td>AIC-02</td><td>The tool creates an image file according to the file format the user specified.</td></tr>
<tr><td>AIC-11</td><td>The tool reports to the user if any irregularities found in the digital source.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table>
</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source Hashes:
md5: 3170cec7e6720af973cc37a946c32ae3
sha1: 6366ad8cd563c05f086dfe7b7884b08fd9795069
/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>20980764</td><td>20980827</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>20980890</td><td>79168320</td><td>58187430</td><td>Ext3</td></tr>
<tr><td>/dev/sdb3</td><td>79100000</td><td>156296385</td><td>77128065</td><td>NTFS (Modified)</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By AccessData® FTK® Imager 2.9.0.1385 100406
Case Number: TC-OverlappingPartition-FTK
Examiner: James Liang
 [Drive Geometry]
 Cylinders: 9,729
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 156,301,488
[Physical Drive Information]
 Drive Model: ST380817 AS USB Device
 Drive Serial Number: 5MR18V18
 Drive Interface Type: USB</td></tr>
</table>

```
 Source data size: 76319 MB
 Sector count:    156301488
[Computed Hashes]
 MD5 checksum:    3170cec7e6720af973cc37a946c32ae3
 SHA1 checksum:   6366ad8cd563c05f086dfe7b7884b08fd9795069

Image Information:
 Acquisition started:   Wed Sep 08 13:08:19 2010
 Acquisition finished:  Wed Sep 08 14:24:42 2010
 Segment list:
  E:\Image\FTK-OverlapPartition.001
  E:\Image\FTK-OverlapPartition.002
  ………………..
  E:\Image\FTK-OverlapPartition.051
Image Verification Results:
 Verification started:  Wed Sep 08 14:24:42 2010
 Verification finished: Wed Sep 08 14:42:36 2010
 MD5 checksum:    3170cec7e6720af973cc37a946c32ae3 : verified
 SHA1 checksum:   6366ad8cd563c05f086dfe7b7884b08fd9795069 :
verified
```

Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-02 PASSED AFR-03 PASSED AIC-11 **FAILED** AFR-04 PASSED ALOG-01 PASSED AFR-05 PASSED ALOG-02 PASSED AFR-07 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. FTK Imager is able to recover the overlapped partition table. However, irregularity of the partition table is not reported to the user.

1.29 TC-14 Partition out of boundary

Test Case TC-14 Partition out of boundary (FTK Imager 2.9.0.1385)		
Test & Case Summary:	Acquire a hard disk with a partition's end address ended outside the physical boundary **Notes**: Partitions ended out of the physical boundary of the disk. The last partition end sector **changed from 72,331,264 to 72,380,000**.	
Assertions:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-11	The tool reports to the user if any irregularities found in the digital source.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-	The tool display correct information about the acquisition to the user. The

	02 information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA and DCO are not set

Partition Table:

Device	**Start**	**End**	**#sectors**	**File System**
/dev/sdb1	2048	40962047	40960000	NTFS
/dev/sdb2	40962048	83970047	43008000	Ext4
/dev/sdb3	83972096	**156350047**	72377951	Extended **(Modified)**

Log highlights:

```
Created By AccessData® FTK® Imager 2.9.0.1385 100406
Case Number: FTK-OutOfBoundaryPartition
Examiner: James Liang
 [Drive Geometry]
 Cylinders: 9,729
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 156,301,488
[Physical Drive Information]
 Drive Model: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
 Drive Serial Number: 02cc0e0010903500
 Drive Interface Type: 1394
 Source data size: 76319 MB
 Sector count:    156301488
[Computed Hashes]
 MD5 checksum:    b42f526d394078656308a9b96aa77188
 SHA1 checksum:   e2977a0cd2d2608519b1750e980252d01cdb4718
Image Information:
 Acquisition started:   Fri Sep 10 02:02:27 2010
 Acquisition finished:  Fri Sep 10 02:56:06 2010
 Segment list:
  E:\Image\FTK-OutOfBoundaryPartition.001
  E:\Image\FTK-OutOfBoundaryPartition.002
  …………………….
  E:\Image\FTK-OutOfBoundaryPartition.051
Image Verification Results:
 Verification started:  Fri Sep 10 02:56:11 2010
 Verification finished: Fri Sep 10 03:42:24 2010
 MD5 checksum:    b42f526d394078656308a9b96aa77188 : verified
 SHA1 checksum:   e2977a0cd2d2608519b1750e980252d01cdb4718 :
```

	verified
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-11 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. All the data are acquired correctly but FTK Imager failed to report to the user that irregularities in the digital source.

1.30 TC-15 Unreadable MBR

Test Case TC-15 Unreadable MBR (FTK Imager 2.9.0.1385)		
Test & Case Summary:	Acquire a hard disk with an unreadable MBR **Notes**: Partitions ended out of the physical boundary of the disk. Data of MBR is replaced by value 0.	
Assertions:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AFR-08	The tool reports to the user of the error type and the location of the error if error occurred during the reading from a digital source.
	AFR-09	If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-03	The tool reports to the user if an error occurs during the image creation process.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	AIC-11	The tool reports to the user if any irregularities found in the digital source.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18	

	Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA and DCO are not set
Partition Table:	**Device** **Start** **End** **#sectors** **File System** /dev/sdb1 2048 40962047 40960000 NTFS /dev/sdb2 40962048 83970047 43008000 Ext4 /dev/sdb3 83972096 156301311 72329125 Extended
Log highlights:	Created By AccessData® FTK® Imager 2.9.0.1385 100406 Case Number: Test015 - Unreadable MBR [Drive Geometry] Cylinders: 9,729 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 156,301,488 [Physical Drive Information] Drive Model: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device Drive Serial Number: 02cc0e0010903500 Drive Interface Type: 1394 Source data size: 76319 MB Sector count: 156301488 [Computed Hashes] MD5 checksum: 2ab63e47f402406afed31dad063df7f8 SHA1 checksum: d337f09ba2b9069668c70a14a2fc87a3b21a5887 Image Information: Acquisition started: Sun Sep 12 07:15:35 2010 Acquisition finished: Sun Sep 12 08:11:10 2010 Segment list: E:\Image\T015-unreadableMBR.001 E:\Image\T015-unreadableMBR.002 ………………………….. E:\Image\T015-unreadableMBR.051 Image Verification Results: Verification started: Sun Sep 12 08:11:12 2010 Verification finished: Sun Sep 12 08:36:30 2010 MD5 checksum: 2ab63e47f402406afed31dad063df7f8 : verified SHA1 checksum: d337f09ba2b9069668c70a14a2fc87a3b21a5887 : verified
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AFR-08 PASSED AFR-09 PASSED AIC-01 PASSED AIC-02 PASSED AIC-03 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AIC-11 **FAILED** ALOG-01 PASSED ALOG-02 **FAILED** ALOG-03 PASSED

Analysis:	Test **FAILED** to achieve the expected Result. FTK Imager is not able to recognise the partition table existed in the device. The entire device is recognised as unallocated space.

1.31 TC-16-01 Acquire a Single GUID Partition

<table>
<tr><th colspan="2">Test Case TC-16-01 Acquire a Single GUID Partition (FTK Imager 2.9.0.1385)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a Single GUID Partition
Notes: Hard drive partitioned as GPT disk. 6 partitions are created.</td></tr>
<tr><td>Assertions:</td><td><table>
<tr><td>AFR-01</td><td>The tool accesses the digital source with a supported access interface</td></tr>
<tr><td>AFR-02</td><td>The tool acquires a digital source</td></tr>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-04</td><td>The tool creates an image file of the digital source</td></tr>
<tr><td>AFR-05</td><td>The tool acquires all the visible data sectors from the digital source</td></tr>
<tr><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-01</td><td>The data represented by an image file is the same as the data acquired by the tool</td></tr>
<tr><td>AIC-02</td><td>The tool creates an image file according to the file format the user specified.</td></tr>
<tr><td>AIC-05</td><td>If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller</td></tr>
<tr><td>AIC-06</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.</td></tr>
<tr><td>AIC-07</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.</td></tr>
<tr><td>AIC-08</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table></td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set</td></tr>
<tr><td>Partition Table (GPT disk):</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>34</td><td>262110</td><td>262144</td><td>Microsoft Reserved</td></tr>
<tr><td>/dev/sdb2</td><td>264192</td><td>8652799</td><td>8388608</td><td>NTFS</td></tr>
<tr><td>/dev/sdb3</td><td>8652800</td><td>12847103</td><td>4194304</td><td>NTFS</td></tr>
<tr><td>/dev/sdb4</td><td>12847104</td><td>14944255</td><td>2097152</td><td>NTFS</td></tr>
<tr><td>/dev/sdb5</td><td>14944256</td><td>25380863</td><td>10436608</td><td>NTFS</td></tr>
<tr><td>/dev//sdb6</td><td>25380864</td><td>156299264</td><td>130918400</td><td>NTFS</td></tr>
</table></td></tr>
</table>

FTK Imager 2.9.0.1385 (Release Date: 8th, Apr 2010)

Log highlights:

```
Created By AccessData® FTK® Imager 2.9.0.1385 100406
Case Number: Test18-GUIDPartition
Examiner: James Liang
 [Partition Information]
 Starting Sector: 12,847,104
 Sector Count: 2,097,152
[GUID Partition Table Information]
 Partition Type GUID: {EBD0A0A2-B9E5-4433-87C0-68B6B72699C7}
 Unique Partition GUID: {9D8702A4-FDFA-475B-A90D-40105F558FD8}
 Source data size: 1024 MB
 Sector count:    2097152
[Computed Hashes]
 MD5 checksum:    68fd8aa6e64b5f7fb7cd02e5444f14a1
 SHA1 checksum:   249dcfa032899d4f1a04c37c7c4621b3b05cebac
Image Information:
 Acquisition started:   Wed Sep 15 00:03:01 2010
 Acquisition finished:  Wed Sep 15 00:03:43 2010
 Segment list:
  E:\Image\Test018-SingleGUIDPartition.001
Image Verification Results:
 Verification started:  Wed Sep 15 00:03:43 2010
 Verification finished: Wed Sep 15 00:03:49 2010
 MD5 checksum:    68fd8aa6e64b5f7fb7cd02e5444f14a1 : verified
 SHA1 checksum:   249dcfa032899d4f1a04c37c7c4621b3b05cebac :
verified
```

Results by assertion:

AFR-01 PASSED	AIC-01 PASSED	ALOG-01 PASSED
AFR-02 PASSED	AIC-02 PASSED	ALOG-02 PASSED
AFR-03 PASSED	AIC-05 PASSED	ALOG-03 PASSED
AFR-04 PASSED	AIC-06 PASSED	
AFR-05 PASSED	AIC-07 PASSED	
AFR-07 PASSED	AIC-08 PASSED	

Analysis: Test **achieved** expected result.

1.32 TC-17 Acquire a partially hidden GPT Partition

<table>
<tr><th colspan="2">Test Case TC-16-01 Acquire a Single GUID Partition (FTK Imager 2.9.0.1385)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a GPT partition that is partially hidden by HPA
Note: Total visible sectors are 202,400.</td></tr>
<tr><td>Assertions:</td><td><table>
<tr><td>AFR-01</td><td>The tool accesses the digital source with a supported access interface</td></tr>
<tr><td>AFR-02</td><td>The tool acquires a digital source</td></tr>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-04</td><td>The tool creates an image file of the digital source</td></tr>
<tr><td>AFR-05</td><td>The tool acquires all the visible data sectors from the digital source</td></tr>
<tr><td>AFR-06</td><td>The tool acquires all the hidden data sectors from the digital source</td></tr>
<tr><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-01</td><td>The data represented by an image file is the same as the data acquired by the tool</td></tr>
<tr><td>AIC-02</td><td>The tool creates an image file according to the file format the user specified.</td></tr>
<tr><td>AIC-05</td><td>If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller</td></tr>
<tr><td>AIC-06</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.</td></tr>
<tr><td>AIC-07</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.</td></tr>
<tr><td>AIC-08</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>AHS-01</td><td>The tool reports to the user if any hidden sectors are found</td></tr>
<tr><td>AHS-02</td><td>The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment</td></tr>
<tr><td>AHS-03</td><td>The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment</td></tr>
</table></td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td>/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA set from sector 6,500,001 to 156,301,487 (Total 149,801,488 sectors are hidden)</td></tr>
<tr><td>Partition Table (GPT disk):</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>2048</td><td>4198399</td><td>4196352</td><td>FAT32</td></tr>
<tr><td>/dev/sdb2</td><td>4198400</td><td>6297599</td><td>2099200</td><td>Ext4</td></tr>
<tr><td>/dev/sdb3</td><td>6297600</td><td>156301311</td><td>150003712</td><td>NTFS (Partially HPA)</td></tr>
</table></td></tr>
</table>

Log highlights:	NOTICE: Imaging failed with the following error: block index out of bounds This image is incomplete! Created By AccessData® FTK® Imager 2.9.0.1385 100406 Starting Sector: 6,297,600 Sector Count: 150,003,712 Partition Type GUID: {E3C9E316-0B5C-4DB8-817D-F92DF00215AE} Unique Partition GUID: {2B66B4BF-B0B0-422A-8A60-FDF827AD7F6E} Source data size: 73244 MB Sector count: 150003712 MD5 checksum: a35d434616ed81bc96c4375d0bea1173 SHA1 checksum: a9930a3edb00db9cb066f2c70616d73c77350909 Acquisition started: Mon Oct 18 17:54:46 2010 Acquisition finished: Mon Oct 18 17:54:49 2010 Segment list: E:\Image\FTK_partGPThpa_acquire.001
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. FTK detected the partition information correctly. However, FTK reported the block index out of bounds instead of the partition was partially hidden. The error encountered is same as the test case TC-12-01.

Test Results – Helix 3 Pro

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

2.1. TC-01-FW

Test Case TC-01-FW (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-01 Acquire a hard drive using Access Interface (AI) and convert to an image file
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	Source hashes MD5 checksum: 436a043c1766f46f3945e605144f22eb SHA1 checksum: 82d4b6226995d11b82979db901e809a06b1574e8 /dev/sda: current max LBA: 156,296,385 /dev/sda: native max LBA: 156,296,385 /dev/sda: physical max LBA: 156,296,385 /dev/sda: HPA not set /dev/sda: DCO not set
Log highlights:	Created By Helix3 Pro 2009R3 DISK INFORMATION physical True size 80023749120 name PhysicalDrive3 mount PhysicalDrive3 Serial number 3.AA SystemAS

	Firmware ST380811 Type Fixed hard disk WholeDisk True ACQUISITION INFORMATION Acquire Format: RAW Acquisition Start: 2010-06-27 20:31:16 Acquisition Stop 2010-06-27 21:46:44 Output File(s): E:\helix\Images\Image.001 E:\helix\Images\Image.002 ………… E:\helix\Images\Image.038 Verification: Passed Hash(es): MD5: 436a043c1766f46f3945e605144f22eb SHA1: 82d4b6226995d11b82979db901e809a06b1574e8
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 **FAILED** AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. The acquired start and end sectors were not displayed and reported to the user.

2.2. TC-01-USB

Test Case TC-01-USB (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-01 Acquire a hard drive using Access Interface (AI) and convert to an image file
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to

	the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: USB 2.0 Drive (4GB) Serial Number: N/A Sector count: 7,987,200 Write blocker: Tableau T8 Forensic USB Bridge
Drive Setup:	Source hashes MD5: fcf954774adec1eefb4b873b3c8f3612 SHA1: 033772e928aea0c52827574cfb2c7f020062aa84 /dev/sda: current max LBA: 7,987,200 /dev/sda: native max LBA: 7,987,200 /dev/sda: physical max LBA: 7,987,200 /dev/sda: HPA not set /dev/sda: DCO not set
Log highlights:	Created By Helix3 Pro 2009R3 OS Name Windows XP OS Patch Service Pack 3 Computer Name JAMES-212DFE2EF Administrator True size 4087964160 name PhysicalDrive1 serialnumber 1100 system Flash Disk firmware USB2.0 WholeDisk True Acquire Format: RAW Acquisition Start: 2010-09-21 08:13:58 Acquisition Stop 2010-09-21 08:27:52 Output File(s): G:\Image\Helix-TC01-USB-WHOLE.001 G:\Image\Helix-TC01-USB-WHOLE.002 Verification: Passed Hash(es): MD5: fcf954774adec1eefb4b873b3c8f3612 SHA1: 033772e928aea0c52827574cfb2c7f020062aa84
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 **FAILED** AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. The acquired start and end sectors were not displayed and reported to the user.

2.3. TC-02-NTFS

Test Case TC-02-NTFS (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire NTFS partition only. Sector start from 63 to 4192964. Total sector:4192902
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	Source hashes MD5: 93d88289dc48d350cf1b979c92897715 SHA1: 8a6172e0ff6b103ce0436d36ffeb274f7f075edb /dev/sdb: current max LBA: 156,296,385 /dev/sdb: native max LBA: 156,296,385 /dev/sdb: physical max LBA: 156,296,385 /dev/sdb: HPA not set /dev/sdb: DCO not set
Partition Table:	see below

Partition Table:

Device	**Start**	**End**	**#sectors**	**System**
/dev/sdb1	63	4192964	4192902	NTFS
/dev/sdb2	4193028	6297479	2104452	FAT32
/dev/sdb3	6297543	10490444	4192902	FAT16
/dev/sdb4	10490508	12594959	2104452	Ext2
/dev/sdb5	12595023	14699474	2104452	Ext3
/deb/sdb6	18892503	19149479	256977	Swap

Log highlights:	Created By Helix3 Pro 2009 R3 **DISK INFORMATION** description Windows NTFS volume logicalname /dev/sdb1 dev 8d:17d serial 7f7e5bd2-2f6c-43b4-b380-ea7d4f66fda8 size 2146733056 capacity 2146765824 clustersize 4096 created 2010-07-26 17:27:33 filesystem ntfs **ACQUISITION INFORMATION** Acquire Format: RAW Acquisition Start: 2010-07-26 18:30:19 Acquisition Stop 2010-07-26 18:32:44 Output File(s): /mnt/new/Image/Test002-Helix-NTFS.001 Verification: Passed Hash(es): MD5: 93d88289dc48d350cf1b979c92897715 SHA1: 8a6172e0ff6b103ce0436d36ffeb274f7f075edb SHA256: 9b51174ce46c814d3540b8e520c3149e0ce6c2c4e0434cbab3fdd467f0b42e7e SHA512: 03bb311ac5dfbbdb60631f863cd33066c074c9a200125eba5ff0347cdd4cd289 48ebf398a7ae708d4052b2fa3dc6b4c2a30f0d96e5b81bf774d658dad31442bd
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 **FAILED** AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. The acquired start and end sectors were not displayed and reported to the user.

2.4. TC-02-Ext2

Test Case TC-02-Ext2 (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire Ext2 only partition in a multi-partitioned HD using Helix Live CD. WriteBlocker is not used. Sector size from:10490508 to 12594959 total sector: 2104452
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment

<table>
<tr><td></td><td>AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5: df377203665cf28c0db52707aa6f71d5
SHA1: 4194cfb81f69ad412cd0cc3806f81daa37102d73
/dev/sdb: current max LBA: 156,296,385
/dev/sdb: native max LBA: 156,296,385
/dev/sdb: physical max LBA: 156,296,385
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>4192964</td><td>4192902</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sdb3</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sdb4</td><td>10490508</td><td>12594959</td><td>2104452</td><td>Ext2</td></tr>
<tr><td>/dev/sdb5</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Created By Helix3 Pro 2009R3
logicalname /dev/sdb4
dev 8d:23d
capacity 1077479424
WholeDisk False
VendorName Unknown

ACQUISITION INFORMATION
Acquire Format: RAW
Acquisition Start: 2010-07-26 18:50:08
Acquisition Stop 2010-07-26 18:51:05
Output File(s):</td></tr>
</table>

	/mnt/new/Image/Test002-Helix-Ext2.001 Verification: Passed Hash(es): MD5: df377203665cf28c0db52707aa6f71d5 SHA1: 4194cfb81f69ad412cd0cc3806f81daa37102d73 SHA256: 10dd1c0221d60a0047a67c20652a888f793af42b8a8d4421ca34497e2f9ec44f SHA512: d0bfd1fd3532b0e962d34de6cf46248bd9b8a5f8acdc7db887b9f66c0e02c3dc 23d5feafe20cf1670111871725e9f6fb8d146e6dfb90050d97ea1c8da52b573c
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 **FAILED** AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. The acquired start and end sectors were not displayed and reported to the user.

2.5. TC-02-Ext3

Test Case TC-02-Ext3 (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire Ext3 only partition in a multi-partitioned HD using Helix Live CD. WriteBlocker not used Sector start from: 12595023 to 14699474 total sector: 2104452
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source	Drive Model: ST380811 AS (80GB)

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

Device:	Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: N/A
Drive Setup:	Source hashes MD5: f7c2c38630b0c995732a87cce003dcca SHA1: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed /dev/sda: current max LBA: 156,296,385 /dev/sda: native max LBA: 156,296,385 /dev/sda: physical max LBA: 156,296,385 /dev/sda: HPA not set /dev/sda: DCO not set
Partition Table:	**Device** **Start** **End** **#sectors** **System** /dev/sdb1 63 4192964 4192902 NTFS /dev/sdb2 4193028 6297479 2104452 FAT32 /dev/sdb3 6297543 10490444 4192902 FAT16 /dev/sdb4 10490508 12594959 2104452 Ext2 /dev/sdb5 12595023 14699474 2104452 Ext3 /deb/sdb6 18892503 19149479 256977 Swap unallocated 19149480 156296384 137146905 Empty
Log highlights:	Created By Helix3 Pro 2009R3 DISK INFORMATION description Linux filesystem partition physid 5 logicalname /dev/sdb5 dev 8d:24d capacity 1077479424 WholeDisk False VendorName Unknown ACQUISITION INFORMATION Acquire Format: RAW Acquisition Start: 2010-07-26 18:52:41 Acquisition Stop 2010-07-26 18:53:38 Output File(s): /mnt/new/Image/Test002-Helix-Ext3.001 Verification: Passed Hash(es): MD5: f7c2c38630b0c995732a87cce003dcca SHA1: 2043d334ef1ee9c1749427b249b3c983d4fcc8ed SHA256: fe0a39c37c73c774d3f4a1f5ab0cb4c089ed38ceb99b3212910911d40a79fd50 SHA512: 87f6ca5c98f36f86e078d926c719d4519ecca5ea86712250341ef92d1a86db56 badc0dc4f70c3cd51d60678a55327672aa495454747da25ad3ea035b3173eb0 2
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED

	AFR-04 PASSED ALOG-02 **FAILED** AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. The acquired start and end sectors were not displayed and reported to the user.

2.6. TC-02-FAT16

Test Case TC-02-FAT16 (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire FAT16 only partition in a multi-partitioned HD using Helix Live CD. WriteBlocker not used Sector start from:6297543 to 10490444 total sector: 4192902
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: N/A
Drive Setup:	Source hashes MD5: cbf8f802e41c7ddbfb0afeaa5c7d0de0 SHA1: fa59e48af260bcd9e874286b0e1026f03b461220 /dev/sda: current max LBA: 156,296,385 /dev/sda: native max LBA: 156,296,385 /dev/sda: physical max LBA: 156,296,385 /dev/sda: HPA not set /dev/sda: DCO not set

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

<table>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>4192964</td><td>4192902</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sdb3</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sdb4</td><td>10490508</td><td>12594959</td><td>2104452</td><td>Ext2</td></tr>
<tr><td>/dev/sdb5</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By Helix3 Pro 2009R3
description FAT16 partition
physid 3
logicalname /dev/sdb3
dev 8d:22d
capacity 2146765824
WholeDisk False
VendorName Unknown
Acquire Format: RAW
Acquisition Start: 2010-07-26 18:44:46
Acquisition Stop 2010-07-26 18:47:08
Output File(s):
/mnt/new/Image/Test002-Helix-Fat16.001
Verification: Passed
MD5: cbf8f802e41c7ddbfb0afeaa5c7d0de0
SHA1: fa59e48af260bcd9e874286b0e1026f03b461220
SHA256:
75e7d8ea495b7b7d83580d9293e50bc993e911be02de92449a9310817e55055c
SHA512:
3bb07ba36cf8a5cde912f9c18d20be7746a656519b999c793d3ee2e68cb07db74fbb220e8bb0956c297fb98349e0c3808dc53379760dde94ef32ab64475b2cef</td></tr>
<tr><td>Results by assertion:</td><td>AFR-01 PASSED
AFR-02 PASSED
AFR-03 PASSED
AFR-04 PASSED
AFR-05 PASSED
AFR-07 PASSED
AIC-01 PASSED
AIC-05 PASSED
ALOG-01 PASSED
ALOG-02 FAILED
ALOG-03 PASSED</td></tr>
<tr><td>Analysis:</td><td>Test FAILED to achieve the expected Result. The acquired start and end sectors were not displayed and reported to the user.</td></tr>
</table>

2.7. TC-02-FAT32

<table>
<tr><th colspan="2">Test Case TC-02-FAT32 (Helix3 Pro 2009 R3)</th></tr>
<tr><td>Test & Case Summary:</td><td>TC-02 Acquire a digital source that supported by the tools to an image file

Notes: Acquire FAT32 only partition in a multi-partitioned HD using Helix Live CD. WriteBlocker not used
Sector starts from:4193028 to 6297479
total sector: 2104452</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5: 2c22fded78dc8ccc2c935944883a2e1b
SHA1: 10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5
/dev/sdb: current max LBA: 156,296,385
/dev/sdb: native max LBA: 156,296,385
/dev/sdb: physical max LBA: 156,296,385
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>4192964</td><td>4192902</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sdb3</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sdb4</td><td>10490508</td><td>12594959</td><td>2104452</td><td>Ext2</td></tr>
<tr><td>/dev/sdb5</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
</table>

Log highlights:

```
Created By Helix3 Pro 2009R3

DISK INFORMATION
description     W95 FAT32 partition
physid 2
logicalname     /dev/sdb2
dev     8d:21d
capacity        1077479424
WholeDisk       False
VendorName      Unknown

ACQUISITION INFORMATION
Acquire Format: RAW
Acquisition Start:      2010-07-26 18:41:31
Acquisition Stop        2010-07-26 18:42:28
Output File(s):
/mnt/new/Image/Test002-Helix-Fat32.001
Verification:   Passed
Hash(es):
MD5: 2c22fded78dc8ccc2c935944883a2e1b
SHA1: 10eaa99a609cd8d215c9dc5a68f46e2e0d5c68c5
SHA256:
887f563613a73452422fc12a38af8dbb36103cdf203c9f9cadc06640eb4ac3f4
SHA512:
55421eee58abd277f4df93561d85aa88cb3f5f4fc157fe507f4ccddc4815f9ce35ec1e4b8422df73dc28553f96208d2f3a34535dca9cb9034b3a6ded4f8092dd
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED	AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 **FAILED** ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. The acquired start and end sectors were not displayed and reported to the user.	

2.8. TC-02-SWAP

Test Case TC-02-SWAP (Helix3 Pro 2009 R3)		
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire Swap partition only in a multi-partitioned HD using Helix Live CD. WriteBlocker not used Sector start from 18892503 to 19149479 Total sector: 256977	
Assertion:	AFR-01	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment

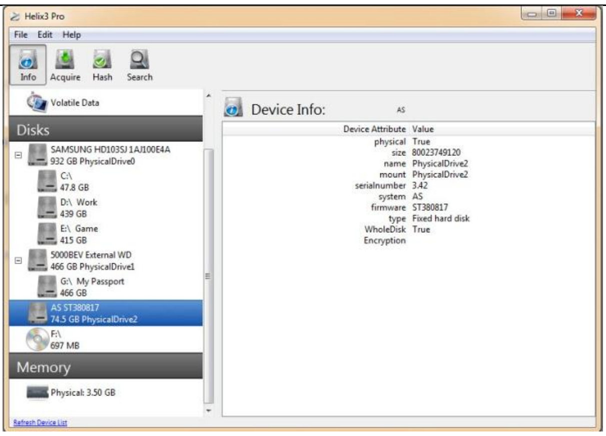
<table>
<tr><td></td><td>AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5: d7465eb87f553639e35c177775561e77
SHA1: ddd3a59446ce3fe46582f505a37a4e77f52caca2

/dev/sdb: current max LBA: 156,296,385
/dev/sdb: native max LBA: 156,296,385
/dev/sdb: physical max LBA: 156,296,385
/dev/sdb: HPA not set
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>4192964</td><td>4192902</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sdb3</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sdb4</td><td>10490508</td><td>12594959</td><td>2104452</td><td>Ext2</td></tr>
<tr><td>/dev/sdb5</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By Helix3 Pro 2009R3
description Linux swap / Solaris partition
physid 6
logicalname /dev/sdb6
dev 8d:26d
capacity 131572224
nofs No filesystem
WholeDisk False
VendorName Unknown
Acquire Format: RAW
Acquisition Start: 2010-07-26 18:57:35</td></tr>
</table>

	Acquisition Stop 2010-07-26 18:57:44 Output File(s): /mnt/new/Image/Test002-Helix-Swap.001 Verification: Passed Hash(es): MD5: d7465eb87f553639e35c177775561e77 SHA1: ddd3a59446ce3fe46582f505a37a4e77f52caca2 SHA256: bfbdf4db1d346ef8ef1ffb3fe17e40ce9965adaf3a0f057b08ac13b11490b1d7 SHA512: d14ba77e3d31c558daf544b18d45ecebbaff6081a4ef59e9945c452b4b84181941641b62784b356017a6c957909548cb11ca7cf1838c2ffceb2fee4d0f35dbe1
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 **FAILED** AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. The acquired start and end sectors were not displayed and reported to the user.

2.9. TC-02-HFS & HFS+

Test Case TC-02-HFS & HFS+ (Helix3 Pro 2009 R3)		
Test & Case Summary:	TC-02 Acquire a digital source that supported by the tools to an image file Notes: Acquire HFS and HFS+ partition only in a multi-partitioned HD using Helix Live CD.	
Assertion:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user.
	ALOG-03	The tool display correct information regarding to the the acquisition to the user and the information displayed is

	consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: N/A
Drive Setup:	Source hashes MD5: d8235a6c57ddf91c902d42f0e39cb7d5 SHA1: b91e9115388276b961e6a94a6322337048734d6c /dev/sdb: current max LBA: 156,296,385 /dev/sdb: native max LBA: 156,296,385 /dev/sdb: physical max LBA: 156,296,385 /dev/sdb: HPA not set /dev/sdb: DCO not set
Partition Table:	**Device** **Start** **End** **#sectors** **File System** **Size** **/dev/sdb1** **4096** **4198399** **4194304** **HFS** **2Gb** /dev/sdb2 4198400 14999551 10801152 HFS+ 5Gb Unallocated
Log highlights:	 Device Info: AS Device Attribute Value physical True size 80023749120 name PhysicalDrive2 mount PhysicalDrive2 serialnumber 3.42 system AS firmware ST380817 type Fixed hard disk WholeDisk True Encryption
Results by assertion:	AFR-01 PASSED AIC-01 N/A AFR-02 **FAILED** AIC-05 N/A AFR-03 PASSED ALOG-01 N/A AFR-04 **FAILED** ALOG-02 N/A AFR-05 N/A ALOG-03 N/A AFR-07 N/A
Analysis:	Test **FAILED** to achieve the expected Result. Helix 3 Pro cannot identify the HFS or HFS+ partitions

2.10. TC-03-HPA

Test Case TC-03-HPA (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-03 Acquire a hard drive with hidden sectors to an image file Notes: HPA actived
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-06** The tool acquires all the hidden data sectors from the digital source

<table>
<tr><td rowspan="13"></td><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-01</td><td>The data represented by an image file is the same as the data acquired by the tool</td></tr>
<tr><td>AIC-02</td><td>The tool creates an image file according to the file format the user specified.</td></tr>
<tr><td>AIC-05</td><td>If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller</td></tr>
<tr><td>AIC-06</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.</td></tr>
<tr><td>AIC-07</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.</td></tr>
<tr><td>AIC-08</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>AHS-01</td><td>The tool reports to the user if any hidden sectors are found</td></tr>
<tr><td>AHS-02</td><td>The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment</td></tr>
<tr><td>AHS-03</td><td>The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment</td></tr>
<tr><td>Source Device:</td><td colspan="2">Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td colspan="2">Source hashes
MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd
SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59
/dev/sdb: current max LBA: 94,863,827
/dev/sdb: native max LBA: 94,863,827
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA set from sector 94,863,828 to 156,301,487
/dev/sdb: DCO not set</td></tr>
<tr><td>Partition Table:</td><td colspan="2"><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>41945714</td><td>41945652</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>41945715</td><td>94863824</td><td>52918110</td><td>Ext3</td></tr>
<tr><td>/dev/sdb3</td><td>94863825</td><td>156296384</td><td>61432560</td><td>NTFS (HPA)</td></tr>
</table></td></tr>
</table>

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

Log highlights:	Created By Helix3 Pro 2009R3 physical True size 48570278400 name PhysicalDrive1 mount PhysicalDrive1 serialnumber 5MR18V18 system ST380817AS firmware 3.42 T type Fixed hard disk WholeDisk True Acquire Format: RAW Acquisition Start: 2010-07-22 15:17:43 Acquisition Stop 2010-07-22 16:15:43 Output File(s): E:\Image\Test003-HPA-Helix-ST380817AS.001 E:\Image\Test003-HPA-Helix-ST380817AS.002 ……………….................... E:\Image\Test003-HPA-Helix-ST380817AS.023 Verification: Passed MD5: 69fdef5d5de3a207bc2a04017c38c3fd SHA1: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 SHA256: 1169e7b9c33014c48a07a885c57fb16c7fc71f19e96b82d42a377730bc670973 SHA512: 1a1d137df8d5f15d9da8369f13ba2fa4ad4f0c166cce5e37ada65c71ab02826385d6b658010ebe61d2fae5713f4d150ebee382de6a09eb9aeeb4aa28723f85c7
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 **FAILED** ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. Helix3 Pro failed to detect and acquire the hidden areas in the hard drive.

2.11. TC-03-DCO

Test Case TC-03-DCO (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-03 Acquire a hard drive with hidden sectors to an image file Notes: DCO active
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-06** The tool acquires all the hidden data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported **AHS-01** The tool reports to the user if any hidden sectors are found **AHS-02** The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment **AHS-03** The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: N/A
Drive Setup:	**Source hashes:** MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 /dev/sdb: current max LBA: **94,863,828** /dev/sdb: native max LBA: 94,863,828 /dev/sdb: physical max LBA: **156,301,488** /dev/sdb: HPA not set /dev/sdb: **DCO set from sector 94,863,828 to 156,301,487**
Partition Table:	**Device** **Start** **End** **#sectors** **File System** /dev/sdb1 63 41945714 41945652 NTFS /dev/sdb2 41945715 94863824 52918110 Ext3

	/dev/sdb3 94863825 156296384 61432560 NTFS **(DCO)**
Log highlights:	Created By Helix3 Pro 2009R3 description ATA Disk product ST380817AS vendor Seagate physid 0 logicalname /dev/sdb dev 8d:16d version3.42 serial 5MR18V18 size 48572891136 ansiversion 5 signature 000ae8b9 partitioned Partitioned disk partitioned:dosMS-DOS partition table VendorName WholeDisk True Acquire Format: RAW Acquisition Start: 2010-07-26 04:22:45 Acquisition Stop 2010-07-26 05:17:26 Output File(s): /mnt/new/new/ImageHelix_DCO_Active.001 /mnt/new/new/ImageHelix_DCO_Active.002 …………………………. /mnt/new/new/ImageHelix_DCO_Active.023 Verification: Passed Hash(es): MD5: 69fdef5d5de3a207bc2a04017c38c3fd SHA1: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 SHA256: 1169e7b9c33014c48a07a885c57fb16c7fc71f19e96b82d42a377730bc670973 SHA512: 1a1d137df8d5f15d9da8369f13ba2fa4ad4f0c166cce5e37ada65c71ab02826385 d6b658010ebe61d2fae5713f4d150ebee382de6a09eb9aeeb4aa28723f85c7
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AHS-02 **FAILED** AFR-02 PASSED AIC-02 PASSED AHS-03 **FAILED** AFR-03 PASSED AIC-05 PASSED ALOG-01 PASSED AFR-04 PASSED AIC-06 PASSED ALOG-02 **FAILED** AFR-05 PASSED AIC-07 PASSED ALOG-03 PASSED AFR-06 **FAILED** AIC-08 PASSED AFR-07 PASSED AHS-01 **FAILED**
Analysis:	Test FAILED to achieve the expected Result. Helix3 Pro failed to detect and acquire the hidden areas in the hard drive.

2.12. TC-05-EnCase6

Test Case TC-05-EnCase 6 (Helix3 Pro 2009 R3)	
Test & Case Summary:	TC-05 Acquire a digital source to an image file in an alternate supported format Notes: Convert images from test002 Hard drive to Encase 6 format to see whether helix can output other type of images except dd.
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool. AIC-02 The tool creates an image file according to the file format the user specified. ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdc: current max LBA: 156,296,385 /dev/sdc: native max LBA: 156,296,385 /dev/sdc: physical max LBA: 156,296,385 /dev/sdc: HPA not set /dev/sdc: DCO not set

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

Log highlights:

```
Created By Helix3 Pro 2009R3
OS Name        Windows Vista
OS Mode        Workstation
OS Build       6.1.7600
OS Suite       Single User Terminal Services
Computer Name       JAMES-PC
Uptime0 Days -11 Hours -35 Minutes -37 Seconds
User Name      James
Administrator  True
NIC 1 - IP     192.168.1.4
NIC 1 - MAC    00:04:61:4E:44:BC
NIC 1 - Subnet      255.255.255.0
physical       True
size     80023749120
name     PhysicalDrive2
mount    PhysicalDrive2
serialnumber   3.AA
system AS
firmware       ST380811
type     Fixed hard disk
WholeDisk      True
Encryption
Acquire Format: EnCase 6
Acquiry started at: Sun Jul 11 01:15:04 2010
Acquiry completed at: Sun Jul 11 02:13:13 2010
Written: 74 GiB (80010543916 bytes) in 58 minute(s) and 9 second(s) with
21 MiB/s (22932228 bytes/second).
MD5 hash calculated over data:        21e01ccc3fd65c262c20cf6a0a771b60
SHA1 hash calculated over data:
         50a1965ec394d97f9db97fc4353da4cab87a67bc
```

Results by assertion:

AFR-01	PASSED	AIC-01	PASSED
AFR-02	PASSED	AIC-02	PASSED
AFR-03	PASSED	ALOG-01	**FAILED**
AFR-04	PASSED	ALOG-02	**FAILED**
AFR-05	PASSED	ALOG-03	PASSED
AFR-07	PASSED		

Analysis: Test result **FAILED**. Verification hashes are not calculated.

2.13. TC-06-UNC

Test Case TC-06-UNC (Helix3 Pro 2009 R3)	
Test & Case Summary:	Acquire a digital source that has at least one faulty data sector Notes: 15 UNC errors existed
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AFR-08** The tool report to the user of the error type and the location of the error if error occurred during the reading from a digital source. **AFR-09** If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-03** The tool reports to the user if an error occurs during the image creation process. **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdc: current max LBA: 156,296,385 /dev/sdc: native max LBA: 156,296,385 /dev/sdc: physical max LBA: 156,296,385 /dev/sdc: HPA not set /dev/sdc: DCO not set Following sectors are marked as faulty: 5161564, 12135645, 16429701, 28210195, 33486075, 40694940, 40828560, 57691700, 90179820, 91800252, 92763320, 104129017, 109477200, 118026966, 140386491

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

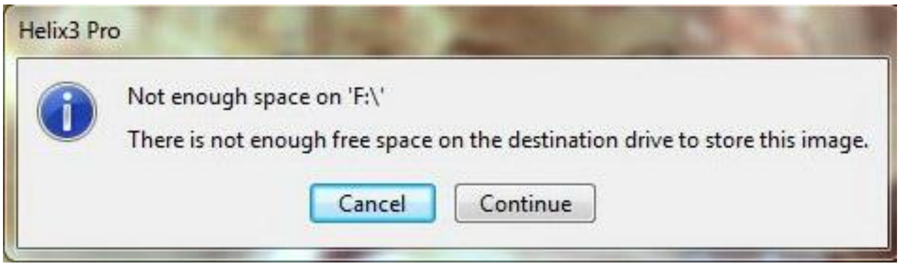
Log highlights:

```
Created By Helix3 Pro

DISK INFORMATION
description     ATA Disk
product         ST380811AS
vendor Seagate
physid 0
logicalname     /dev/sda
dev     8d:0d
version3.AA
serial  6PS2CA4Z
size    80026361856
ansiversion     5
WholeDisk       True
VendorName

ACQUISITION INFORMATION
Acquire Format: RAW
Acquisition Start:      2010-08-06 19:52:23
Acquisition Stop        2010-08-06 22:30:16
Output File(s):
\\tsclient\E\Image\New Folder\2010-08-07 07.52.21 - 192.168.1.4\Output.001
\\tsclient\E\Image\New Folder\2010-08-07 07.52.21 - 192.168.1.4\Output.002
……………………………
\\tsclient\E\Image\New Folder\2010-08-07 07.52.21 - 192.168.1.4\Output.038
Verification:   Passed
Hash(es):
MD5: 1b26c0e62b79f528793199a3d2de4034
SHA1: 52bafa6d754870b33cb85089ae89538c9355844c
SHA256:
7dae7de2edc15a48e6343f7410f63ccaab773942df1474d9ce613f9608957074
SHA512:
c0894e8903cfccca47989ed0589f34d69943e417824a37442ef7240e9bf0b186d
736679911ad0c80565e339420b3c285e9f386217f1d1d1e7bba7e8e7a27bd17
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AFR-08 **FAILED** AFR-09 PASSED	AIC-01 PASSED AIC-02 PASSED AIC-03 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED	ALOG-01 PASSED ALOG-02 **FAILED** ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. Errors type and location did not report to the user.		

2.14. TC-07-InsufficientSpace & TC-08

<table>
<tr><td colspan="2">Test Case TC-07-Insufficient space & TC-08 (Helix3 Pro 2009 R3)</td></tr>
<tr><td>Test & Case Summary:</td><td>Attempt to create an image file where destination device has insufficient space, and see whether the tool notifies the user and offer another destination device to continue</td></tr>
<tr><td>Assertion:</td><td><table>
<tr><td>AFR-01</td><td>The tool accesses the digital source with a supported access interface</td></tr>
<tr><td>AFR-02</td><td>The tool acquires a digital source</td></tr>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-04</td><td>The tool creates an image file of the digital source</td></tr>
<tr><td>AFR-05</td><td>The tool acquires all the visible data sectors from the digital source</td></tr>
<tr><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-04</td><td>The tool reports to the user if insufficient space in the destination device during the image creation process.</td></tr>
<tr><td>AIC-05</td><td>If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller</td></tr>
<tr><td>AIC-10</td><td>The tool reports to the user if insufficient space in the destination device to contain the multi-image file creation and if destination device switching function is supported, the image is continue on the selected destination device.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table></td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380811 AS (80GB)
Serial Number: 6PS2CA4Z
Sector count: 156,296,385
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>/dev/sdc: current max LBA: 156,296,385
/dev/sdc: native max LBA: 156,296,385
/dev/sdc: physical max LBA: 156,296,385
/dev/sdc: HPA not set
/dev/sdc: DCO not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>System</th></tr>
<tr><td>/dev/sdc1</td><td>63</td><td>4192964</td><td>4192902</td><td>NTFS</td></tr>
<tr><td>/dev/sdc2</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sdc3</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sdc4</td><td>10490508</td><td>12594959</td><td>2104452</td><td>Ext2</td></tr>
<tr><td>/dev/sdc5</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/deb/sdc6</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
<tr><td>unallocated</td><td>19149480</td><td>156296384</td><td>137146905</td><td>Empty</td></tr>
</table></td></tr>
</table>

Log highlights:	 Helix3 Pro Not enough space on 'F:\' There is not enough free space on the destination drive to store this image. **Image 1:Insufficient Space**
Results by assertion:	**TC-07** AFR-01 PASSED ALOG-01 PASSED AFR-02 PASSED ALOG-02 **FAILED** AFR-03 PASSED ALOG-03 PASSED AFR-04 PASSED AIC-04 PASSED **TC-08** AFR-01 PASSED AIC-04 PASSED ALOG-01 PASSED AFR-02 PASSED AIC-05 PASSED ALOG-02 **FAILED** AFR-03 PASSED AIC-10 **FAILED** ALOG-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 FAILED
Analysis:	Test result **FAILED**. Notification has provided to the user that the destination device does not have enough free space to store the full image. Space checking is done prior Imaging starts. Alternative storage device option should provide to the user. However, the acquired start and end sectors were not displayed and reported to the user.

2.15. TC-12 Partially and Completely Hidden by HPA

Test Case TC-12 Partially and Completely Hidden by HPA (Helix3 Pro 2009 R3)	
Test & Case Summary:	Acquire a partition that is partially or completely hidden by HPA or DCO **Notes**: FAT32 partition has been partially hidden by HPA from 150301488 to 156301487.
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-06** The tool acquires all the hidden data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported **AHS-01** The tool reports to the user if any hidden sectors are found **AHS-02** The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment **AHS-03** The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: N/A
Drive Setup:	/dev/sdb: current max LBA: 150,301,484 /dev/sdb: native max LBA: 150,301,484 /dev/sdb: physical max LBA: **156,301,488** /dev/sdb: **HPA set from sector 150,301,488 to 156,301,487** **(Total 736,388 sectors)**
Partition Table:	**Device** | **Start** | **End** | **#sectors** | **File System** /dev/sdb1 | 63 | 2104514 | 2104452 | NTFS /dev/sdb2 | 2104515 | 149565149 | 145460535 | Ext3 /dev/sdb3 | 149565150 | 156296384 | 6731234 | FAT32 **(Partially HPA)**

Log highlights:	Both tests came back with the same result. No Log is created.
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 **FAILED** AFR-06 **FAILED** AFR-07 N/A AIC-01 N/A AIC-02 N/A AIC-05 N/A AIC-06 N/A AIC-07 N/A AIC-08 N/A AHS-01 N/A AHS-02 N/A AHS-03 N/A ALOG-01 N/A ALOG-02 N/A ALOG-03 N/A
Analysis:	Test **FAILED** to achieve the expected Result. No Log is created due to the reason that Helix 3 pro acquiring image in extremely slow speed.

2.16. TC-12 Partially Hidden by HPA

Test Case TC-12 Partially and Completely Hidden by HPA (Helix3 Pro 2009 R3)	
Test & Case Summary:	Acquire a partition that is partially or completely hidden by HPA or DCO **Notes**: NTFS partition has been partially hidden by HPA from 6301488 to 156301487. No partition table was detected in this case.
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-06** The tool acquires all the hidden data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported **AHS-01** The tool reports to the user if any hidden sectors are found **AHS-02** The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment **AHS-03** The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution

	environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: N/A
Drive Setup:	/dev/sdb: current max LBA: 150,301,484 /dev/sdb: native max LBA: 150,301,484 /dev/sdb: physical max LBA: **156,301,488** /dev/sdb: **HPA set from sector 6,301,488 to 156,301,487** **(Total 150,000,000 sectors)**
Partition Table:	**Device** **Start** **End** **#sectors** **File System** /dev/sdb1 4096 2101247 2097152 FAT32 /dev/sdb2 2101248 6297599 4196352 NTFS /dev/sdb3 6297600 156301311 150003712 NTFS **(Partially HPA)**
Log highlights:	Created By Helix3 Pro 2009R3 OS Name Windows Vista OS Mode Workstation OS Build 6.1.7600 Administrator True physical True size **<u>3224567808</u>** name PhysicalDrive1 mount PhysicalDrive1 serialnumber 5MR18V18 system ST380817AS firmware 3.42 T type Fixed hard disk WholeDisk True Acquire Format: RAW Acquisition Start: 2010-10-17 09:19:51 Acquisition Stop 2010-10-17 09:21:28 E:\Image\Helix_PartHPA_Test2.001 E:\Image\Helix_PartHPA_Test2.002 Verification: Passed MD5: 203a251380ef3fe11a6ab0c8ead814ee SHA1: e01ef3dcbcc9851b40cb64b52f0ba1d89bef3cf6
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AHS-02 PASSED AFR-02 PASSED AIC-02 PASSED AHS-03 PASSED AFR-03 PASSED AIC-05 PASSED ALOG-01 **FAILED** AFR-04 PASSED AIC-06 PASSED ALOG-02 PASSED AFR-05 PASSED AIC-07 PASSED ALOG-03 PASSED AFR-06 PASSED AIC-08 PASSED AFR-07 PASSED AHS-01 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. The logged size information of the hard disk is inaccurate. The correct size of the visible data is **<u>3,226,361,856</u>** bytes instead. However, the total amount of data acquired is correct and complete.

2.17. TC-13- Overlapping Partitions

<table>
<tr><th colspan="2">Test Case TC-13 Overlapping Partitions (Helix3 Pro 2009 R3)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a partition that is overlapping with another partition
Notes: Partitions are overlapped. The last NTFS partition started before the end of the last partition. Starting sector changed from 79,168,320 to 79,100,000.</td></tr>
<tr><td>Assertions:</td><td>
<table>
<tr><td>AFR-01</td><td>The tool accesses the digital source with a supported access interface</td></tr>
<tr><td>AFR-02</td><td>The tool acquires a digital source</td></tr>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-04</td><td>The tool creates an image file of the digital source</td></tr>
<tr><td>AFR-05</td><td>The tool acquires all the visible data sectors from the digital source</td></tr>
<tr><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-01</td><td>The data represented by an image file is the same as the data acquired by the tool</td></tr>
<tr><td>AIC-02</td><td>The tool creates an image file according to the file format the user specified.</td></tr>
<tr><td>AIC-11</td><td>The tool reports to the user if any irregularities found in the digital source.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table>
</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source Hashes:
md5: 3170cec7e6720af973cc37a946c32ae3
sha1: 6366ad8cd563c05f086dfe7b7884b08fd9795069
/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>20980764</td><td>20980827</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>20980890</td><td>79168320</td><td>58187430</td><td>Ext3</td></tr>
<tr><td>/dev/sdb3</td><td>79100000</td><td>156296385</td><td>77128065</td><td>NTFS (Modified)</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Created By Helix3 Pro 2009R3
Computer Name: helix
Uptime: 6 minutes
User Name root
description ATA Disk
product ST380817AS
vendor Seagate
physid 0
businfo scsi@2:0.0.0
logicalname /dev/sda
dev 8d:0d
version 3.42
serial 5MR18V18</td></tr>
</table>

	size 80026361856 ansiversion 5 signature 00055737 WholeDisk True VendorName ATA ST380817AS ACQUISITION INFORMATION Acquire Format: RAW Acquisition Start: 2010-09-08 08:05:09 Acquisition Stop 2010-09-08 09:29:39 Output File(s): /mnt/Image/Helix3-OverlappingPartition-Nowriteblock.001 /mnt/Image/Helix3-OverlappingPartition-Nowriteblock.002 …………………………………. /mnt/Image/Helix3-OverlappingPartition-Nowriteblock.038 Verification: Passed Hash(es): MD5: 3170cec7e6720af973cc37a946c32ae3 SHA1: 6366ad8cd563c05f086dfe7b7884b08fd9795069
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-02 PASSED AFR-03 PASSED AIC-11 **FAILED** AFR-04 PASSED ALOG-01 PASSED AFR-05 PASSED ALOG-02 **FAILED** AFR-07 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. Helix 3 pro is unable to recover the partition table and the irregularity of the partition table is not reported to the user. The image is acquired correctly.

2.18. TC-14 Partition out of boundary

Test Case TC-14 Partition out of boundary (Helix3 Pro 2009 R3)	
Test & Case Summary:	Acquire a hard disk with a partition's end address ended outside the physical boundary **Notes**: Partitions ended out of the physical boundary of the disk. The last partition end sector **changed from 72,331,264 to 72,380,000**.
Assertions:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-11** The tool reports to the user if any irregularities found in the digital source. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

	sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	Source hashes: MD5 - b42f526d394078656308a9b96aa77188 SHA1 - e2977a0cd2d2608519b1750e980252d01cdb4718 /dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA and DCO are not set
Partition Table:	**Device** **Start** **End** **#sectors** **File System** /dev/sdb1 2048 40962047 40960000 NTFS /dev/sdb2 40962048 83970047 43008000 Ext4 /dev/sdb3 83972096 **156350047** 72377951 Extended **(Modified)**
Log highlights:	Created By Helix3 Pro 2009R3 Examiner: James Liang ST380817AS SYSTEM INFORMATION OS Name Windows XP OS Mode Workstation OS Patch Service Pack 3 OS Build 5.1.2600 User Name Administrator Administrator True NIC 1 - IP 192.168.182.134 DISK INFORMATION physical True size 80023749120 serialnumber 3.42 system AS firmware ST380817 type Fixed hard disk WholeDisk True Encryption ACQUISITION INFORMATION Acquire Format: RAW Acquisition Start: 2010-09-10 15:56:16 Acquisition Stop 2010-09-10 20:02:50 Output File(s): G:\Image\Helix3-Partition_OutOfBound.001 G:\Image\Helix3-Partition_OutOfBound.002 ………………………… G:\Image\Helix3-Partition_OutOfBound.038 Verification: Passed

	Hash(es): MD5: b42f526d394078656308a9b96aa77188 SHA1: e2977a0cd2d2608519b1750e980252d01cdb4718
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-02 PASSED AFR-03 PASSED AIC-11 **FAILED** AFR-04 PASSED ALOG-01 PASSED AFR-05 PASSED ALOG-02 **FAILED** AFR-07 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. All the data are acquired correctly but Helix 3 Pro failed to report to the user that irregularity existed in the digital source. Serial Number of the source device is not displayed correctly.

2.19. TC-15 Unreadable MBR

Test Case TC-15 Unreadable MBR (Helix3 Pro 2009 R3)	
Test & Case Summary:	Acquire a hard disk with an unreadable MBR **Notes**: Partitions ended out of the physical boundary of the disk. Data of MBR is replaced by value 0.
Assertions:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AFR-08** The tool reports to the user of the error type and the location of the error if error occurred during the reading from a digital source. **AFR-09** If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-03** The tool reports to the user if an error occurs during the image creation process. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **AIC-11** The tool reports to the user if any irregularities found in the digital source. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

	ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA and DCO are not set
Partition Table:	**Device Start End #sectors File System** /dev/sdb1 2048 40962047 40960000 NTFS /dev/sdb2 40962048 83970047 43008000 Ext4 /dev/sdb3 83972096 156301311 72329125 Extended
Log highlights:	Created By Helix3 Pro 2009R3 SYSTEM INFORMATION OS Name Windows XP OS Mode Workstation OS Patch Service Pack 3 OS Build 5.1.2600 Computer Name JAMES-212DFE2EF User Name Administrator Administrator True NIC 1 - IP 192.168.182.134 NIC 1 - MAC 00:0C:29:E1:F8:FA NIC 1 - Subnet 255.255.255.0 DISK INFORMATION physical True size 80023749120 name PhysicalDrive2 mount PhysicalDrive2 serialnumber 3.42 system AS firmware ST380817 type Fixed hard disk WholeDisk True ACQUISITION INFORMATION Acquire Format: RAW Acquisition Start: 2010-09-12 23:58:54 Acquisition Stop 2010-09-13 04:17:59 Output File(s): G:\Image\Helix-UnReadableMBR.001 G:\Image\Helix-UnReadableMBR.002 …………………………….. G:\Image\Helix-UnReadableMBR.038 Verification: Passed Hash(es): MD5: 2ab63e47f402406afed31dad063df7f8 SHA1: d337f09ba2b9069668c70a14a2fc87a3b21a5887

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AFR-08 PASSED **AFR-09 PASSED**	AIC-01 PASSED AIC-02 PASSED AIC-03 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AIC-11 **FAILED**	ALOG-01 PASSED ALOG-02 **FAILED** ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. Helix Imager is not able to recognise the partition table that existed in the device.		

2.20. TC-16-01 Acquire a Single GUID Partition

Test Case TC-16-01 Acquire a Single GUID Partition (Helix3 Pro 2009 R3)		
Test & Case Summary:	Acquire a Single GUID Partition **Notes**: Hard drive partitioned as GPT disk. 6 partitions are created.	
Assertions:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device	
Drive Setup:	/dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488	

<table>
<tr><td></td><td>/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set</td></tr>
<tr><td>Partition Table (GPT disk):</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>34</td><td>262110</td><td>262144</td><td>Microsoft Reserved</td></tr>
<tr><td>/dev/sdb2</td><td>264192</td><td>8652799</td><td>8388608</td><td>NTFS</td></tr>
<tr><td>/dev/sdb3</td><td>8652800</td><td>12847103</td><td>4194304</td><td>NTFS</td></tr>
<tr><td>/dev/sdb4</td><td>12847104</td><td>14944255</td><td>2097152</td><td>NTFS</td></tr>
<tr><td>/dev/sdb5</td><td>14944256</td><td>25380863</td><td>10436608</td><td>NTFS</td></tr>
<tr><td>/dev/sdb6</td><td>25380864</td><td>156299264</td><td>130918400</td><td>NTFS</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>No logs were generated.</td></tr>
<tr><td>Results by assertion:</td><td>
<table>
<tr><td>AFR-01</td><td>PASSED</td><td>AIC-01</td><td>N/A</td><td>ALOG-01</td><td>N/A</td></tr>
<tr><td>AFR-02</td><td>FAILED</td><td>AIC-02</td><td>N/A</td><td>ALOG-02</td><td>N/A</td></tr>
<tr><td>AFR-03</td><td>PASSED</td><td>AIC-05</td><td>N/A</td><td>ALOG-03</td><td>N/A</td></tr>
<tr><td>AFR-04</td><td>N/A</td><td>AIC-06</td><td>N/A</td><td></td><td></td></tr>
<tr><td>AFR-05</td><td>N/A</td><td>AIC-07</td><td>N/A</td><td></td><td></td></tr>
<tr><td>AFR-07</td><td>N/A</td><td>AIC-08</td><td>N/A</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Analysis:</td><td>Test FAILED expected result. Helix 3 Pro cannot identify the GUID partitions in the test drive.</td></tr>
</table>

2.21. TC-16-02 Acquire a GPT disk

<table>
<tr><th colspan="2">Test Case TC-16-02 Acquire a GPT disk (Helix3 Pro 2009 R3)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a GPT disk
Notes: Hard drive partitioned as GPT disk. 6 partitions are created. Helix 3 pro cannot detect GUID partitions.</td></tr>
<tr><td>Assertions:</td><td>
<table>
<tr><td>AFR-01</td><td>The tool accesses the digital source with a supported access interface</td></tr>
<tr><td>AFR-02</td><td>The tool acquires a digital source</td></tr>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-04</td><td>The tool creates an image file of the digital source</td></tr>
<tr><td>AFR-05</td><td>The tool acquires all the visible data sectors from the digital source</td></tr>
<tr><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-01</td><td>The data represented by an image file is the same as the data acquired by the tool</td></tr>
<tr><td>AIC-02</td><td>The tool creates an image file according to the file format the user specified.</td></tr>
<tr><td>AIC-05</td><td>If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller</td></tr>
<tr><td>AIC-06</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.</td></tr>
<tr><td>AIC-07</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.</td></tr>
<tr><td>AIC-08</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-</td><td>The tool display correct information about the acquisition to the user. The</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>02</td><td>information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td></td><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td colspan="2">Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td colspan="2">Source Hashes:
MD5: 7a84a94aae46d34ac61dc26800f6dd19
SHA1: f913fd6832de537c78dc4da881281984daed37f5
/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set</td></tr>
<tr><td>Partition Table (GPT disk):</td><td colspan="2"><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>34</td><td>262110</td><td>262144</td><td>Microsoft Reserved</td></tr>
<tr><td>/dev/sdb2</td><td>264192</td><td>8652799</td><td>8388608</td><td>NTFS</td></tr>
<tr><td>/dev/sdb3</td><td>8652800</td><td>12847103</td><td>4194304</td><td>NTFS</td></tr>
<tr><td>/dev/sdb4</td><td>12847104</td><td>14944255</td><td>2097152</td><td>NTFS</td></tr>
<tr><td>/dev/sdb5</td><td>14944256</td><td>25380863</td><td>10436608</td><td>NTFS</td></tr>
<tr><td>/dev//sdb6</td><td>25380864</td><td>156299264</td><td>130918400</td><td>NTFS</td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td colspan="2">Created By Helix3 Pro 2009R3
OS Name Windows XP
OS Patch Service Pack 3
Administrator True
physical True
size 80023749120
serialnumber 3.42
firmware ST380817
type Fixed hard disk
WholeDisk True
Acquire Format: RAW
Acquisition Start: 2010-09-17 01:44:28
Acquisition Stop 2010-09-17 06:01:05
Output File(s):
G:\Image\Helix3-GUID.001
G:\Image\Helix3-GUID.002
………………………
G:\Image\Helix3-GUID.038
Verification: Passed
Hash(es):
MD5: 7a84a94aae46d34ac61dc26800f6dd19
SHA1: f913fd6832de537c78dc4da881281984daed37f5</td></tr>
</table>

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED ALOG-01 PASSED ALOG-02 **FAILED** ALOG-03 PASSED
Analysis:	Test **PASSED** to achieve expected result.

2.22. TC-17 Acquire a partially hidden GPT Partition

Test Case TC-17 Acquire a partially hidden GPT Partition (Helix3 Pro 2009 R3)		
Test & Case Summary:	**Acquire a partially hidden GPT Partition** **Notes**: Hard drive partitioned as GPT disk.	
Assertions:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-06	The tool acquires all the hidden data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
	AHS-01	The tool reports to the user if any hidden sectors are found
	AHS-02	The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment
	AHS-03	The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	**Source Hashes:** MD5: 795830763fb69dbc4a08d99c010f967a SHA1: 177b71e876a8595edd1dafbf221b5af4178afecd	

Helix3 Pro R3 (Release Date: 30th, Dec 2009)

<table>
<tr><td></td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td>/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA set from sector 6,500,001 to 156, 301,487
(Total 149,801,847 sectors are hidden)</td></tr>
<tr><td>Partition Table (GPT disk):</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>1</td><td>63</td><td>63</td><td>MS Reserved</td></tr>
<tr><td>Unallocated</td><td>4096</td><td>2101247</td><td>2097152</td><td>Unallocated</td></tr>
<tr><td>/dev/sdb2</td><td>2101248</td><td>6297599</td><td>4196352</td><td>Ext4</td></tr>
<tr><td>/dev/sdb3</td><td>6297600</td><td>156301311</td><td>150003712</td><td>NTFS (Partially HPA)</td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Created By Helix3 Pro 2009R3
OS Name Windows Vista
OS Mode Workstation
OS Build 6.1.7600
OS Suite Single User Terminal Services
Computer Name JAMES-I5
Uptime0 Days 0 Hours 35 Minutes 28 Seconds
User Name James
Administrator True
physical True
size 3327787008
name PhysicalDrive1
mount PhysicalDrive1
serialnumber 5MR18V18
system ST380817AS
firmware 3.42 T
type Fixed hard disk
WholeDisk True
Acquire Format: RAW
Acquisition Start: 2010-10-18 17:59:19
Acquisition Stop 2010-10-18 18:01:04
Output File(s):
E:\Image\helix_GPThpaPart_acq.001
E:\Image\helix_GPThpaPart_acq.002
Verification: Passed
MD5: 795830763fb69dbc4a08d99c010f967a
SHA1: 177b71e876a8595edd1dafbf221b5af4178afecd</td></tr>
</table>

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 **FAILED** ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected result. Helix 3 Pro is not support GPT partition. HPA is not detected and acquired.

2.23. TC-18 Network Image Acquisition

Test Case TC-18 Network Image Acquisition (Helix3 Pro 2009 R3)	
Test & Case Summary:	Network Image Acquisition Notes: Images are transferring from Windows 7 environment to Windows XP SP3 environment that running using VMware
Assertions:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **AIC-11** The tool reports to the user if any irregularities found in the digital source. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: N/A
Drive	Source Hashes:

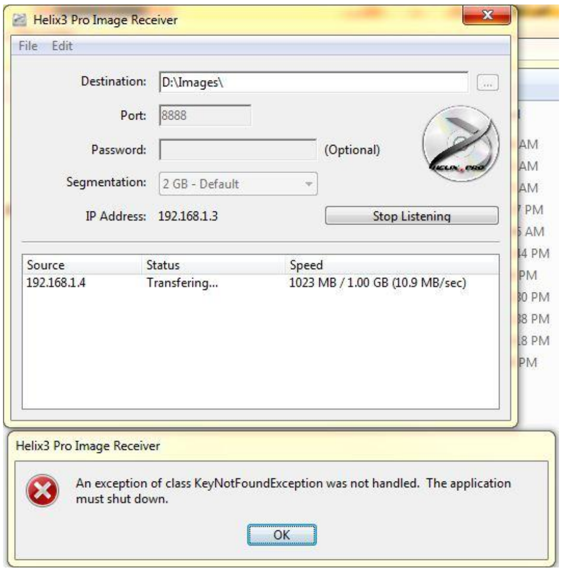
Helix3 Pro R3 (Release Date: 30th, Dec 2009)

<table>
<tr><td>Setup:</td><td>MD5 d48a1018a5fbb72b40d36da51e396eb3
SHA1 37350ce8c4f21a07fac3ac625e43d8e6d0c99878
/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>4192964</td><td>4192902</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>4193028</td><td>6297479</td><td>2104452</td><td>FAT32</td></tr>
<tr><td>/dev/sdb3</td><td>6297543</td><td>10490444</td><td>4192902</td><td>FAT16</td></tr>
<tr><td>/dev/sdb4</td><td>10490508</td><td>12594959</td><td>2104452</td><td>Ext2</td></tr>
<tr><td>/dev/sdb5</td><td>12595023</td><td>14699474</td><td>2104452</td><td>Ext3</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>19149479</td><td>256977</td><td>Swap</td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Created By Helix3 Pro
Notes: From address 192.168.1.4 to 192.168.1.8
DISTRIB ID Ubuntu
DISTRIB RELEASE 9.04
User Name root
NIC 1 - IP 192.168.1.4
NIC 1 - MAC 00:04:61:4E:44:BC
NIC 1 - Subnet 255.255.255.0
description Windows NTFS volume
logicalname /dev/sda1
version3.1
serial 4caad899-0215-4406-929a-691d362ccfb8
size 3224244736
capacity 3224277504
clustersize 4096
created2010-07-26 12:39:19
filesystem ntfs
ntfs Windows NTFS
Acquire Format: RAW
Acquisition Start: 2010-08-03 10:41:29
Acquisition Stop 2010-08-03 10:43:38
Output File(s):
C:\Image\2010-08-03 22.41.28 - 192.168.1.4\Output.001
C:\Image\2010-08-03 22.41.28 - 192.168.1.4\Output.002
Verification: Passed
Hash(es):
MD5: d48a1018a5fbb72b40d36da51e396eb3
SHA1: 37350ce8c4f21a07fac3ac625e43d8e6d0c99878</td></tr>
<tr><td>Results by assertion:</td><td><table>
<tr><td>AFR-01 PASSED</td><td>AIC-01 PASSED</td><td>ALOG-01 PASSED</td></tr>
<tr><td>AFR-02 PASSED</td><td>AIC-02 PASSED</td><td>ALOG-02 FAILED</td></tr>
<tr><td>AFR-03 PASSED</td><td>AIC-05 PASSED</td><td>ALOG-03 PASSED</td></tr>
<tr><td>AFR-04 PASSED</td><td>AIC-06 PASSED</td><td></td></tr>
<tr><td>AFR-05 PASSED</td><td>AIC-07 PASSED</td><td></td></tr>
<tr><td>AFR-07 PASSED</td><td>AIC-08 PASSED</td><td></td></tr>
</table></td></tr>
</table>

Analysis: Test **PASSED** to achieve the expected Result after few attempted. Source Hashes matched verification hashes.

However, program clashed under Windows 7 environment (See Image 2).

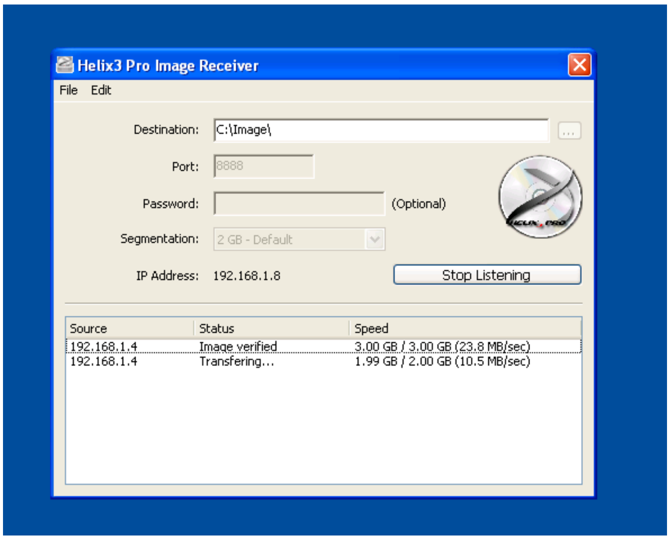
Also, program freeze in windows XP environment when transferring images to the destination using a local network connection (See Image 3).



```
Destination:   D:\Images\
Port:          8888
Password:                  (Optional)
Segmentation:  2 GB - Default
IP Address:    192.168.1.3

Source         Status          Speed
192.168.1.4    Transfering...  1023 MB / 1.00 GB (10.9 MB/sec)
```

An exception of class KeyNotFoundException was not handled. The application must shut down.

Image 2: Program Clashed



```
Destination:   C:\Image\
Port:          8888
Password:                  (Optional)
Segmentation:  2 GB - Default
IP Address:    192.168.1.8

Source         Status          Speed
192.168.1.4    Image verified  3.00 GB / 3.00 GB (23.8 MB/sec)
192.168.1.4    Transfering...  1.99 GB / 2.00 GB (10.5 MB/sec)
```

Image 3: Program Freeze

Test Results – AIR

3.1. TC-01-FW

Test Case TC-01-FW **(AIR 2.0.0)**	
Test & Case Summary:	Acquire a hard drive using Access Interface (AI) and convert to an image file Notes: Firewire Access Interface (AI)
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	Source hashes MD5 checksum: 436a043c1766f46f3945e605144f22eb SHA1 checksum: 82d4b6226995d11b82979db901e809a06b1574e8 /dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA not set /dev/sdb: DCO not set

Log highlights:

```
Command-line:
dc3dd 6.12.4 started at 2010-07-01 11:21:08 +1200
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log
status=noxfer if=/dev/sdd skip=0 conv=noerror,sync iflag=direct
ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
md5 TOTAL: 436a043c1766f46f3945e605144f22eb
sha1 TOTAL: 82d4b6226995d11b82979db901e809a06b1574e8
156301488+0 sectors in
156301488+0 sectors out
dc3dd completed at 2010-07-01 12:32:27 +1200
Command completed: Thu Jul  1 12:32:30 NZST 2010
Start VERIFY: Thu Jul  1 12:32:30 NZST 2010
Command-line: cat /mnt/Images/Caine/caine_80g.dd.* | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 436a043c1766f46f3945e605144f22eb
        sha1 TOTAL: 82d4b6226995d11b82979db901e809a06b1574e8
Copy = md5 TOTAL: 436a043c1766f46f3945e605144f22eb
        sha1 TOTAL: 82d4b6226995d11b82979db901e809a06b1574e8
Command completed: Thu Jul  1 13:01:17 NZST 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED	AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.	

3.2. TC-01-USB

Test Case TC-01-USB **(AIR 2.0.0)**	
Test & Case Summary:	Acquire a hard drive using Access Interface (AI) and convert to an image file Notes: USB interface
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool AIC-05 If multi-file image creation and the image file size is selected,

	the tool creates a multi-file image except that one file may be smaller ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: Kingston DT 101 II (16 GB) Serial Number: 5MR18V18 Sector count: 31,272,544 Write blocker: Tableau T8 Forensic USB Bridge
Drive Setup:	Source hashes MD5: 7ca6d932d51138e1a8e4cfbb9540483c SHA1: fc4d8c39e052331e15a0b7bdd5ae08804bbab2a6 /dev/sda: current max LBA: 31,272,544 /dev/sda: native max LBA: 31,272,544 /dev/sda: physical max LBA: 31,272,544 /dev/sda: HPA not set /dev/sda: DCO not set
Log highlights:	Start DC3DD (md5 sha1): Thu Jul 1 10:59:00 NZST 2010 command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sdc skip=0 conv=noerror,sync iflag=direct ibs=32768 compiled options: DEFAULT_BLOCKSIZE=32768 sector size: 512 (assumed) md5 TOTAL: 7ca6d932d51138e1a8e4cfbb9540483c sha1 TOTAL: fc4d8c39e052331e15a0b7bdd5ae08804bbab2a6 31272544+0 sectors in 31272544+0 sectors out Command completed: Thu Jul 1 11:14:44 NZST 2010 Start VERIFY: Thu Jul 1 11:14:44 NZST 2010 dc3dd if=/mnt/Images/Caine/caine.dd hash=md5,sha1 conv=noerror,sync hashlog=/tmp/verify_hash.log status=noxfer | air-counter 2>> /usr/local/share/air/logs/air.buffer.data > /dev/null VERIFY SUCCESSFUL: Hashes match Orig = md5 TOTAL: 7ca6d932d51138e1a8e4cfbb9540483c sha1 TOTAL: fc4d8c39e052331e15a0b7bdd5ae08804bbab2a6 Copy = md5 TOTAL: 7ca6d932d51138e1a8e4cfbb9540483c sha1 TOTAL: fc4d8c39e052331e15a0b7bdd5ae08804bbab2a6 Command completed: Thu Jul 1 11:18:48 NZST 2010
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

3.3. TC-02-NTFS

<table>
<tr><th colspan="2">Test Case TC-02-NTFS (AIR 2.0.0)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a digital source that supported by the tools to an image file
Notes: Acquire NTFS partition only</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: d48a1018a5fbb72b40d36da51e396eb3
SHA512 checksum:
ff3a752011324ca7b70219c03e230051235aa3cf3a3097698f8a879be9f8e08a64
de7b791e185fa19f58905a2496955302da4a775d31ddaefe26cf31a5e6956f
/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#Sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>6297479</td><td>6297417</td><td>NTFS</td><td>3Gb</td></tr>
<tr><td>/dev/sdb2</td><td>6297543</td><td>10490444</td><td>4192902</td><td>Ext2</td><td>2Gb</td></tr>
<tr><td>/dev/sdb3</td><td>10490508</td><td>14683409</td><td>4192902</td><td>Ext3</td><td>2Gb</td></tr>
<tr><td>/dev/sdb4</td><td>14683473</td><td>16787924</td><td>2104452</td><td>FAT16</td><td>1Gb</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>20996954</td><td>2104452</td><td>Swap</td><td>1Gb</td></tr>
</table>
</td></tr>
</table>

AIR 2.0.0 (Release Date: 17th, Feb 2010)

Log highlights:

```
Start DC3DD (md5 sha512): Tue Jul 27 02:57:07 NZST 2010

Hash will be calculated on /dev/sdc1.
dc3dd 6.12.4 started at 2010-07-27 02:57:07 +1200
command line: dc3dd hash=md5,sha512 hashlog=/tmp/hash.log status=noxfer
if=/dev/sdc1 skip=0 conv=noerror iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)

md5 TOTAL: d48a1018a5fbb72b40d36da51e396eb3
sha512 TOTAL:
ff3a752011324ca7b70219c03e230051235aa3cf3a3097698f8a879be9f8e08a64
de7b791e185fa19f58905a2496955302da4a775d31ddaefe26cf31a5e6956f
6297417+0 sectors in
6297417+0 sectors out
Command completed: Tue Jul 27 03:02:10 NZST 2010

Start VERIFY: Tue Jul 27 03:02:10 NZST 2010

Command-line: cat /mnt/new/new/Test002/Test002_AIR_NTFS.* | air-
counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha512
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: d48a1018a5fbb72b40d36da51e396eb3
sha512 TOTAL:
ff3a752011324ca7b70219c03e230051235aa3cf3a3097698f8a879be9f8e08a64
de7b791e185fa19f58905a2496955302da4a775d31ddaefe26cf31a5e6956f

Copy = md5 TOTAL: d48a1018a5fbb72b40d36da51e396eb3
sha512 TOTAL:
ff3a752011324ca7b70219c03e230051235aa3cf3a3097698f8a879be9f8e08a64
de7b791e185fa19f58905a2496955302da4a775d31ddaefe26cf31a5e6956f

Command completed: Tue Jul 27 03:07:19 NZST 2010
```

Results by assertion:

AFR-01	PASSED	AIC-01	PASSED
AFR-02	PASSED	AIC-05	PASSED
AFR-03	PASSED	ALOG-01	PASSED
AFR-04	PASSED	ALOG-02	PASSED
AFR-05	PASSED	ALOG-03	PASSED
AFR-07	PASSED		

Analysis: Test achieved the expected Result. Source hashes match verification hashes.

3.4. TC-02-Ext2

<table>
<tr><th colspan="2">Test Case TC-02-Ext2 (AIR 2.0.0)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a digital source that supported by the tools to an image file

Notes: Acquire Ext2 partition only</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5 checksum: b5c637ffdd3c94d855be01391ada64fe
SHA1 checksum: 4e681e1197929248a1e968943190d0886482c90b

/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>6297479</td><td>6297417</td><td>NTFS</td><td>3Gb</td></tr>
<tr><td>/dev/sdb2</td><td>6297543</td><td>10490444</td><td>4192902</td><td>Ext2</td><td>2Gb</td></tr>
<tr><td>/dev/sdb3</td><td>10490508</td><td>14683409</td><td>4192902</td><td>Ext3</td><td>2Gb</td></tr>
<tr><td>/dev/sdb4</td><td>14683473</td><td>16787924</td><td>2104452</td><td>FAT16</td><td>1Gb</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>20996954</td><td>2104452</td><td>Swap</td><td>1Gb</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Start DC3DD (md5 sha512): Tue Jul 27 03:08:36 NZST 2010
Command-line:
command line: dc3dd hash=md5,sha512 hashlog=/tmp/hash.log</td></tr>
</table>

```
status=noxfer if=/dev/sdc5 skip=0 conv=noerror iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
md5 TOTAL: b5c637ffdd3c94d855be01391ada64fe
sha512 TOTAL:
4c95bf198a427bb671f41aba378ecb34bd0cbc4f254708bbe59172ea6443e41e
6c18ea55cbe3441589ee8ad2db7d64a9beab70e33afd2d462d4de6eb350eb67c
4192902+0 sectors in
4192902+0 sectors out
Command completed: Tue Jul 27 03:11:39 NZST 2010

Start VERIFY: Tue Jul 27 03:11:39 NZST 2010
Command-line: cat /mnt/new/new/Test002/Test002_AIR_Ext2.* | air-
counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd
hash=md5,sha512 hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null

VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: b5c637ffdd3c94d855be01391ada64fe
sha512 TOTAL:
4c95bf198a427bb671f41aba378ecb34bd0cbc4f254708bbe59172ea6443e41e
6c18ea55cbe3441589ee8ad2db7d64a9beab70e33afd2d462d4de6eb350eb67c
Copy = md5 TOTAL: b5c637ffdd3c94d855be01391ada64fe
sha512 TOTAL:
4c95bf198a427bb671f41aba378ecb34bd0cbc4f254708bbe59172ea6443e41e
6c18ea55cbe3441589ee8ad2db7d64a9beab70e33afd2d462d4de6eb350eb67c
Command completed: Tue Jul 27 03:15:09 NZST 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED	AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.	

3.5. TC-02-Ext3

<table>
<tr><th colspan="2">Test Case TC-02-Ext3 (AIR 2.0.0)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a digital source that supported by the tools to an image file

Notes: Acquire Ext3 partition only</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
md5: dd010be4950db17ebe05b213cd57f6c4
sha512:
5eb120505c2daf982a42633d5ba1cc0ae45626adab95c9454a3d609be7557a01f0ad248d28f42f2b2ad8c6e2814473d027cdb495448491f157c37581ea5a456f
/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>6297479</td><td>6297417</td><td>NTFS</td><td>3Gb</td></tr>
<tr><td>/dev/sdb2</td><td>6297543</td><td>10490444</td><td>4192902</td><td>Ext2</td><td>2Gb</td></tr>
<tr><td>/dev/sdb3</td><td>10490508</td><td>14683409</td><td>4192902</td><td>Ext3</td><td>2Gb</td></tr>
<tr><td>/dev/sdb4</td><td>14683473</td><td>16787924</td><td>2104452</td><td>FAT16</td><td>1Gb</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>20996954</td><td>2104452</td><td>Swap</td><td>1Gb</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Start DC3DD (md5 sha512): Tue Jul 27 03:18:10 NZST 2010
dc3dd hash=md5,sha512 hashlog=/tmp/hash.log status=noxfer</td></tr>
</table>

	if=/dev/sdc6 skip=0 conv=noerror iflag=direct ibs=32768 compiled options: DEFAULT_BLOCKSIZE=32768 sector size: 512 (assumed) md5 TOTAL: dd010be4950db17ebe05b213cd57f6c4 sha512 TOTAL: 5eb120505c2daf982a42633d5ba1cc0ae45626adab95c9454a3d609be7557a01f0ad248d28f42f2b2ad8c6e2814473d027cdb495448491f157c37581ea5a456f 4192902+0 sectors in 4192902+0 sectors out Command completed: Tue Jul 27 03:21:18 NZST 2010 Start VERIFY: Tue Jul 27 03:21:18 NZST 2010 Command-line: cat /mnt/new/new/Test002/Test002_AIR_Ext3.* | air-counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha512 hashlog=/tmp/verify_hash.log status=noxfer of=/dev/null VERIFY SUCCESSFUL: Hashes match Orig = md5 TOTAL: dd010be4950db17ebe05b213cd57f6c4 sha512 TOTAL: 5eb120505c2daf982a42633d5ba1cc0ae45626adab95c9454a3d609be7557a01f0ad248d28f42f2b2ad8c6e2814473d027cdb495448491f157c37581ea5a456f Copy = md5 TOTAL: dd010be4950db17ebe05b213cd57f6c4 sha512 TOTAL: 5eb120505c2daf982a42633d5ba1cc0ae45626adab95c9454a3d609be7557a01f0ad248d28f42f2b2ad8c6e2814473d027cdb495448491f157c37581ea5a456f Command completed: Tue Jul 27 03:24:36 NZST 2010
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-05 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 PASSED AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

3.6. TC-02-FAT16

<table>
<tr><th colspan="2">Test Case TC-02-FAT16 (AIR 2.0.0)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a digital source that supported by the tools to an image file
Notes: Acquire FAT16 partition only</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
md5: dd010be4950db17ebe05b213cd57f6c4
sha512:
5eb120505c2daf982a42633d5ba1cc0ae45626adab95c9454a3d609be7557a01f0ad248d28f42f2b2ad8c6e2814473d027cdb495448491f157c37581ea5a456f
/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Table:</td><td>
<table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>6297479</td><td>6297417</td><td>NTFS</td><td>3Gb</td></tr>
<tr><td>/dev/sdb2</td><td>6297543</td><td>10490444</td><td>4192902</td><td>Ext2</td><td>2Gb</td></tr>
<tr><td>/dev/sdb3</td><td>10490508</td><td>14683409</td><td>4192902</td><td>Ext3</td><td>2Gb</td></tr>
<tr><td>/dev/sdb4</td><td>14683473</td><td>16787924</td><td>2104452</td><td>FAT16</td><td>1Gb</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>20996954</td><td>2104452</td><td>Swap</td><td>1Gb</td></tr>
</table>
</td></tr>
<tr><td>Log highlights:</td><td>Start DC3DD (md5 sha512): Tue Jul 27 03:26:16 NZST 2010
dc3dd hash=md5,sha512 hashlog=/tmp/hash.log status=noxfer if=/dev/sdc7 skip=0 conv=noerror iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768</td></tr>
</table>

```
sector size: 512 (assumed)

md5 TOTAL: b446594538d0f400fb80f54f6c78c481
sha512 TOTAL:
e54e842dbeccc3af83d1d81f8f8cca8c37947473bf41a5fd13d2dd5222d6ca6c0
a14cff1a0a0c6426637cc50e19df84c8efa4fa3f937b49c32ab7e4d5075b932
2104452+0 sectors in
2104452+0 sectors out
Command completed: Tue Jul 27 03:27:54 NZST 2010

Start VERIFY: Tue Jul 27 03:27:54 NZST 2010
Command-line: cat /mnt/new/new/Test002/Test002_AIR_FAT16.* | air-
counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd
hash=md5,sha512 hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: b446594538d0f400fb80f54f6c78c481
sha512 TOTAL:
e54e842dbeccc3af83d1d81f8f8cca8c37947473bf41a5fd13d2dd5222d6ca6c0
a14cff1a0a0c6426637cc50e19df84c8efa4fa3f937b49c32ab7e4d5075b932
Copy = md5 TOTAL: b446594538d0f400fb80f54f6c78c481
sha512 TOTAL:
e54e842dbeccc3af83d1d81f8f8cca8c37947473bf41a5fd13d2dd5222d6ca6c0
a14cff1a0a0c6426637cc50e19df84c8efa4fa3f937b49c32ab7e4d5075b932
Command completed: Tue Jul 27 03:29:39 NZST 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.

3.7. TC-02-SWAP

Test Case TC-02-SWAP (AIR 2.0.0)	
Test & Case Summary:	Acquire a digital source that supported by the tools to an image file Notes: Acquire Linux SWAP partition only
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool

<table>
<tr><td></td><td><table>
<tr><td>AIC-05</td><td>If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table></td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
md5: dd010be4950db17ebe05b213cd57f6c4
sha512:
5eb120505c2daf982a42633d5ba1cc0ae45626adab95c9454a3d609be7557a
01f0ad248d28f42f2b2ad8c6e2814473d027cdb495448491f157c37581ea5a
456f
/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>6297479</td><td>6297417</td><td>NTFS</td><td>3Gb</td></tr>
<tr><td>/dev/sdb2</td><td>6297543</td><td>10490444</td><td>4192902</td><td>Ext2</td><td>2Gb</td></tr>
<tr><td>/dev/sdb3</td><td>10490508</td><td>14683409</td><td>4192902</td><td>Ext3</td><td>2Gb</td></tr>
<tr><td>/dev/sdb4</td><td>14683473</td><td>16787924</td><td>2104452</td><td>FAT16</td><td>1Gb</td></tr>
<tr><td>/deb/sdb6</td><td>18892503</td><td>20996954</td><td>2104452</td><td>Swap</td><td>1Gb</td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Start DC3DD (md5 sha512): Tue Jul 27 03:31:20 NZST 2010
dc3dd hash=md5,sha512 hashlog=/tmp/hash.log status=noxfer
if=/dev/sdc9 skip=0 conv=noerror iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)

md5 TOTAL: 4e1e7f58383e4d89b6357293005cd1b3
sha512 TOTAL:
90801655cc2632352406b44e591eb1569fca6e16844a5bc9e1c01b0a80101d
585be0e5d443047f57ebe95acb2a59387c87428b1239e9bcd1748ad8151633
af81
2104452+0 sectors in
2104452+0 sectors out
Command completed: Tue Jul 27 03:32:58 NZST 2010

Start VERIFY: Tue Jul 27 03:32:58 NZST 2010
cat /mnt/new/new/Test002/Test002_AIR_Swap.* | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha512</td></tr>
</table>

```
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 4e1e7f58383e4d89b6357293005cd1b3
sha512 TOTAL:
90801655cc2632352406b44e591eb1569fca6e16844a5bc9e1c01b0a80101d
585be0e5d443047f57ebe95acb2a59387c87428b1239e9bcd1748ad8151633
af81
Copy = md5 TOTAL: 4e1e7f58383e4d89b6357293005cd1b3
sha512 TOTAL:
90801655cc2632352406b44e591eb1569fca6e16844a5bc9e1c01b0a80101d
585be0e5d443047f57ebe95acb2a59387c87428b1239e9bcd1748ad8151633
af81
Command completed: Tue Jul 27 03:34:47 NZST 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED	AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.	

3.8. TC-02-HFS

Test Case TC-02-HFS (AIR 2.0.0)		
Test & Case Summary:	Acquire a digital source that supported by the tools to an image file Notes: Acquire Mac partition type HFS partition only	
Assertion:	AFR-01	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported

AIR 2.0.0 (Release Date: 17th, Feb 2010)

<table>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
MD5: d8235a6c57ddf91c902d42f0e39cb7d5
SHA1: b91e9115388276b961e6a94a6322337048734d6c
/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>4096</td><td>4198399</td><td>4194304</td><td>HFS</td><td>2Gb</td></tr>
<tr><td>/dev/sdb2</td><td>4198400</td><td>14999551</td><td>10801152</td><td>HFS+</td><td>5Gb</td></tr>
<tr><td>Unallocated</td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Start DC3DD (md5 sha1): Fri Oct 1 09:21:11 NZDT 2010
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sda2 skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
md5 TOTAL: d8235a6c57ddf91c902d42f0e39cb7d5
sha1 TOTAL: b91e9115388276b961e6a94a6322337048734d6c
4194304+0 sectors in
4194304+0 sectors out
Command completed: Fri Oct 1 09:22:54 NZDT 2010
Start VERIFY: Fri Oct 1 09:22:54 NZDT 2010
Command-line: cat /mnt/new/Image/AcquireHFS.* | air-counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1 hashlog=/tmp/verify_hash.log status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: d8235a6c57ddf91c902d42f0e39cb7d5
sha1 TOTAL: b91e9115388276b961e6a94a6322337048734d6c
Copy = md5 TOTAL: d8235a6c57ddf91c902d42f0e39cb7d5
sha1 TOTAL: b91e9115388276b961e6a94a6322337048734d6c
Command completed: Fri Oct 1 09:24:35 NZDT 2010</td></tr>
<tr><td>Results by assertion:</td><td>AFR-01 PASSED
AFR-02 PASSED
AFR-03 PASSED
AFR-04 PASSED
AFR-05 PASSED
AFR-07 PASSED</td><td>AIC-01 PASSED
AIC-05 PASSED
ALOG-01 PASSED
ALOG-02 PASSED
ALOG-03 PASSED</td></tr>
<tr><td>Analysis:</td><td>Test achieved the expected Result. Source hashes match verification hashes.</td></tr>
</table>

3.9. TC-02-HFS+

<table>
<tr><th colspan="2">Test Case TC-02-HFS+ (AIR 2.0.0)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a digital source that supported by the tools to an image file
Notes: Acquire Mac partition type HFS+ partition only</td></tr>
<tr><td>Assertion:</td><td>AFR-01 The tool accesses the digital source with a supported access interface
AFR-02 The tool acquires a digital source
AFR-03 The tool operates in an execution environment
AFR-04 The tool creates an image file of the digital source
AFR-05 The tool acquires all the visible data sectors from the digital source
AFR-07 All data sectors acquired from the digital source are acquired accurately.
AIC-01 The data represented by an image file is the same as the data acquired by the tool
AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02 The tool display correct information about the acquisition to the user.
ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source hashes
md5: 5781d0f597685d4eff4cc3423900d73a
sha1: e878400c062b1690b586be41523d303edf3eae52
/dev/sda: current max LBA: 156,301,488
/dev/sda: native max LBA: 156,301,488
/dev/sda: physical max LBA: 156,301,488
/dev/sda: HPA not set
/dev/sda: DCO not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th><th>Size</th></tr>
<tr><td>/dev/sdb1</td><td>4096</td><td>4198399</td><td>4194304</td><td>HFS</td><td>2Gb</td></tr>
<tr><td>/dev/sdb2</td><td>4198400</td><td>14999551</td><td>10801152</td><td>HFS+</td><td>5Gb</td></tr>
<tr><td>Unallocated</td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Start DC3DD (md5 sha1): Fri Oct 1 10:11:33 NZDT 2010
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sda3 skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
md5 TOTAL: 5781d0f597685d4eff4cc3423900d73a</td></tr>
</table>

```
sha1 TOTAL: e878400c062b1690b586be41523d303edf3eae52
10801152+0 sectors in
10801152+0 sectors out
Command completed: Fri Oct  1 10:15:47 NZDT 2010
Start VERIFY: Fri Oct  1 10:15:47 NZDT 2010
cat /mnt/new/Image/AIR_HFSplus.* | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 5781d0f597685d4eff4cc3423900d73a
sha1 TOTAL: e878400c062b1690b586be41523d303edf3eae52
Copy = md5 TOTAL: 5781d0f597685d4eff4cc3423900d73a
sha1 TOTAL: e878400c062b1690b586be41523d303edf3eae52
Command completed: Fri Oct  1 10:19:59 NZDT 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED	AIC-01 PASSED AIC-05 PASSED ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test achieved the expected Result. Source hashes match verification hashes.	

3.10. TC-03-HPA

Test Case TC-03-HPA (AIR 2.0.0)		
Test & Case Summary:	Acquire a hard drive with hidden sectors to an image file Notes: HPA active	
Assertion:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-06	The tool acquires all the hidden data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.

	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
	AHS-01	The tool reports to the user if any hidden sectors are found
	AHS-02	The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment
	AHS-03	The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: N/A	
Drive Setup:	Source hashes MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 /dev/sdb: current max LBA: **94,868,928** /dev/sdb: native max LBA: 94,868,928 /dev/sdb: physical max LBA: **156,301,488** /dev/sdb: **HPA set from sector 94,868,928 to 156,301,488** /dev/sdb: DCO not set	

Partition Table:

Device	Start	End	#sectors	File System
/dev/sdb1	63	41945714	41945652	NTFS
/dev/sdb2	41945715	94863824	52918110	Ext3
/dev/sdb3	94863825	156296384	61432560	NTFS **(HPA)**

Log highlights:

```
Start DC3DD (md5 sha512): Mon Jul 26 08:00:39 NZST 2010
command line: dc3dd hash=md5,sha512 hashlog=/tmp/hash.log
status=noxfer if=/dev/sda skip=0 conv=noerror iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
md5 TOTAL: 69fdef5d5de3a207bc2a04017c38c3fd
sha512 TOTAL:
4ad5009bfc6232521fd893ad7d8cc7e0d592aa5de8cb6904b8d189664656ec51
7cc0e31fb57a93d034a3c23498c1494d54e2488835c2b6c3588b3607af48ad5f
94868928+0 sectors in
94868928+0 sectors out
Command completed: Mon Jul 26 09:14:50 NZST 2010
Start VERIFY: Mon Jul 26 09:14:50 NZST 2010
Command-line: cat /mnt/new/image_AIR_HPA.* | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha512
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 69fdef5d5de3a207bc2a04017c38c3fd
sha512 TOTAL:
4ad5009bfc6232521fd893ad7d8cc7e0d592aa5de8cb6904b8d189664656ec51
7cc0e31fb57a93d034a3c23498c1494d54e2488835c2b6c3588b3607af48ad5f
Copy = md5 TOTAL: 69fdef5d5de3a207bc2a04017c38c3fd
sha512 TOTAL:
4ad5009bfc6232521fd893ad7d8cc7e0d592aa5de8cb6904b8d189664656ec51
7cc0e31fb57a93d034a3c23498c1494d54e2488835c2b6c3588b3607af48ad5f
Command completed: Mon Jul 26 10:42:31 NZST 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. AIR failed to detect and acquire the hidden areas in the hard drive. Dc3dd command line option has the ability of detect Hidden areas.

3.11. TC-03-DCO

Test Case TC-03-DCO (AIR 2.0.0)	
Test & Case Summary	Acquire a hard drive with hidden sectors to an image file Notes: DCO active
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-06** The tool acquires all the hidden data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported **AHS-01** The tool reports to the user if any hidden sectors are found **AHS-02** The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment **AHS-03** The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18

	Sector count: 156,301,488 Write blocker: N/A
Drive Setup:	Source hashes MD5 checksum: 69fdef5d5de3a207bc2a04017c38c3fd SHA1 checksum: 9d768ab184ed9a172031f0f7b7f721f2bdf80b59 /dev/sdb: current max LBA: **94,863,828** /dev/sdb: native max LBA: 94,863,828 /dev/sdb: physical max LBA: **156,301,488** /dev/sdb: HPA not set /dev/sdb: **DCO set from sector 94,863,828 to 156,301,487**

Partition Table:

Device	Start	End	#sectors	File System
/dev/sdb1	63	41945714	41945652	NTFS
/dev/sdb2	41945715	94863824	52918110	Ext3
/dev/sdb3	94863825	156296384	61432560	NTFS **(DCO)**

Log highlights:

```
Start DC3DD (md5 sha512): Mon Jul 26 02:57:13 NZST 2010
dc3dd 6.12.4 started at 2010-07-26 02:57:13 +1200
command line: dc3dd hash=md5,sha512 hashlog=/tmp/hash.log status=noxfer
if=/dev/sda skip=0 conv=noerror iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)

md5 TOTAL: 69fdef5d5de3a207bc2a04017c38c3fd
sha512 TOTAL:
4ad5009bfc6232521fd893ad7d8cc7e0d592aa5de8cb6904b8d189664656ec517
cc0e31fb57a93d034a3c23498c1494d54e2488835c2b6c3588b3607af48ad5f
94868928+0 sectors in
94868928+0 sectors out
dc3dd completed at 2010-07-26 04:16:50 +1200
Command completed: Mon Jul 26 04:16:53 NZST 2010

Start VERIFY: Mon Jul 26 04:16:53 NZST 2010
Command-line: cat /mnt/dconew/new/ST380817AS_DCO_94868928.* | air-
counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha512
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null

VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 69fdef5d5de3a207bc2a04017c38c3fd
sha512 TOTAL:
4ad5009bfc6232521fd893ad7d8cc7e0d592aa5de8cb6904b8d189664656ec517
cc0e31fb57a93d034a3c23498c1494d54e2488835c2b6c3588b3607af48ad5f
Copy = md5 TOTAL: 69fdef5d5de3a207bc2a04017c38c3fd
sha512 TOTAL:
4ad5009bfc6232521fd893ad7d8cc7e0d592aa5de8cb6904b8d189664656ec517
cc0e31fb57a93d034a3c23498c1494d54e2488835c2b6c3588b3607af48ad5f
Command completed: Mon Jul 26 05:50:14 NZST 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. AIR failed to detect and acquire the hidden areas in the hard drive. Dc3dd itself supports hidden areas detection.

3.12. TC-05-DD

Test Case TC-05-DD **(AIR 2.0.0)**	
Test & Case Summary:	Acquire a digital source to an image file in an alternate supported format Notes: The original testing purpose was to acquire a HD image to DD format but error occurred during acquisition.
Assertion:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool. AIC-02 The tool creates an image file according to the file format the user specified. ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	Source hashes MD5 checksum: d615c245f1124a2482a5d56ffa8a1c55 Total sectors: 156,296,385 (80GB) /dev/sdb: current max LBA: 156,296,385 /dev/sdb: native max LBA: 156,296,385

	/dev/sdb: physical max LBA: 156,296,385 /dev/sdb: HPA not set /dev/sdb: DCO not set

Partition Setup:

Device	Start	End	#Sectors	File System
/dev/sda1	63	41945714	41945652	HPFS/NTFS
/dev/sda2	4192965	156296384	152103420	Extended
/dev/sda5	4193028	6297479	2104452	FAT32
/dev/sda6	6297543	10490444	4192902	FAT16
/dev/sda7	10490508	12594959	1052226	Ext2
/dev/sda8	12595023	14699474	2104452	Ext3
/dev/sda9	14699538	18892439	4192902	HPFS/NTFS
/dev/sda10	18892503	19149479	256977	Swap
unallocated	19149480	156296384	137146905	Empty

Log highlights:

```
Start DD (md5 inline): Sat Aug  7 17:41:26 NZST 2010
md5 hash will be calculated on /dev/sdc.
dd if=/dev/sdc skip=0 conv=noerror,sync iflag=direct ibs=32768 2>>
/usr/local/share/air/logs/air.image.log | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | tee /usr/local/share/air/air-fifo |
md5sum > /tmp/hash.log 2>&1
dd if=/usr/local/share/air/air-fifo 2>> /usr/local/share/air/logs/air.image.log
| /usr/local/bin/split -a 3 -d -b 2047m - /mnt/new/new/Test005-
Caine/test005-altFormat-caine.
dd: reading `/dev/sdc': Input/output error
80649+0 records in
5161536+0 records out
2642706432 bytes (2.6 GB) copied, 224.915 s, 11.7 MB/s
80649+1 records in
5161600+0 records out
2642739200 bytes (2.6 GB) copied, 248.058 s, 10.7 MB/s
2442185+2 records in
156299968+0 records out
80025583616 bytes (80 GB) copied, 6549.06 s, 12.2 MB/s
2442185+3 records in
156300032+0 records out
80025616384 bytes (80 GB) copied, 6572.11 s, 12.2 MB/s
2442185+4 records in
156300096+0 records out
80025649152 bytes (80 GB) copied, 6595.05 s, 12.1 MB/s
2442185+5 records in
156300160+0 records out
80025681920 bytes (80 GB) copied, 6617.97 s, 12.1 MB/s
2442185+6 records in
156300224+0 records out
80025714688 bytes (80 GB) copied, 6640.9 s, 12.1 MB/s
2442185+7 records in
156300288+0 records out
80025747456 bytes (80 GB) copied, 6663.92 s, 12.0 MB/s
2442185+8 records in
156300352+0 records out
80025780224 bytes (80 GB) copied, 6686.94 s, 12.0 MB/s
```

```
2442185+9 records in
156300416+0 records out
80025812992 bytes (80 GB) copied, 6709.94 s, 11.9 MB/s
2442185+10 records in
156300480+0 records out
80025845760 bytes (80 GB) copied, 6732.91 s, 11.9 MB/s
2442185+11 records in
156300544+0 records out
80025878528 bytes (80 GB) copied, 6755.86 s, 11.8 MB/s
2442185+12 records in
156300608+0 records out
80025911296 bytes (80 GB) copied, 6778.85 s, 11.8 MB/s
2442185+13 records in
156300672+0 records out
80025944064 bytes (80 GB) copied, 6801.85 s, 11.8 MB/s
2442185+14 records in
156300736+0 records out
80025976832 bytes (80 GB) copied, 6824.97 s, 11.7 MB/s
2442185+15 records in
156300800+0 records out
80026009600 bytes (80 GB) copied, 6847.97 s, 11.7 MB/s
2442185+16 records in
156300864+0 records out
80026042368 bytes (80 GB) copied, 6870.94 s, 11.6 MB/s
2442185+17 records in
156300928+0 records out
80026075136 bytes (80 GB) copied, 6893.95 s, 11.6 MB/s
2442185+18 records in
156300992+0 records out
80026107904 bytes (80 GB) copied, 6916.91 s, 11.6 MB/s
2442185+19 records in
156301056+0 records out
80026140672 bytes (80 GB) copied, 6939.82 s, 11.5 MB/s
2442190+21 records in
156296385+0 records out
80026370048 bytes (80 GB) copied, 6939.84 s, 11.5 MB/s
156296385+0 records in
156296385+0 records out
80026370048 bytes (80 GB) copied, 6940.26 s, 11.5 MB/s
Command completed: Sat Aug  7 19:37:09 NZST 2010
Start VERIFY: Sat Aug  7 19:37:09 NZST 2010
Command-line: cat /mnt/new/new/Test005-Caine/test005-altFormat-caine.* | air-counter 2>> /usr/local/share/air/logs/air.buffer.data | md5sum > /tmp/verify_hash.log
VERIFY SUCCESSFUL: Hashes match
Orig = d615c245f1124a2482a5d56ffa8a1c55
Copy = d615c245f1124a2482a5d56ffa8a1c55
Command completed: Sat Aug  7 19:54:02 NZST 2010
```

Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-02 PASSED AFR-03 PASSED ALOG-01 PASSED AFR-04 PASSED ALOG-02 PASSED AFR-05 PASSED ALOG-03 PASSED AFR-07 PASSED
Analysis:	Test achieved the expected Result.

3.13. TC-06-UNC

Test Case TC-06-UNC (AIR 2.0.0)		
Test & Case Summary	Acquire a digital source that has uncorrectable read errors Notes: 15 uncorrectable errors are existed	
Assertion:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AFR-08	The tool report to the user of the error type and the location of the error if error occurred during the reading from a digital source.
	AFR-09	If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-03	The tool reports to the user if an error occurs during the image creation process.
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device	
Drive Setup:	/dev/sdc: current max LBA: 156,301,488 /dev/sdc: native max LBA: 156,301,488 /dev/sdc: physical max LBA: 156,301,488 /dev/sdc: HPA not set	

	/dev/sdc: DCO not set Following sectors are marked as faulty: 5161564, 12135645, 16429701, 28210195, 33486075, 40694940, 40828560, 57691700, 90179820, 91800252, 92763320, 104129017, 109477200, 118026966, 140386491
Log highlights:	Start DC3DD (md5 sha1): Fri Aug 6 05:29:37 NZST 2010 command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sdc skip=0 conv=noerror,sync iflag=direct ibs=32768 compiled options: DEFAULT_BLOCKSIZE=32768 sector size: 512 (assumed) dc3dd: reading `/dev/sdc' at sector 5161564: Input/output error dc3dd: reading `/dev/sdc' at sector 12135645: Input/output error dc3dd: reading `/dev/sdc' at sector 16429701: Input/output error dc3dd: reading `/dev/sdc' at sector 28210195: Input/output error dc3dd: reading `/dev/sdc' at sector 33486075: Input/output error dc3dd: reading `/dev/sdc' at sector 40694940: Input/output error dc3dd: reading `/dev/sdc' at sector 40828560: Input/output error dc3dd: reading `/dev/sdc' at sector 57691700: Input/output error dc3dd: reading `/dev/sdc' at sector 90179820: Input/output error dc3dd: reading `/dev/sdc' at sector 91800252: Input/output error dc3dd: reading `/dev/sdc' at sector 92763320: Input/output error dc3dd: reading `/dev/sdc' at sector 104129017: Input/output error dc3dd: reading `/dev/sdc' at sector 109477200: Input/output error dc3dd: reading `/dev/sdc' at sector 118026966: Input/output error dc3dd: reading `/dev/sdc' at sector 140386491: Input/output error md5 TOTAL: 1b26c0e62b79f528793199a3d2de4034 sha1 TOTAL: 52bafa6d754870b33cb85089ae89538c9355844c **156301473+15 sectors in** **156301488+0 sectors out** Command completed: Fri Aug 6 06:58:17 NZST 2010 Start VERIFY: Fri Aug 6 06:58:17 NZST 2010 Command-line: cat /mnt/new/new/Test004-caine/test004-caine-UNC-error.* | air-counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1 hashlog=/tmp/verify_hash.log status=noxfer of=/dev/null VERIFY SUCCESSFUL: Hashes match Orig = md5 TOTAL: 1b26c0e62b79f528793199a3d2de4034 sha1 TOTAL: 52bafa6d754870b33cb85089ae89538c9355844c Copy = md5 TOTAL: 1b26c0e62b79f528793199a3d2de4034 sha1 TOTAL: 52bafa6d754870b33cb85089ae89538c9355844c Command completed: Fri Aug 6 07:29:08 NZST 2010
Results by assertion:	AFR-01 PASSED AIC-01 PASSED ALOG-01 PASSED AFR-02 PASSED AIC-02 PASSED ALOG-02 PASSED AFR-03 PASSED AIC-03 PASSED ALOG-03 PASSED AFR-04 PASSED AIC-05 PASSED AFR-05 PASSED AIC-06 PASSED AFR-07 PASSED AIC-07 PASSED AFR-08 PASSED AIC-08 PASSED AFR-09 PASSED
Analysis:	Test achieved the expected Result.

3.14. TC-07 & TC-08

Test Case TC-07-Insufficient space & TC-08 **(AIR 2.0.0)**	
Test & Case Summary:	TC-07 Attempt to create an image file where destination device has insufficient space TC-08 Attempt to create an image file where destination device has insufficient space, and see whether the tool offer the user another destination device to continue **Notes**: No partition in the source drive.
Assertions:	AFR-01 The tool accesses the digital source with a supported access interface AFR-02 The tool acquires a digital source AFR-03 The tool operates in an execution environment AFR-04 The tool creates an image file of the digital source AFR-05 The tool acquires all the visible data sectors from the digital source AFR-07 All data sectors acquired from the digital source are acquired accurately. AIC-01 The data represented by an image file is the same as the data acquired by the tool. AIC-02 The tool creates an image file according to the file format the user specified. AIC-04 The tool reports to the user if insufficient space in the destination device during the image creation process. AIC-05 If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller AIC-10 The tool reports to the user if insufficient space in the destination device to contain the multi-image file creation and if destination device switching function is supported, the image is continue on the selected destination device. ALOG-01 If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. ALOG-02 The tool display correct information about the acquisition to the user. ALOG-03 The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380811 AS (80GB) Serial Number: 6PS2CA4Z Sector count: 156,296,385 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdc: current max LBA: 156,296,385 /dev/sdc: native max LBA: 156,296,385 /dev/sdc: physical max LBA: 156,296,385 /dev/sdc: HPA not set /dev/sdc: DCO not set
Log highlights:	Start DC3DD (md5 sha512): Wed Jul 14 04:38:50 NZST 2010 command line: dc3dd hash=md5,sha512 hashlog=/tmp/hash.log status=noxfer if=/dev/sdd skip=0 conv=noerror,sync iflag=direct ibs=32768 compiled options: DEFAULT_BLOCKSIZE=32768 sector size: 512 (assumed) Start VERIFY: Wed Jul 14 04:38:54 NZST 2010 Command-line: cat /media/DATA/Test Imges space/test007_nospace.dd.* | air-counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha512 hashlog=/tmp/verify_hash.log status=noxfer of=/dev/null VERIFY FAILED: Hashes don't match

	Orig = Copy = md5 TOTAL: d41d8cd98f00b204e9800998ecf8427e sha512 TOTAL: cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e Command completed: Wed Jul 14 04:38:57 NZST 2010
Results by assertion:	**TC-07-InsufficientSpace** AFR-01 PASSED ALOG-01 PASSED AFR-02 PASSED ALOG-02 PASSED AFR-03 PASSED ALOG-03 PASSED AFR-04 PASSED AIC-04 **FAILED** **TC-08** AFR-01 PASSED AIC-04 **FAILED** ALOG-01 PASSED AFR-02 PASSED AIC-05 PASSED ALOG-02 **FAILED** AFR-03 PASSED AIC-10 **FAILED** ALOG-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 FAILED
Analysis:	Test result **FAILED**. Does not support space checking prior disk imaging. Imaging will stop also immediately after it starts. **TC-07** AIR imager does not report to the user that insufficient space in the destination device during the image creation process. **TC-08** AIR imager does not offer alternate destination device to continue disk imaging when destination device has insufficient space.

3.15. TC-12-01 Partially Hidden by HPA

Test Case TC-12-01 Partially Hidden by HPA (AIR 2.0.0)	
Test & Case Summary:	Acquire a partition that is partially or completely hidden by HPA or DCO **Notes**: FAT32 partition has been partially hidden by HPA from 150301488 to 156301487. Total acquired 377,005,056 bytes same as FTK imager. Nature of the error is not reported.
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-06** The tool acquires all the hidden data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the

	image file has been changed if the image file has been changed.
AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
AHS-01	The tool reports to the user if any hidden sectors are found
AHS-02	The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment
AHS-03	The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment

Source Device:

Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: N/A

Drive Setup:

Source hashes
MD5 checksum: 554357b44e0334f254e80ab537a299c7
SHA1 checksum: aa314705b7addb0bf230974b30967fa74082f490
/dev/sdb: current max LBA: 150,301,484
/dev/sdb: native max LBA: 150,301,484
/dev/sdb: physical max LBA: **156,301,488**
/dev/sdb: **HPA set from sector 150,301,488 to 156,301,487 (Total 736,388 sectors)**

Partition Table:

Device	**Start**	**End**	**#sectors**	**File System**
/dev/sdb1	63	2104514	2104452	NTFS
/dev/sdb2	2104515	149565149	145460535	Ext3
/dev/sdb3	149565150	156296384	6731234	FAT32 **(Partially HPA)**

Log highlights:

```
Start DC3DD (md5 sha1): Wed Sep  1 00:26:35 NZST 2010
Command-line:
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer
if=/dev/sda3 skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
md5 TOTAL: 554357b44e0334f254e80ab537a299c7
sha1 TOTAL: aa314705b7addb0bf230974b30967fa74082f490
736338+0 sectors in
736338+0 sectors out
dc3dd completed at 2010-09-01 00:26:53 +1200
Command completed: Wed Sep  1 00:26:56 NZST 2010

Start VERIFY: Wed Sep  1 00:26:56 NZST 2010
Command-line: cat /mnt/new/Image/partition_part_HPA.* | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
```

	VERIFY SUCCESSFUL: Hashes match Orig = md5 TOTAL: 554357b44e0334f254e80ab537a299c7 sha1 TOTAL: aa314705b7addb0bf230974b30967fa74082f490 Copy = md5 TOTAL: 554357b44e0334f254e80ab537a299c7 sha1 TOTAL: aa314705b7addb0bf230974b30967fa74082f490 Command completed: Wed Sep 1 00:27:06 NZST 2010
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. AIR failed to detect and acquire the hidden areas in the hard drive. Dc3dd command line option has the ability of detect Hidden areas.

3.16. TC-12-02 Completely Hidden by HPA

Test Case TC-12-02 Completely Hidden by HPA (AIR 2.0.0)	
Test & Case Summary:	Acquire a partition that is partially or completely hidden by HPA or DCO **Notes**: FAT32 partition has been completely hidden by HPA from 149565150 to 156301487.
Assertion:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-06** The tool acquires all the hidden data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-05** If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller **AIC-06** If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed. **AIC-07** If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed. **AIC-08** If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported **AHS-01** The tool reports to the user if any hidden sectors are found

	AHS-02 The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment **AHS-03** The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: N/A
Drive Setup:	/dev/sdb: current max LBA: 149,565,150 /dev/sdb: native max LBA: 149,565,150 /dev/sdb: physical max LBA: **156,301,488** /dev/sdb: **HPA set from sector 149,565,150 to 156,301,487 (Total 6,736,337 sectors)**

Partition Table:

Device	**Start**	**End**	**#sectors**	**File System**
/dev/sdb1	63	2104514	2104452	NTFS
/dev/sdb2	2104515	149565149	145460535	Ext3
/dev/sdb3	149565150	156296384	6731234	FAT32 **(Entire HPA)**

Log highlights:

```
Start DC3DD (md5 sha1): Wed Sep  1 02:36:13 NZST 2010
dc3dd hash=md5,sha1  hashlog=/tmp/hash.log status=noxfer if=/dev/sda3
skip=0 conv=noerror,sync iflag=direct ibs=32768 2>>
/usr/local/share/air/logs/air.image.log | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | /usr/local/bin/split -a 3 -d -b 2047m -
/mnt/new/Image/partition_whole_HPA. >>
/usr/local/share/air/logs/air.image.log 2>&1
dc3dd: opening `/dev/sda3': No such file or directory
Command completed: Wed Sep  1 02:36:16 NZST 2010

Start VERIFY: Wed Sep  1 02:36:16 NZST 2010
Command-line: cat /mnt/new/Image/partition_whole_HPA.* | air-counter
2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY FAILED: Hashes don't match
Orig =
Copy = md5 TOTAL: d41d8cd98f00b204e9800998ecf8427e
sha1 TOTAL: da39a3ee5e6b4b0d3255bfef95601890afd80709
Command completed: Wed Sep  1 02:36:19 NZST 2010
```

Results by assertion:

AFR-01 PASSED
AFR-02 PASSED
AFR-03 PASSED
AFR-04 PASSED
AFR-05 PASSED
AFR-06 **FAILED**
AFR-07 PASSED
AIC-01 PASSED
AIC-02 PASSED
AIC-05 PASSED
AIC-06 PASSED
AIC-07 PASSED
AIC-08 PASSED
AHS-01 **FAILED**
AHS-02 **FAILED**
AHS-03 **FAILED**
ALOG-01 PASSED
ALOG-02 PASSED
ALOG-03 PASSED

Analysis: Test **FAILED** to achieve the expected Result. AIR failed to detect and acquire the hidden areas in the hard drive. AIR stopped immediately when attempting to acquire the hidden partition and indicated no such file or directory in the partition.

3.17. TC-13 Overlapping Partitions

<table>
<tr><th colspan="2">Test Case TC-13 Overlapping Partitions (AIR 2.0.0)</th></tr>
<tr><td>Test & Case Summary:</td><td>TC-13 Acquire a partition that is overlapping with another partition
Notes: Partitions are overlapped. The last NTFS partition started before the end of the last partition. Starting sector changed from 79,168,320 to 79,100,000.</td></tr>
<tr><td>Assertions:</td><td><table>
<tr><td>AFR-01</td><td>The tool accesses the digital source with a supported access interface</td></tr>
<tr><td>AFR-02</td><td>The tool acquires a digital source</td></tr>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-04</td><td>The tool creates an image file of the digital source</td></tr>
<tr><td>AFR-05</td><td>The tool acquires all the visible data sectors from the digital source</td></tr>
<tr><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-01</td><td>The data represented by an image file is the same as the data acquired by the tool</td></tr>
<tr><td>AIC-02</td><td>The tool creates an image file according to the file format the user specified.</td></tr>
<tr><td>AIC-11</td><td>The tool reports to the user if any irregularities found in the digital source.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table></td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>Source Hashes:
md5: 3170cec7e6720af973cc37a946c32ae3
sha1: 6366ad8cd563c05f086dfe7b7884b08fd9795069
/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set</td></tr>
<tr><td>Partition Table:</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>63</td><td>20980764</td><td>20980827</td><td>NTFS</td></tr>
<tr><td>/dev/sdb2</td><td>20980890</td><td>79168320</td><td>58187430</td><td>Ext3</td></tr>
<tr><td>/dev/sdb3</td><td>79100000</td><td>156296385</td><td>77128065</td><td>NTFS (Modified)</td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Start DC3DD (md5 sha1): Wed Sep 8 06:58:56 NZST 2010
dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sdb skip=0 conv=noerror,sync iflag=direct ibs=32768
md5 TOTAL: 3170cec7e6720af973cc37a946c32ae3
sha1 TOTAL: 6366ad8cd563c05f086dfe7b7884b08fd9795069
156301488+0 sectors in
156301488+0 sectors out
Command completed: Wed Sep 8 08:20:42 NZST 2010

Start VERIFY: Wed Sep 8 08:20:42 NZST 2010
Command-line: cat /mnt/new/Image/caine-overlapPartition.* | air-counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1 hashlog=/tmp/verify_hash.log status=noxfer of=/dev/null</td></tr>
</table>

	VERIFY SUCCESSFUL: Hashes match Orig = md5 TOTAL: 3170cec7e6720af973cc37a946c32ae3 sha1 TOTAL: 6366ad8cd563c05f086dfe7b7884b08fd9795069 Copy = md5 TOTAL: 3170cec7e6720af973cc37a946c32ae3 sha1 TOTAL: 6366ad8cd563c05f086dfe7b7884b08fd9795069 Command completed: Wed Sep 8 09:20:51 NZST 2010
Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-11 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. AIR fails to report to the user that irregularities in the digital source.

3.18. TC-14 Partition out of boundary

Test Case TC-14 Partition out of boundary (AIR 2.0.0)	
Test & Case Summary:	Acquire a hard disk with a partition's end address ended outside the physical boundary **Notes**: Partitions ended out of the physical boundary of the disk. The last partition end sector **changed from 72,331,264 to 72,380,000**.
Assertions:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AIC-01** The data represented by an image file is the same as the data acquired by the tool **AIC-02** The tool creates an image file according to the file format the user specified. **AIC-11** The tool reports to the user if any irregularities found in the digital source. **ALOG-01** If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file. **ALOG-02** The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition. **ALOG-03** The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA and DCO are not set

Partition Table:	**Device** **Start** **End** **#sectors** **File System** /dev/sdb1 2048 40962047 40960000 NTFS /dev/sdb2 40962048 83970047 43008000 Ext4 /dev/sdb3 83972096 **156350047** 72377951 Extended **(Modified)**
Log highlights:	Start DC3DD (md5 sha1): Fri Sep 10 05:02:41 NZST 2010 command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sdc skip=0 conv=noerror,sync iflag=direct ibs=32768 sector size: 512 (assumed) md5 TOTAL: b42f526d394078656308a9b96aa77188 sha1 TOTAL: e2977a0cd2d2608519b1750e980252d01cdb4718 156301488+0 sectors in 156301488+0 sectors out Command completed: Fri Sep 10 06:31:40 NZST 2010 Start VERIFY: Fri Sep 10 06:31:40 NZST 2010 Command-line: cat /mnt/new/Image/PartitionOutOfBound.* | air-counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1 hashlog=/tmp/verify_hash.log status=noxfer of=/dev/null VERIFY SUCCESSFUL: Hashes match Orig = md5 TOTAL: b42f526d394078656308a9b96aa77188 sha1 TOTAL: e2977a0cd2d2608519b1750e980252d01cdb4718 Copy = md5 TOTAL: b42f526d394078656308a9b96aa77188 sha1 TOTAL: e2977a0cd2d2608519b1750e980252d01cdb4718 Command completed: Fri Sep 10 07:31:37 NZST 2010
Results by assertion:	AFR-01 PASSED AIC-01 PASSED AFR-02 PASSED AIC-02 PASSED AFR-03 PASSED AIC-11 **FAILED** AFR-04 PASSED ALOG-01 PASSED AFR-05 PASSED ALOG-02 PASSED AFR-07 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. AIR fails to report to the user that irregularities in the digital source.

3.19. TC-15 Unreadable MBR

Test Case TC-15 Unreadable MBR (AIR 2.0.0)	
Test & Case Summary:	Acquire a hard disk with an unreadable MBR **Notes:** Partitions ended out of the physical boundary of the disk. Data of MBR is replaced by value 0.
Assertions:	**AFR-01** The tool accesses the digital source with a supported access interface **AFR-02** The tool acquires a digital source **AFR-03** The tool operates in an execution environment **AFR-04** The tool creates an image file of the digital source **AFR-05** The tool acquires all the visible data sectors from the digital source **AFR-07** All data sectors acquired from the digital source are acquired accurately. **AFR-08** The tool reports to the user of the error type and the location of the error if

		error occurred during the reading from a digital source.
	AFR-09	If there are unresolved errors reading from a digital source, then the tool uses a benign fill in the destination object in place of the inaccessible data.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-03	The tool reports to the user if an error occurs during the image creation process.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	AIC-11	The tool reports to the user if any irregularities found in the digital source.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported

Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA and DCO are not set

Partition Table:

Device	**Start**	**End**	**#sectors**	**File System**
/dev/sdb1	2048	40962047	40960000	NTFS
/dev/sdb2	40962048	83970047	43008000	Ext4
/dev/sdb3	83972096	156301311	72329125	Extended

Log highlights:

```
Start DC3DD (md5 sha1): Mon Sep 13 18:34:06 NZST 2010
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer
if=/dev/sdc skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
md5 TOTAL: 2ab63e47f402406afed31dad063df7f8
sha1 TOTAL: d337f09ba2b9069668c70a14a2fc87a3b21a5887
156301488+0 sectors in
156301488+0 sectors out
dc3dd completed at 2010-09-13 19:56:20 +1200
Command completed: Mon Sep 13 19:56:24 NZST 2010

Start VERIFY: Mon Sep 13 19:56:24 NZST 2010
Command-line: cat /mnt/new/Image/Caine_UnReadableMBR.* | air-counter
2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1
```

```
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 2ab63e47f402406afed31dad063df7f8
sha1 TOTAL: d337f09ba2b9069668c70a14a2fc87a3b21a5887
Copy = md5 TOTAL: 2ab63e47f402406afed31dad063df7f8
sha1 TOTAL: d337f09ba2b9069668c70a14a2fc87a3b21a5887
Command completed: Mon Sep 13 20:56:54 NZST 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED	AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AIC-11 **FAILED**	ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected Result. No notification of irregularity of the partition table.		

3.20. TC-16-01 Acquire a Single GUID Partition

Test Case TC-16-01Acquire a Single GUID Partition (AIR 2.0.0)		
Test & Case Summary:	Acquire a Single GUID Partition **Notes**: Hard drive partitioned as GPT disk. 6 partitions are created.	
Assertions:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488	

	Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device
Drive Setup:	/dev/sdb: current max LBA: 156,301,488 /dev/sdb: native max LBA: 156,301,488 /dev/sdb: physical max LBA: 156,301,488 /dev/sdb: HPA and DCO are not set

Partition Table (GPT disk):

Device	**Start**	**End**	**#sectors**	**File System**
/dev/sdb1	34	262110	262144	Microsoft Reserved
/dev/sdb2	264192	8652799	8388608	NTFS
/dev/sdb3	8652800	12847103	4194304	NTFS
/dev/sdb4	**12847104**	**14944255**	**2097152**	**NTFS**
/dev/sdb5	14944256	25380863	10436608	NTFS
/dev/sdb6	25380864	156299264	130918400	NTFS

Log highlights:

```
Start DC3DD (md5 sha1): Fri Sep 17 20:14:18 NZST 2010
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer
if=/dev/sdc4 skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
md5 TOTAL: 68fd8aa6e64b5f7fb7cd02e5444f14a1
sha1 TOTAL: 249dcfa032899d4f1a04c37c7c4621b3b05cebac
2097152+0 sectors in
2097152+0 sectors out
dc3dd completed at 2010-09-17 20:15:23 +1200
Command completed: Fri Sep 17 20:15:26 NZST 2010
Start VERIFY: Fri Sep 17 20:15:26 NZST 2010
Command-line: cat /mnt/Image/AIR_GUID_Partition.* | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null

VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 68fd8aa6e64b5f7fb7cd02e5444f14a1
sha1 TOTAL: 249dcfa032899d4f1a04c37c7c4621b3b05cebac
Copy = md5 TOTAL: 68fd8aa6e64b5f7fb7cd02e5444f14a1
sha1 TOTAL: 249dcfa032899d4f1a04c37c7c4621b3b05cebac
Command completed: Fri Sep 17 20:15:46 NZST 2010
```

Results by assertion:

AFR-01 PASSED	AIC-01 PASSED	ALOG-01 PASSED
AFR-02 PASSED	AIC-02 PASSED	ALOG-02 PASSED
AFR-03 PASSED	AIC-05 PASSED	ALOG-03 PASSED
AFR-04 PASSED	AIC-06 PASSED	
AFR-05 PASSED	AIC-07 PASSED	
AFR-07 PASSED	AIC-08 PASSED	

Analysis: Test **achieved** expected result.

3.21. TC-16-02 Acquire a GPT disk

<table>
<tr><th colspan="2">Test Case TC-16-02 Acquire a GPT disk (AIR 2.0.0)</th></tr>
<tr><td>Test & Case Summary:</td><td>Acquire a GPT disk
Notes: Hard drive partitioned as GPT disk. 6 partitions are created.</td></tr>
<tr><td>Assertions:</td><td><table>
<tr><td>AFR-01</td><td>The tool accesses the digital source with a supported access interface</td></tr>
<tr><td>AFR-02</td><td>The tool acquires a digital source</td></tr>
<tr><td>AFR-03</td><td>The tool operates in an execution environment</td></tr>
<tr><td>AFR-04</td><td>The tool creates an image file of the digital source</td></tr>
<tr><td>AFR-05</td><td>The tool acquires all the visible data sectors from the digital source</td></tr>
<tr><td>AFR-07</td><td>All data sectors acquired from the digital source are acquired accurately.</td></tr>
<tr><td>AIC-01</td><td>The data represented by an image file is the same as the data acquired by the tool</td></tr>
<tr><td>AIC-02</td><td>The tool creates an image file according to the file format the user specified.</td></tr>
<tr><td>AIC-05</td><td>If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller</td></tr>
<tr><td>AIC-06</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.</td></tr>
<tr><td>AIC-07</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.</td></tr>
<tr><td>AIC-08</td><td>If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.</td></tr>
<tr><td>ALOG-01</td><td>If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.</td></tr>
<tr><td>ALOG-02</td><td>The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
</table></td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device</td></tr>
<tr><td>Drive Setup:</td><td>/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set</td></tr>
<tr><td>Partition Table (GPT disk):</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>34</td><td>262110</td><td>262144</td><td>Microsoft Reserved</td></tr>
<tr><td>/dev/sdb2</td><td>264192</td><td>8652799</td><td>8388608</td><td>NTFS</td></tr>
<tr><td>/dev/sdb3</td><td>8652800</td><td>12847103</td><td>4194304</td><td>NTFS</td></tr>
<tr><td>/dev/sdb4</td><td>12847104</td><td>14944255</td><td>2097152</td><td>NTFS</td></tr>
<tr><td>/dev/sdb5</td><td>14944256</td><td>25380863</td><td>10436608</td><td>NTFS</td></tr>
<tr><td>/dev/sdb6</td><td>25380864</td><td>156299264</td><td>130918400</td><td>NTFS</td></tr>
</table></td></tr>
<tr><td>Log highlights:</td><td>Start DC3DD (md5 sha1): Fri Sep 17 17:48:35 NZST 2010
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sdc skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)</td></tr>
</table>

```
md5 TOTAL: 7a84a94aae46d34ac61dc26800f6dd19
sha1 TOTAL: f913fd6832de537c78dc4da881281984daed37f5
156301488+0 sectors in
156301488+0 sectors out
Command completed: Fri Sep 17 19:09:48 NZST 2010
Start VERIFY: Fri Sep 17 19:09:48 NZST 2010
Command-line: cat /mnt/Image/AIR_GUID_Whole.* | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null

VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 7a84a94aae46d34ac61dc26800f6dd19
sha1 TOTAL: f913fd6832de537c78dc4da881281984daed37f5
Copy = md5 TOTAL: 7a84a94aae46d34ac61dc26800f6dd19
sha1 TOTAL: f913fd6832de537c78dc4da881281984daed37f5
Command completed: Fri Sep 17 20:10:02 NZST 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-07 PASSED	AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED	ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **achieved** expected result.		

3.22. TC-17 Acquire a partially hidden GPT Partition

Test Case TC-17 Acquire a partially hidden GPT Partition (AIR 2.0.0)		
Test & Case Summary:	Acquire a partially hidden GPT Partition	
Assertions:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-06	The tool acquires all the hidden data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-	The tool display correct information about the acquisition to the user. The

<table>
<tr><td></td><td><table>
<tr><td>02</td><td>information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.</td></tr>
<tr><td>ALOG-03</td><td>The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported</td></tr>
<tr><td>AHS-01</td><td>The tool reports to the user if any hidden sectors are found</td></tr>
<tr><td>AHS-02</td><td>The tool reports to the user that digital source may contain hidden sector but undetected if the tool is unable to determine whether hidden sectors are present due to incompatible execution environment</td></tr>
<tr><td>AHS-03</td><td>The tool reports to the user that hidden sectors will not be acquired if the tool is unable to acquire hidden sectors due to incompatible execution environment</td></tr>
</table></td></tr>
<tr><td>Source Device:</td><td>Drive Model: ST380817AS (80GB)
Serial Number: 5MR18V18
Sector count: 156,301,488
Write blocker: N/A</td></tr>
<tr><td>Drive Setup:</td><td>/dev/sdb: current max LBA: 156,301,488
/dev/sdb: native max LBA: 156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA set from sector 6,500,001 to 156,301,487 (Total 149,801,488 sectors are hidden)</td></tr>
<tr><td>Partition Table (GPT disk):</td><td><table>
<tr><th>Device</th><th>Start</th><th>End</th><th>#sectors</th><th>File System</th></tr>
<tr><td>/dev/sdb1</td><td>2048</td><td>4198399</td><td>4196352</td><td>FAT32</td></tr>
<tr><td>/dev/sdb2</td><td>4198400</td><td>6297599</td><td>2099200</td><td>EXT4</td></tr>
<tr><td>/dev/sdb3</td><td>6301488</td><td>156305199</td><td>150003712</td><td>NTFS (Partially HPA)</td></tr>
</table></td></tr>
</table>

Log highlights:

```
Start DC3DD (md5 sha1): Mon Oct 18 05:48:27 NZDT 2010
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer
if=/dev/sda skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
md5 TOTAL: 66b09a0f6194157cbd492b16c58e9900
sha1 TOTAL: cab5ec0c50fd232bcce40fa71deaaeb83b7af675
6500000+0 sectors in
6500000+0 sectors out
Command completed: Mon Oct 18 05:51:00 NZDT 2010
Start VERIFY: Mon Oct 18 05:51:00 NZDT 2010
Command-line: cat /mnt/new/AIR_GPThpa.* | air-counter 2>>
/usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1
hashlog=/tmp/verify_hash.log  status=noxfer of=/dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 66b09a0f6194157cbd492b16c58e9900
sha1 TOTAL: cab5ec0c50fd232bcce40fa71deaaeb83b7af675
Copy = md5 TOTAL: 66b09a0f6194157cbd492b16c58e9900
sha1 TOTAL: cab5ec0c50fd232bcce40fa71deaaeb83b7af675
Command completed: Mon Oct 18 05:53:36 NZDT 2010
```

Results by assertion:	AFR-01 PASSED AFR-02 PASSED AFR-03 PASSED AFR-04 PASSED AFR-05 PASSED AFR-06 **FAILED** AFR-07 PASSED AIC-01 PASSED AIC-02 PASSED AIC-05 PASSED AIC-06 PASSED AIC-07 PASSED AIC-08 PASSED AHS-01 **FAILED** AHS-02 **FAILED** AHS-03 **FAILED** ALOG-01 PASSED ALOG-02 PASSED ALOG-03 PASSED
Analysis:	Test **FAILED** to achieve the expected result. HPA area was not detected and acquired. However, the visible sectors were acquired accurately and completely.

3.23. TC-18 Network Image Acquisition

Test Case TC-18 Network Image Acquisition (AIR 2.0.0)		
Test & Case Summary:	Network Image Acquisition	
Assertions:	**AFR-01**	The tool accesses the digital source with a supported access interface
	AFR-02	The tool acquires a digital source
	AFR-03	The tool operates in an execution environment
	AFR-04	The tool creates an image file of the digital source
	AFR-05	The tool acquires all the visible data sectors from the digital source
	AFR-07	All data sectors acquired from the digital source are acquired accurately.
	AIC-01	The data represented by an image file is the same as the data acquired by the tool
	AIC-02	The tool creates an image file according to the file format the user specified.
	AIC-05	If multi-file image creation and the image file size is selected, the tool creates a multi-file image except that one file may be smaller
	AIC-06	If the image file integrity check is selected, the tool shall report to the user the image file has not been changed if the image file has not been changed.
	AIC-07	If the image file integrity check is selected, the tool shall report to the user the image file has been changed if the image file has been changed.
	AIC-08	If the image file integrity check is selected, the tool shall report to the user the image file has been changed and the involved location if the image file has been changed.
	ALOG-01	If the tool logs any information regarding to the acquisition, the information is accurately logged in the log file.
	ALOG-02	The tool display correct information about the acquisition to the user. The information about the acquisition at least including following: device, start sector, end sector, type and number of errors encountered, and start time and end time of acquisition.
	ALOG-03	The tool display correct information regarding to the acquisition to the user and the information displayed is consistent with the log file if the log file function is supported
Source Device:	Drive Model: ST380817AS (80GB) Serial Number: 5MR18V18 Sector count: 156,301,488 Write blocker: Tableau Forensic SATA/IDE Bridge IEEE 1394 SBP2 Device	
Drive Setup:	Source Hashes: MD5 d48a1018a5fbb72b40d36da51e396eb3 SHA1 37350ce8c4f21a07fac3ac625e43d8e6d0c99878	

```
/dev/sdb: current max LBA:   156,301,488
/dev/sdb: native max LBA:     156,301,488
/dev/sdb: physical max LBA: 156,301,488
/dev/sdb: HPA and DCO are not set
```

Partition Table:

Device	Start	End	#sectors	System
/dev/sdb1	63	2104514	2104452	FAT32
/dev/sdb2	2104515	6297479	4192965	NTFS
/dev/sdb3	6297480	156296384	149998905	NTFS

Log highlights:

```
Start DC3DD (md5 sha1): Sun Oct 17 16:32:52 NZDT 2010
Hash will be calculated on port:5058.
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer
of=/root/AIR_Network seek=0 obs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
md5 TOTAL: 14d2c1027467bc11c8405c0ff961f2e4
sha1 TOTAL: 583d77bf05a1b12600eaa4100b740459dda34308
2104452+0 sectors in
2104452+0 sectors out
Command completed: Sun Oct 17 16:36:23 NZDT 2010
Start VERIFY: Sun Oct 17 16:36:23 NZDT 2010
Command-line: dc3dd if=/root/AIR_Network hash=md5,sha1
conv=noerror,sync hashlog=/tmp/verify_hash.log status=noxfer | air-counter
2>> /usr/local/share/air/logs/air.buffer.data > /dev/null
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 14d2c1027467bc11c8405c0ff961f2e4
          sha1 TOTAL: 583d77bf05a1b12600eaa4100b740459dda34308
Copy = md5 TOTAL: 14d2c1027467bc11c8405c0ff961f2e4
           sha1 TOTAL: 583d77bf05a1b12600eaa4100b740459dda34308
Command completed: Sun Oct 17 16:36:44 NZDT
```

Results by assertion:

AFR-01 PASSED
AFR-02 PASSED
AFR-03 PASSED
AFR-04 PASSED
AFR-05 PASSED
AFR-07 PASSED

AIC-01 PASSED
AIC-02 PASSED
AIC-05 PASSED
AIC-06 PASSED
AIC-07 PASSED
AIC-08 PASSED

ALOG-01 PASSED
ALOG-02 PASSED
ALOG-03 PASSED

Analysis: Test **achieved** expected result.