UNIVERSITY OF CENTRAL OKLAHOMA

Edmond, Oklahoma

Jackson College of Graduate Studies

Current State of Validation and Testing of Digital Forensic Tools in the United States

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

In partial fulfillment of the requirements

For the degree of

MASTER OF SCIENCE IN FORENSIC SCIENCE

By

Megan L. Dorman

Edmond, Oklahoma

2012

Current State of Validation and Testing of Digital Forensic Tools in the United States

By: Megan Lynn Dorman

A THESIS

APPROVED FOR THE W. ROGER WEBB FORENSIC SCIENCE INSTITUTE

June 2012

By _____

Dr. Mark R. McCoy Committee Chair

_____

Dr. Wayne D. Lord Committee Member

_____

Dr. John P. Mabry Committee Member

TABLE OF CONTENTS

TABLE OF FIGURES

Abstract

The Federal courts' decision in Dauber v. Merrell Dow Pharmaceutical, Inc. (1993) requires forensic testing protocols and tools to be validated and tested for reliability before they can be used to support expert witness testimony. Digital forensic labs and individual examiners in the United States should be performing their own validation and verification tests on their digital forensic tools. The Scientific Working Group of Digital Evidence (SWDGE) recommends that examiners perform validation testing whenever there are new, revised, or reconfigured tools, techniques, or procedures.

This study surveyed digital forensics examiners in the U.S. to provide a description of the current state of validation and testing of digital forensic tools, current protocols used for validation, and barriers to performing these tests. The findings included, 95% validate and test their Digital Forensic tools. 80.3% document the validation and testing process and their results. 53.6% validate and test each function if the forensic tool performs several different functions. Examiners should test their digital forensic tools to make sure they are working properly and receiving accurate results. The findings and testimony can be dismissed in court if the examiner is not following set standards.

Introduction

Digital Forensics is a growing field in forensic science. There are many subfields which stem from digital forensics, such as computer forensics, network forensics, database forensics, data recovery, and disaster recovery. Digital forensics is quickly expanding and research is needed, especially information detailing the validation and verification processes. Previously there was not research that included information about the current state of the validation and verification testing process in the United States. This research is necessary because this field is of enormous importance and crucial to the forensic community and law enforcement. It is essential to digital forensics that practices and protocols of digital forensics labs be observed, examined, and documented.

Digital forensics has unique problems, which cause difficulties for its acceptance as an accredited science. Research and accreditation in digital evidence is an increasing necessity and concern. Accreditation requires documentation and publication, which is lacking in the digital forensic field. In some cases, research and publications exist, but they are not available to the public. This unavailability may be due to companies keeping their testing process, research, and documentation of their software secret. Some digital forensic software companies worry about their competitor companies copying their work, so they do not release documentation for their software. Companies may also keep them secret to keep "criminals" from defeating them. This unpublished documentation could be helpful for the digital examiners' testing and documentation process. Publishing documentation would improve and contribute to the lack of publications and information in the digital evidence field. For the advancement of the digital forensic field, it is necessary to have research and publications on the accuracy, reliability, and validity of the digital forensic tools used to conduct examinations.

Verification and validation are key factors for the testing process. Using a combination of these processes in a set procedure or protocol is needed to achieve accreditation. Understanding the meaning and definition of verification and validation is necessary for the comprehension of this process. Wilsdon and Slay (2005) explain that verification is 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.3). Simply, verification is the practice of making sure that the tool is doing what it is supposed to be doing. If the tool states that it checks certain areas of a drive and then moves to a next step, examiners want to make sure it is actually performing the task it says it does. The other key phase of the process is validation. Beckett and Slay (2007) explain that validation is the process of evaluating a system or component during or at the end of the development process to determine whether it satisfies requirements. The process of providing evidence that the software and its associated products satisfy system requirements allocated to software at the end of each life cycle activity solves the right problem and satisfies intended use and user needs (p.2). Intended use could be that it finds hidden files. Validation is the step in which the examiner ensures that the tool is producing the expected results.

On July 26, 2012, the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) reported that there are 389 crime laboratories that they have accredited. These labs are divided up by 193 state laboratories, 133 local agency laboratories, 23 federal laboratories, 17 international laboratories (outside of the United States), and 23 private laboratories. Under the International Testing Program, there are 225 accredited crime laboratories. Under the International Calibration Program, 6 crime laboratories are accredited. There are also 158 crime laboratories that are accredited under the Legacy Program (American

Society of Crime Laboratory Directors Laboratory Accreditation Board, 2012). Australia adopted the International Organization for Standardization 17025E (ISO 17025E) standards (Guo, Slay, & Beckeet, 2009).

Beckett and Slay (2007) stated:

> Internal standard ISO 17025 specifies general requirements for the competence to carry out test and calibrations. It encompasses testing and calibrations performed by the laboratory using standard methods, non-standard methods, and laboratory-developed methods. Some of the requirements for a laboratory to meet include Management requirements, Document Control, Subcontracting tests and calibrations, Service to the customer, Corrective action, Prevention actions, internal audits, and measurement traceability just to name a few (p.2).

Document control guarantees documents are filled out fully and properly and states what documents are kept and which are discarded from the lab. Corrective action is when equipment has an issue that needs to be fixed or when an examiner may be performing a test incorrectly. Preventative actions are intended to make sure accidents and problems do not arise in the labs. All of these requirements are essential and should be adopted as standards for the United States.

In the United States, Scientific Working Group on Digital Evidence (SWGDE), a group of digital forensic examiners, is currently working on the validation and verification process. This group recognizes the need for the organization of the process and accreditation. SWGDE (2009) states that it "brings together organizations actively engaged in the field of digital and multimedia evidence, to foster communication and cooperation as well as ensuring quality and consistency within the forensic community" (p.1). Building accreditation for this scientific field

is especially critical. This inability to conduct a proper validation test could cause issues and concerns in court cases asking about the accuracy of testing, the validation process, and the software program.

SWGDE states that when performing individual test scenarios, there must be documentation and a summary report. The report should include the overall pass/fail status of the tool, technique, or procedure, along with any recommendation, concerns, and etcetera. (Evidence, Scientific Working Group on Digital Evidence, 2009, p. 7). It is critical to keep detailed documentation when testing tools. This documentation will give information on the examination and could help find faults with the tools.

Bianchi and Pollitt (2006) also suggest that the final report should contain enough detail and information that another examiner could perform the examination and get the same results (p.84). If the information provided is faulty or tampered with, it needs to be stated and portrayed accurately. Documentation will also help the examiner, who becomes the expert, during the trial. This documentation is a reminder of what exactly was performed and the results from the testing. Bianchi and Pollitt (2006) reported that expert testimony must be given in a way that everyone, including people with no digital evidence experience, will understand the process and results (p.80). Clear information and results should be presented during court proceedings, so the jury has enough knowledge and understanding of the process to make an informed decision. If the jury members do not understand or are confused, they may disregard the evidence.

Before use in actual criminal, civil, or administrative cases, testing and validation needs to be performed on Digital Forensic tools used in the examination. Digital forensics is used in legal cases in which a crime has been committed on or with a piece of digital media. Digital

devices can be the target of a crime, an instrument used in a crime, and/or the place that evidence is stored. A case that has helped set standards in many scientific fields in regards to testimony and evidence is Daubert vs. Merrell Dow Pharmaceuticals, Inc., 509U.S. 113 S. Ct. 2786, L. Ed. 2d 469 (1993) (Feder & Houck, 2008, p. 132). This was a monumental case about the admissibility of scientific expert testimony in federal court. In this case, pregnant women took Benedictin, an antinausea medicine, and stated that their children suffered birth defects. Before this incident, there was no previous link to birth defects and Benedictin. The plaintiffs brought eight credible experts who stated that this drug could cause birth defects. The district court found their evidence to be inadmissible because the scientific technique was not generally accepted (Scribner, 2008, p. 85). This case is influential because eight credible experts' opinions were disregarded because their techniques were not accepted. If the experts' evidence had been accepted, then the case may have had a different outcome.

The "Daubert Standards" were formed from the Dauber v. Merrell Dow Pharmaceutical, Inc., 509U.S. 113 S. Ct. 2786, L. Ed. 2d 469 (1993) case and include Rule 104(a) from the U.S. Supreme Court. Rule 104(a) states that there are four standards for checking the admissibility and accuracy of information or data. The standards that should be checked are whether the procedure or technique has been published, if the procedure is generally accepted, whether the procedure has been or can be tested, and what error rate the procedure carries. (Johnson, 2006, p. 27). It is imperative that results are accurate when looking at the validation and verification process. When building accreditation, Daubert's standards for admissibility in court must be met, this can be difficult for most digital forensic labs. Data sets could be used during testing to check the accuracy. Data sets are a variety of known data used to test software to make sure it is accurate.

The National Institute of Standards and Technology (NIST) is in the process of developing Computer Forensic Reference Data Sets (CFReDS) for digital evidence. These reference sets will help the digital forensic labs with the testing process. Currently, there is not a protocol for data sets used to perform the tests. The NIST (2008) suggests that reference sets provide an investigator with documented sets of simulated digital evidence for examination and testing (p.1). Data sets can determine if a program accurately recovers data and information.

The Problem

Bianchi and Pollitt (2006) declare that a goal of a digital evidence laboratory should be to provide high quality results using accurate, reliable, reproducible, and legally defensible procedures (p.85). To meet this goal, digital forensic labs in the United States should be performing their own validation and verification tests on their digital forensic tools. Digital forensic examiners should never take the word of the software developer that the tools work without performing their own testing.

To perform the validation and verification tests, the digital forensic lab must first have a standard set of policies and procedures in place for their examiners to follow. Bianchi and Pollitt (2006) argue that top management is responsible for committing resources, establishing policy, assigning responsibilities, and developing overall accountability for the program (p.86). Using a specific set of data to perform testing may be part of an agency's policies and procedures in the validation and verification testing. The digital forensic labs should also set up day and time schedules for performing the testing. Setting up specific days and times will help establish a routine and organization to the testing. This may consist of one or more people in the digital evidence lab taking the time to perform the validation and verification tests.

Two key barriers arise when performing validation and verification tests. One barrier is a lack of funding. Funding is required to purchase the necessary equipment and to pay an employee to perform the testing. Bianchi and Pollitt (2006) acknowledge that as new technology becomes available, the digital evidence examiner must acquire the tools to use to work with the new technology (p. 86). To perform the examination, the examiner may need to update software or buy new hardware. Bianchi and Pollitt (2006) add that a variation of hardware is needed to connect different devices for extraction of evidence (p.86). An example of this hardware is unique boxes that block cell phones signals, called a cellbox. The second barrier is the time; it takes time to perform these tests properly. The examiner must take the time to perform the test in an exact and accurate manner, making sure not to be careless or rushed. Bianchi and Pollitt (2006) warn that serious deficiencies can occur when insufficient attention is given to the quality of the work product (p. 85). It also takes time for the examiner to document the process. Whenever a test is performed, the examiner should give specific details and information on the test. Documentation should include enough information so that another examiner would be able to perform the same test and get the same results.

Digital forensic labs should be performing testing when they use new digital forensic tools or upgrade to a new version of the tool. Periodic testing needs to be in place to ensure that their forensic workstations are still functioning and performing properly. SWGDE (2009) states that the testing processes are to ensure the integrity of the components utilized in the forensic process (p.3). It is vital to make sure that the tools used for the examination are still working properly. This can be done by testing them and making sure that the results given are accurate and sound.

Software programs and technology change at a rapid rate, which creates another problem for the forensic examiner. It is difficult to do proper validation and testing before a newer

version of the program is on the market. Occasionally, outside agencies or manufacturers perform validation testing. Bianchi and Pollitt (2006) argue that improper examination, review, or analysis by unqualified persons can yield inaccurate or misleading results and opinions (p.80). An examiner that did not perform his or her own testing and used an outside agency would not know if the testing was performed accurately. The individual performing the testing from an outside agency may not have the proper qualifications or certification to execute the testing, which is an issue in the examiner's review of the product.

Bianchi and Pollitt (2006) give some background information on the progression of software tools used to conduct digital forensic examinations:

> "The software tools first used in conducting examinations were products that were produced by manufacturers of hardware, operating systems, and network operating systems to troubleshoot their products. Software tools followed, often written by forensic practitioners, to perform specific steps, or even sub steps, in the forensic process. These tools become more numerous and complex over time and evolved into complex graphical user interface tools that are the backbone of current practice" pg.87.

The tools digital examiners use to examine digital forensic evidence have progressed immensely since digital forensic was first introduced. At the beginning those tools were made by manufactures' for their products, now there are companies that make tools solely for examinations by digital forensic examiners. Not only are the tools being used by examiners advancing in their processing tasks but also by adding graphical user interface, making it easier for the examiner.

Purpose of study

The purpose of this study was to provide a description of the current state of validation and testing procedures that digital evidence examiners perform in their labs in the United States. Currently, there is not a scientifically accepted protocol in place for the validation and testing procedures of digital forensic software. Data was collected from digital forensic laboratories and their examiners. The data collected described the methods used by digital forensics examiners to test and validate their tools.

Research questions

1. What is the current state of validation and testing of digital forensic tools in the United States?
2. What are the primary methods used to validate and test digital forensic tools by digital forensic labs and examiners in the United States?
3. What are the barriers to validation and testing of digital forensic tools?

Significance to the field

Data gathered from this study can help determine the current state of validation and testing of digital evidence tools in the United States. The information will provide insight on the procedures examiners are currently using for validation and testing of digital evidence. Because there is not a currently accepted scientific protocol for the validation and testing, this information and documentation can be a starting point to build on for current standards and procedures.

Review of Literature

Volonino, Anzaldua, & Godwin (2007) write about in certain cases, digital evidence can be the only thing that ties a person to a crime. If it was not for the digital evidence, the crime may have gone unsolved. One of the more famous notable crimes is the BTK killer case, which started in 1974. Dennis Rader was linked to the killings by a floppy disk that had deleted files on it. The floppy disk was given to a television station that turned the disk over to the police. The police examined the floppy and found deleted information pertaining to a church. They then checked the hard drive from a computer at the church to make sure the disk had been used there. This led them to Dennis Rader. If deleted information had not been recovered from the disk, Dennis Rader may have never been caught (Volonino, Anzaldua, & Godwin, 2007, p. 46). This case proves the importance of digital forensic evidence. The field of digital evidence has grown a vast amount since this case.

Introduction

Cybercrime can be in two forms. One is where computers are the target of a crime, such as taking customer credit card numbers. The second form is computers as the instrument of the crime, such as illegal electronic funds transfers. Files that can be recovered include deleted, hidden, password protected, and encrypted files. Sometimes examiners are unable to retrieve the whole file and have to retrieve as much of the deleted file as they can. Examiners may also find hidden files or temporary files that may provide useful information. This information may be found in areas that are not conventional areas to look at, such as unallocated space and file slack.

The amount of information when examining a computer can be large. Filters can be applied to sort a large amount of information to a more manageable amount. This requires the

use of forensic tools and software. This must be done correctly and efficiently for the task to be successful. If not done properly, it could be detrimental to the evidence. Examiners may use digital evidence tools to help provide insight on a chain of events, search key words and dates, search for copies of previous documented drafts and potentially privileged information, search for programs, and authenticate data files, and their date and time stamps (Volonino, Anzaldua, & Godwin, 2007, p. 97). All of these things are crucial to digital evidence examiner and can be key pieces of evidence.

It is vital for agencies performing this testing that they have policies and procedures in place. The examiner must know and understand them to be able to follow them. Different departments that are involved with digital evidence policies and procedures may vary due to different circumstances and variables. These policies and procedures establish rules and methodologies.

According to Volonino, Anzaldua, & Godwin (2007) stated, from a legal perspective they ensure that:

1. A baseline or benchmark is set for all cases as needed for external audits or other reference.
2. Processes throughout the case lifecycle from first contact to release of evidence are understood.
3. Technical procedures are well-documented.
4. Integrity is automatically built into the handling of the case.
5. Different forensic investigators can work or collaborate on the same case without significant disruption.

6. The final report has a standard format (p.121).

For evidence to be able to be recognized in court, it must follow certain guidelines. "Things that might be in question are, was everything performed in accordance with forensic science principles, is it based on standard or current best practices, conducted with verified tools to identify, collect, filter, tag and bag, store, and preserve e- evidence, conducted by an individual who is certified in the use of verified tools, if such certification exists, and documented thoroughly" (Volonino, Anzaldua, & Godwin, 2007, p. 82). Examiners must always be prepared to go to court with their case and defend findings. Examiners should be prepared to discuss and explain their methods, tools, and techniques.

Performing Testing & Examinations

There is no single method to perform testing on all devices. There are many factors that must be taken into account before one can start the examination. Examiners must first look at the type of device it is. There is a vast amount of types of devices that contain digital evidence. The second thing is what operating system the device is using. Computer operating systems can be anything from Macintosh, Windows 98, to Windows 7. These are all different in their functioning but may have some similarities. Third are the software applications that can be on the device. This could be different programs that may cause problems for examiners. Fourth are hardware platforms; hardware on the device may change what the examiner needs to perform the examination. The fifth item is the state of the data, meaning that the data could be deleted or in hidden files on the computer. Sixth is the domestic and international laws; some laws may forbid examiners from doing certain things and searches with the device. Lastly are concerns about bad publicity or liability; some people might not even turn in the device since they are worried about the public finding out something that may be bad for the company.

Accreditation Issues

Beckett (2007) reported that there are some problems that are unique to digital forensics, such as the high workload and the lack of resources. Many of the Digital Forensic laboratories are trying to achieve accreditation by the ISO 17025E standard. There is difficulty in meeting the standards of validation and testing of digital forensic tools and meeting the requirements for the accreditation.

Agencies are unable to reproduce the tests performed by other organizations or the manufacturer and to verify the results because they have little time and are poorly equipped. Many agencies will rely on independent validation studies that have used protocols and equipment different than their own. This could lead to the lack of not only valid tools, but also improper testing. The lack of validation and testing of tools can cause a large problem in the accuracy, reliability, and performance of the individual tools.

Beckett defines terms used to assist in the interpretation of proper validation and verification. The first term is "extensibility," which is defined as the function of the tool. This means that, for the function's results to be valid, it must meet specifications for components, and as time goes on new specifications can be added. Extensibility is a critical factor in keeping these tools up-to-date and defining what functions the tool performs.

The second term is "tool neutrality." This is when it does not matter which tool is performing the function as long as the results the tool produces can be measured. The last term, "tool version neutrality" describes the process or a tool developed over time. It identifies the requirements for each function and then measures against the need for the tool to be validated.

These factors will be beneficial in the validation and verification processes because they will meet the requirements of extensibility and tool neutrality (Beckett 2007).

Guo, Slay and Beckett (2009) focus on two key issues related to the validation and testing of digital forensic tools. First, problems in digital forensics are solved as they occur instead of looking at the process of analysis as a whole. The examiners may need to create a new tool to work with this new device instead of examining how it will affect digital forensics as a discipline. The second issue is the methodologies used for validation and testing. These come from the National Institute of Standards and Technology (NIST)/Computer Forensic Tool Testing (CFTT) and Digital Forensic Tool Testing (DFTT). The NIST protocol for methodology is only a general plan that does not provide specific details of how to perform the tests.

In terms of digital evidence as a field of discipline, there is no set standard. To resolve this issue, there needs to be a set procedure on how to complete the evidence investigation, determine the basic functions needed for the investigation, and decide the requirements of the function. Another problem in the field of digital evidence is that the basic functions have never been mapped and specified. Guo, Slay and Beckeet (2009) propose a new functionality oriented validation and verification paradigm of tools (p.10). They attempted to provide specific requirements for the search function and to make reference sets that worked with these requirements. They believed in doing this that the testing process of digital evidence would be made simple by testing the tool against reference sets. They believe the way mapping functions is performed and designed will allow other tools to be tested with it.

Wilsdon & Slay (2005) reported that each discipline and their practices can be grouped together and can be tested by reconstructing the environment. Performing tests should evaluate a

lower-level inspection of the functions that make up forensic computing, but is not an evaluation of the discipline as a whole at the operational level. The ISO7025-1999 standards outline the requirements for competence of testing and calibration laboratories. The laboratories and their equipment test against ISO standards, and they must pass these requirements to gain accreditation. Currently, the digital forensic laboratories are preparing themselves in order to attempt to seek ISO7025-1999 accreditation.

The ISO7025-1999 accreditation standard has precise detailed requirements; these requirements provide a foundation for the documentation and testing procedures by providing insight and direction. For more thorough and technical requirements, one must find out what factors can cause a change or error in their results. Wilsdon and Slay (2005) state such factors include human factors, equipment, measurement traceability, test and method validation, and environmental conditions (p.5). These are all relevant factors that should be accounted for when looking at testing how the digital evidence software works and what would cause errors in the results.

Some of these factors will be difficult to measure the impact of. The operating system, software, and other programs that are installed on a computer could cause issues, making the accreditation process difficult and could affect the ability to produce consistent results. To assist in overcoming these issues, the development of the software must check thorough for the process of isolation. The effects of the software could be tested to a certain degree, but there is a lot of software that is available and not all of it can be tested.

Future of Digital Forensics

Many examiners believe that digital forensics is at a crossroads in its development. The crossroads have many different paths and some will work better than others, but he or she must pick a path. These paths might be a standardized and scientific approach, or a tool driven approach or even a precedent based approach. Some of these paths may be guided by an independent or outside source. The digital forensic leaders need to research and determine the best path for the discipline as a whole.

Data sets could be a helpful tool in the laboratory to assist with validation and verification testing. NIST (2008) states it is developing Computer Forensic Reference Data Sets (CFReDS) for digital evidence (p.1). The data sets would give investigators documented sets, which contain modified digital evidence for examination. NIST (2008) adds these data sets could be used by investigators in multiple ways, which include validating the software tools used in their investigations, equipment check out, training investigators, and proficiency testing of investigators as part of laboratory accreditation (p.1). The CFReDS site will not only be a repository of images, but it will also have resources that will allow the examiner to create his or her own test images.

NIST (2008) claims there are three primary reasons for testing forensic tools, which include establishing that lab equipment is functioning properly, testing proficiency in specific skills and training laboratory staff (p.1). The data sets will be multi-functional and will have slightly different requirements. The examiner needs to be aware of not only what is in the data set but also its location; this process must be documented thoroughly. To make data set testing more authentic, it can be based on an investigation scenario. NIST (2008) proposes these data sets would be generally available but would be comparative to data sets for proficiency testing and staff training (p.1).

Johnson (2006) proposes a set of processes in which identifying, collecting, transporting, storing, analyzing, interpreting, reconstructing, presenting, and destroying of digital forensic evidence occurs. This means that any actions that pertain to digital evidence should have certain actions or functions performed. These actions or functions can be performed either by the examiner or a process by digital evidence software. The elements of the process are what cause the challenges to digital evidence.

The process has some faults, like other processes. These faults could be due to people and systems that perform the processes. For example, Johnson (2006) explains in the United States, evidence in legal cases is admissible or not based on the relative weights of its probative and prejudicial value (p.2). Probative value of evidence gives a further understanding of the issue or issues in the case. Prejudicial value of evidence is the "extent to which it leads the finder of fact to believe one thing or another about the matter at hand" (Johnson, 2006, p. 2). The probative value of the evidence is paramount and can be damaged if flawed evidence is presented. The value of the evidence needs to remain strong and factual. For example, evidence will remain strong and factual if proper techniques and procedures are followed.

For the understanding and meaning of digital evidence to advance, it must be presented in court. Digital data does not stand alone as a finder of fact. It must be presented through expert witnesses who must show the existence, content, and meaning to the fact finders. Digital evidence is latent and hearsay evidence. It is hearsay evidence because the expert performing the analysis did not directly observe the action, but presents the evidence based on the facts or conclusions on what the computer recorded. For the evidence to be admitted to court, it has to be under the normal business records exemption to the hearsay evidence prohibition. The experts must have an unbiased opinion and evidence must be of acceptable quality.

One way to help prove the quality of digital evidence would be by showing the process performed to validate and test its accuracy. Johnson also states, "One of the results of diverse approaches to the collection and analysis of digital forensic evidence is that it has become increasingly difficult to show why the process used in any particular case is reliable, trustworthy, and accurate" (Johnson, 2006, p. 3). There is a vast amount of software and techniques used on digital evidence for collection and analysis that it becomes difficult to prove that each one is accurate. If all digital evidence examiners used designated techniques, it may alleviate the issues of proving the reliable, trustworthy, and accurate.

Reliability could be proven by producing a test with data sets that would show the reliability of the software tool to perform the function accurately. Johnson (2006) also stated the belief that, "The real situation is that there are no best practices or standards for what makes one approach to digital forensic evidence better or worse than another. In the end, what works is what counts" (p.3). The tool's function working properly is essential; however the standards and outline also play a vital role.

Identifying all the possible sources where evidence can be collected is the first step in examining digital evidence. The relationship between the computer and evidence on the computer can cause an issue or even cause failures of the evidence to be properly identified or collected. Daubert's Guidelines created from the Dauber v. Merrell Dow Pharmaceutical, Inc., 509 U.S. 113 S. Ct. 2786, L. Ed. 2d 469 (1993) case are for the admissibility and validity of scientific evidence, due to case law in the United States. In Dauber v. Merrell Dow Pharmaceutical, Inc., expert witness testimony was inadmissible because their studies had not been published or subject to peer review (Feder & Houck, 2008, p. 132). Daubert's Guidelines

apply not only to digital forensic, but to all scientific fields. The Daubert's test of scientific evidence in this case includes four basic issues:

(1) Has the procedure or technique been published?

(2) Is the procedure generally accepted?

(3) Can and has the procedure been tested?

(4) What is the error rate of the procedure?

Currently, meeting these guidelines for digital forensics, have proven to be difficult due to the lack of published material about the digital forensic analysis methods. The materials and studies are rarely published in scientific journals (Johnson, 2006, p. 27). The fact that there is a lack of published material causes many challenges to the admissibility or validity of digital evidence.

Forensic examination and analysis tools have trade secrets that they do not publish. This secrecy is due to the company's desire to have a competitive advantage. When a company finds a new way for their tool to perform a search of a physical drive, they do not want a competitor company to know how this new technique performs functions and copy it. Most of the digital forensic tools used do not provide information about the functions the tool performs; this can cause the use and their results to be challenged. In order to gain acceptance in the courts, there must be publications. Without publications, analysis of digital forensic evidence can be challenged in court. In most cases, one could reasonably challenge the validation tests and the technique used by the digital forensic examiners.

The court decided that the technique must be "generally accepted" as reliable in the relevant scientific community for the experts opinion to be admissible. General acceptance is sometimes decided on by publications and the decisions of other courts (Feder & Houck, 2008, p. 140). Generally acceptance, goes hand in hand with publications. It would be hard to be generally accepted without publications.

It is normally left up to the digital forensic examiner to do their own testing of their digital forensic tools. This means the examiner should be testing his or her digital forensic tools and documenting the process along with the results. If the tool has not been tested, it can lead to challenges not only on the tool but on the examiner (Johnson, 2006, p. 28).

The error rate of a procedure is important information. Most commercial products use independent tests to establish an error rate, which causes difficultly in providing an accurate error rate (Johnson, 2006, p. 28). These independent tests will also show what factors or variables will cause issues with the digital evidence software functioning properly. Some people believe that what a computer says has to be correct because they view computers as infallible.

Summary

There are several ways that digital forensic evidence can be challenged; many of the challenges are successful in the proper circumstances, but these challenges can be avoided with consideration and earnest efforts. There is not a way to avoid all the problems and faults, but almost all of the failure can be avoided with some effort. Digital forensic examiners need to overcome limitations, such as budget, training, tools, and basic human errors that have effects on digital forensic evidence. There is a notion that computers, include the content in them, are totally accurate which; this causes a problem.

Methods

Introduction

The purpose of this study was to provide a description of the current state of validation and testing procedures that digital evidence examiners perform in their labs in the United States. An online survey was used to collect data in this study. According to Salant and Dillman (1994), survey research is a powerful scientific tool for gathering accurate and useful information (p.9). This study will help provide information on the current state of validation and testing.

The data gathered will answer the following research questions:

1. What is the current state of validation and testing of digital forensic tools in the United States?
2. What are the primary methods used to validate and test digital forensic tools by digital forensic labs and examiners in the United States?
3. What are the barriers to validation and testing of digital forensic tools?

The study is a descriptive study using an online survey for data collection. The survey collected demographic information and data on the validation and testing examiners are performing in digital evidence labs across the United States.

The survey was an online survey; the digital forensics examiners had the option of taking the survey wherever and whenever they would like to. There was no regulation in regard to where the survey could be taken. For example, the participant could take the survey at his or her work place or at their home. This was ideal for this survey so the participant would feel comfortable and not feel pressure in taking the survey.

Sample/Participants

The main training and governing board for computer forensics is the International Association of Computer Investigative Specialist, or IACIS. Digital evidence examiners across the United States who are members of the IACIS were the population in this survey. IACIS is an "international volunteer non-profit corporation composed of law enforcement professionals dedicated to education in the field of forensic computer science" (Specialists, 2010, p. 1). IACIS is a major organization dedicated to the field of forensic computer science, making its members an excellent choice of population for the survey. This organization hosts training conferences, produces training materials, and develops accreditation requirements for the professionals in the digital forensic investigative fields. "IACIS prides itself on being the world's leading organization for computer forensics practitioners. IACIS offers the Certified Forensic Computer Examiner (CFCE) certification along with recertification and proficiency testing services" (Specialists, 2010, p. 1).

Its population includes federal, state, and local law enforcement who gave the survey a broad demographic sample of applicants (Specialists, 2010, p. 1). The sample of digital examiners will come from the IACIS website's listserve. A request to take the survey was posted on the IACIS listserve. The listserve will provide a cross selection of participants from across the United States. Each IACIS member will have clicked on the post to be given the link to the survey. Approximately 87 digital forensic examiners participated in the survey.

Instrument

A list of digital evidence examiners who are members of the IACIS, via the IACIS listserve Iacis-1@ops.org, will serve as a master list for the survey. The email sent to the listserve stated:

"Dear List Members,

A graduate student here at the University of Central Oklahoma would like you to take a couple of minutes to fill out the following survey.

http://www.surveymonkey.com/s/C7YLKVZ

The purpose of this survey is to collect data about the current state of validation and testing of digital evidence tools. The survey will take approximately 10 minutes to complete. All submissions will be completely anonymous. Participation in this survey is voluntary. The information will be gathered in aggregate, data combined from several measurements, and at the end of this study, the data collected will be destroyed.

Megan Dorman is the Principal Investigator on this study and it has been approved by the UCO Institutional Review Board. To contact the UCO Institutional Review Board, email irb@uco.edu. If you have any further questions, please feel free to contact Megan by email at mdorman@uco.edu."

The first part of the survey is the implied consent. The implied consent is not only where the participant gives consent, but also contains the purpose of the study and gives a confidentiality disclaimer. It also informs the participant that it takes approximately 10 minutes to take the survey. Participation in the survey is on a voluntary basis. However, participants

must be at least 18 years of age to take the survey. The consent also ensures the participants that all information from the survey will be destroyed after the research has been completed.

Salant and Dillman (1994) note that survey research carries with it an obligation to follow certain ethical norms. Participants in the survey should know why the survey is being given. The study should not discriminate against anyone in any way. Research studies, even in online survey form, should never cause a participant any physical or mental anguish. Any time one asks people to participate in a survey, it is one's responsibility to respect both the participant's privacy and the voluntary nature of his or her involvement (p.9). Letting the participant know that his or her responses will be anonymous and confidential should help the examiner freely and honestly answer the survey. My email address, along with the IRB email address, was also added to the survey for any questions or further information.

There are several types of surveys, including mail, face to face, telephone, and web-based (Salant & Dillman, 1994, p. 19). In this study, a web-based survey was the method used to collect data on the current state of validation and testing of digital forensic tools. The survey consisted of multiple choice and fill-in-the-blank answers.

Bradburn, Sudman, & Wansink (2004) explain:

> A survey is a transaction between two people who are bound by special norms. The interviewer offers no judgment of the respondent replies and must keep them in strict confidence. Respondents have an equivalent obligation to answer each question truthfully and thoughtfully. In the survey, it is difficult to ignore an inconvenient question or give an irrelevant answer (p.9).

These are key factors that make a survey a good choice for this study. The participants involved in the study should not feel like they are being judged because no one will know their response. Survey was selected as the method for the study because it is easy to respond to and does not take a large amount of the examiner's time. The participant's time is a valuable thing due to issues like high workloads. Making the survey simple and not time consuming makes the participant's time to take the survey spent effectively.

Survey Monkey, an online survey website, was the host for this survey. When accessing the survey, the participant selected a link sent to the IACIS list in an email, which took him or her directly to the survey. Nardi (2003) reports that using a web-based survey method is ideal due to its higher response rate among the other methods of surveying (p.60). According to Bradburn, Sudman, & Wansick (2004), web-based surveys are also ideal for many reasons, including:

1. Ease of interviewee response that doesn't depend on an interviewer
2. Improved quality of responses through elimination
3. Elimination of interviewer bias
4. Shorter turn-around times
5. Simple integration of images, sound, and video
6. Automatic data entry (p.295)

The participant took the survey when they had a chance to take it, so they did not have the pressure to take the survey at a certain designated time. The participant also did not have to worry about the interviewer's bias or judgment from having an interviewer perform the survey. Web-based surveys also take a shorter amount of time to receive from the examiners. The

answers given to the survey are automatically put into Survey Monkey and are available for review.

Limitations of survey research

Several issues may arise with the survey that could cause a low response rate. The participants may feel that completing the survey requires too much time and cancel the response. Nardi (2003) suggests that inevitably, many respondents leave some questions blank because they missed them, refused to answer the questions, do not feel the questions applied to them, or do not know how to answer the questions (p.89). The participants could also feel embarrassed by the answers to the survey's questions and cancel their responses also. Therefore, the participants are advised in the consent portion of the survey that their answers will be confidential and no names will ever be taken or revealed.

If the response rate is low, the request will be resent and participants asked if they would prefer a copy of the survey by mail. According to Salant and Dillman (1994), "The process of repeated, personalized, and well-timed contacts is designed to send one basic message, which is that each respondent's participation is essential to the success of an important study" (p.139). The survey was resent after two months of the original post to the IACIS listserve to increase sample size. Another limitation is that the survey will be self-reported. Participants may not be truthful with their answers on the survey and may not completely honest about the procedures and protocols.

Data Collection/ Procedures

Before conducting the survey, the Institutional Review Board's (IRB) approval was needed because the survey conducted did involve contact human subjects. The IRB checks for

any risks for the human subjects. The IRB's approval for this survey is from the Office of Research Compliance at The University of Central Oklahoma. After receiving the IRB's approval, the construction of the survey was started online at Survey Monkey (http://www.surveymonkey.com) (See Appendix A).

An email was sent to members of the IACIS listserve on March 31, 2011. The digital forensic examiners on the IACIS listserve clicked on the link for the survey. This link took the participant directly to the survey on Survey Monkey. The participants were able to follow the online survey from screen to screen until completion.

The questions on the survey are in a font face that is large and clear to prevent eye strain and allow easy reading (Bradburn, Sudman, & Wansink, 2004, p. 284). There were 26 questions on the survey, which included a comment area at the end. The comment area was for information or comments that the participant might feel important to state or add to the survey. Keeping the number of questions low suggested that the survey did not take a large amount of time to take. This also suggested that the survey was not difficult to take (Bradburn, Sudman, & Wansink, 2004, p. 285). After the survey was completed, Survey Monkey recorded the responses or analysis.

When creating the survey on Survey Monkey, the questions were entered one by one. The survey contains multiple-choice answers, fill-in-the-blank answers, as well as a comments section. This variation of answer options helped gather the best information from the questions. An answer was selected, or in some cases, typed by the participant. Typing the answer was selected to provide more insight on the response to the question. There may not be a common

answer to a question that can be proved by the participant. Also, there may be a vast amount of answers to the question.

Bradburn, Sudman, & Wansick (2004) recommend that only one question appear on screen at a time to keep from any confusion between questions and keep the focus on each question (p.291). The participant should be able to focus on each question individually to ensure that the question is answered to the best of the participant's knowledge. The survey was designed to skip questions that did not pertain to the participant based on the previously answered questions. This kept the participant from having to go through questions that did not pertain to him or her.

The survey gathered demographic data. Demographic questions provide information about the participant, such as gender, age, education, and occupation (Nardi P. M., 2003, p. 76). Demographic data is important because it provides insight about the participant and his or her background. Some of the information for occupation consisted of job title and jurisdiction the participant works for. Participants were asked if they did validation and testing and how they performed the testing. Also, if the participants and their agencies had policies and procedures set in place about validation and testing of their digital forensic tools. The participant should also be documenting their validation and testing. Participants were asked if they did documentation and how they documented.

The last window for the participant stated, "Thank you for your time and have a great day." This was to thank the participant for his or her energy and time taken for the survey (Bradburn, Sudman, & Wansink, 2004, p. 294). Since the survey was voluntary, it was important to thank the participants who participated in the study. Their information was the key

to the study and the study can't be done without them. Salant and Dillman (1994) claim that a successful survey produces sound data that can be translated into valuable information for its intended users (p.11). The data collected from the survey provided valuable information for not only the examiners, but the whole digital forensic community.

Since the survey was web based, collecting data immediately after the survey had been completed was quick and easy. The data collection for the study began the spring of 2011. When evaluating the responses for each question on the survey, Survey Monkey showed the response percent and response count. Response count was how many participants selected that answer. The total number of participants that answered the survey question, along with the number that skipped that question, was also given at the bottom of the totals. The questions on the survey collected data on the current state of validation and testing in the United States.

Data Analysis

Data gathered by the survey provided information on the current state of validation. The data gathered from the survey was examined to determine the current state of validation and testing of digital forensic tools in the United States, the primary methods used to validate and test digital forensic tools by digital forensic labs and examiners in the United States, and the barrier to validation and testing of digital forensic tools.

Results

Introduction

The purpose of this study was to provide a description of the current state of validation and testing procedures that digital evidence examiners perform in their labs in the United States. A web based survey was sent to digital forensic examiners via the IACIS listserve. This survey consisted of questions that would help collect data on the validation and testing procedures that the digital evidence use across the United States. Previously, there was little information or research on the current state of validation and testing procedures that digital evidence examiners perform in their labs across the United States.

Demographics

83.5% of respondents were male and 16.5% were female. 41.8% were between the ages of 40-49 years old, while 29.1% were 50-59 years, 25.3% were 30-39 years, 2.5% were 18-29 years, and the remaining 1.3% were 60 and over (See Figure 1).

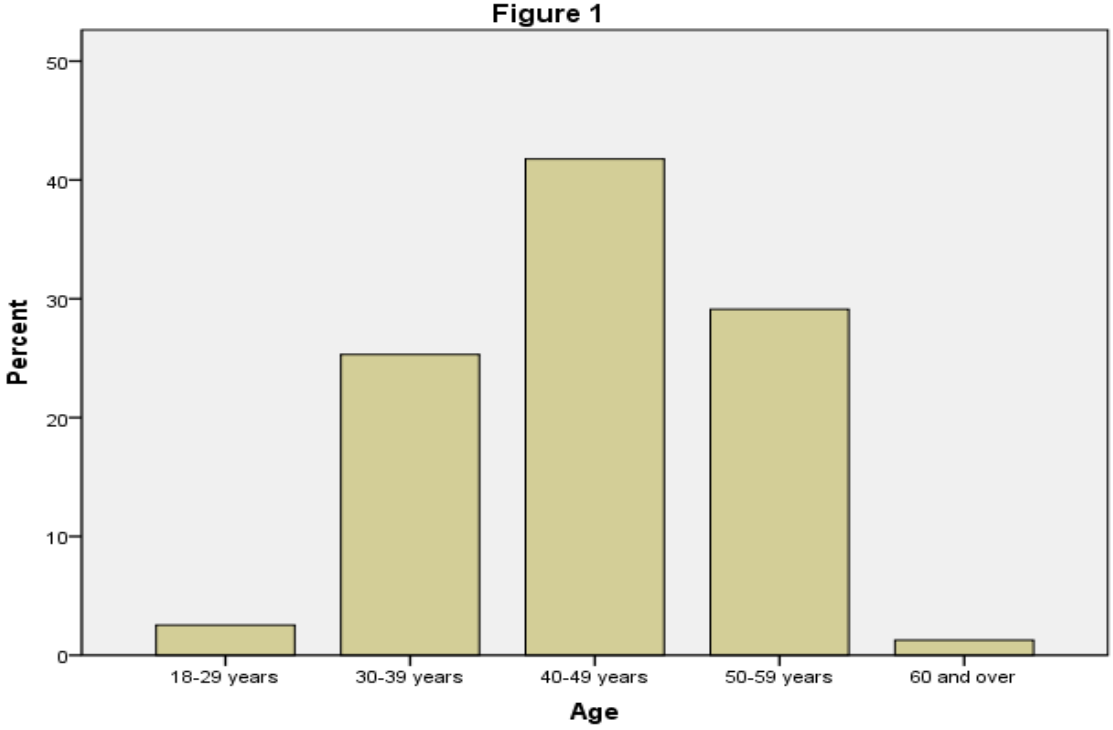
The participates education level, 51.9% acquired a Bachelor's degree, 21.5% stated that they had some college, 16.5% acquired a Master's degree, 6.3% of respondents obtained a High School Diploma or GED, and 3.8% acquired a Doctorate.

41.3% of respondents' answered that they obtained 6-10 years of Digital Forensic experience, 30% with 1-5 years, 20% with 11-15 years, 6.3% with 15-20 years, and 2.5% with 20+ years.

Law Enforcement employed 82.5% of respondents, while 12.5% worked in the Private Industry, and 5% answered other. Of the respondents who selected other, two were employed

for a government agency, one respondent was in the process of transitioning to a private agency, and one worked under a non-profit corporation grant funded under the Bureau of Justice Assistance.

Figure 1



The jurisdiction that best describes who the respondent worked for, 26.3% State, 25% Federal, 21.3% answered Local, 17.5% County, and 10% Other. Of the 10% who selected Other, two of the respondents worked for private companies, one for an international company, one with a corporation, one with the Department of Defense, and one stated that their company serves all levels of law enforcement. A majority answered their job title was a variation of computer forensic examiner or specialist. Also, some were labeled detective or investigator.

Instruments

72.5% used Windows 7as the operating system on their main forensic machine. Also, 22.5% used Windows XP, 2.5% used Windows Vista, and 2.5% used Mac OS 10. One of the respondents who answered other uses Windows 2000 and anther uses a triple boot Mac Pro tower.

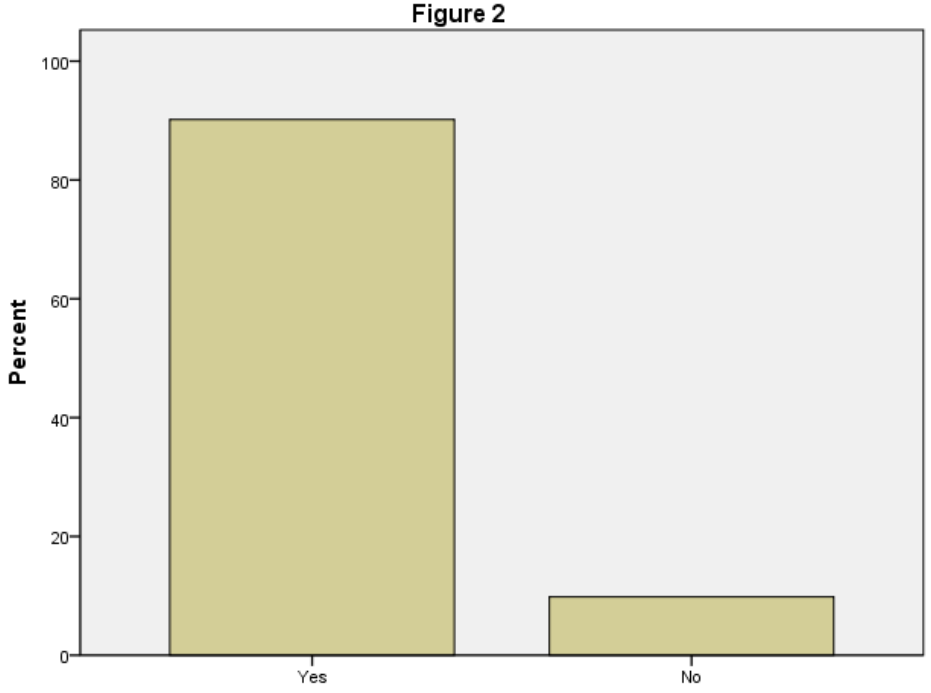
A majority use FTK and EnCase tools/software to validate and confirm their results, other popular answers included WinHex, SPADA, HexEditor, X-Ways, and Linux.

Performing Validation Testing

95% validate and test their Digital Forensic tools, while 5% responded that they do not. 90.2% use standardized data sets to perform their Validation and Testing, leaving 9.8% that do not. (See Figure 2). For validating and testing, 78.6% use self-created data sets, 8.9% are created by agency or unit, and 10.7% obtained them from available data sets in the Digital Forensic Community, and 1.8% selected other. The participant that selected other stated that they had a "researching and testing organization under as part of our laboratory. There employee (SIC) approximately 25 full time employees."

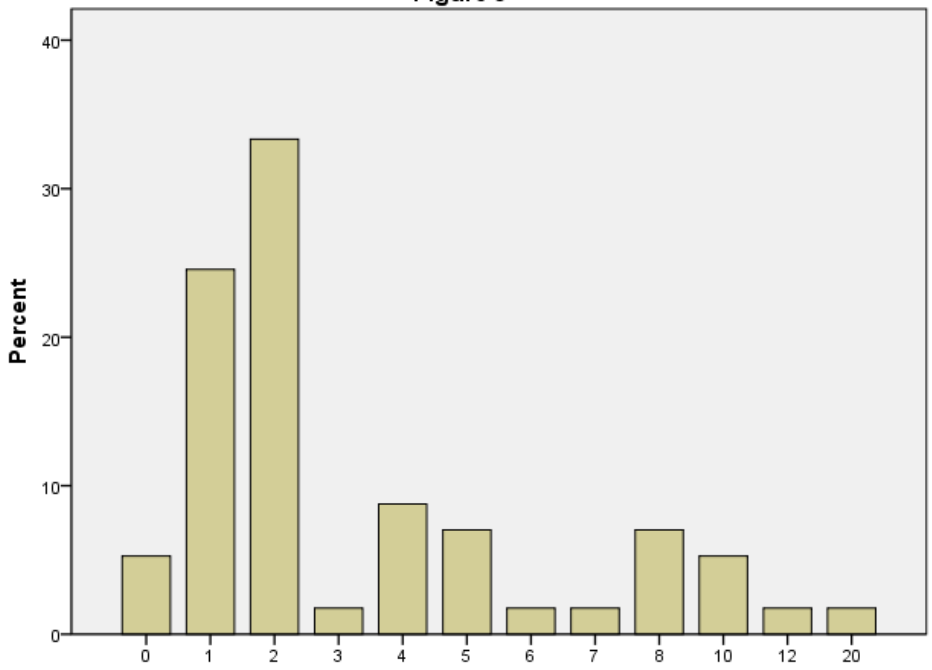
The amount of time, in hours, typically spent in a month validating and testing their Digital Forensic tools: 5.3% answered 0, 24.6% answered 1 hour, 33.3% answered 2 hours, 1.8% answered 3hours, 8.8% answered 4 hours, 7.0% answered 5 hours, 1.8% answered 6 hours, 1.8% answered 7 hours, 7% answered 8 hours, 5.3% answered 10 hours, 1.8% answered 12 hours, and 1.8% answered 20 hours (See Figure 3).

Figure 2



Do you use standardized data sets to perform you validation and testing?

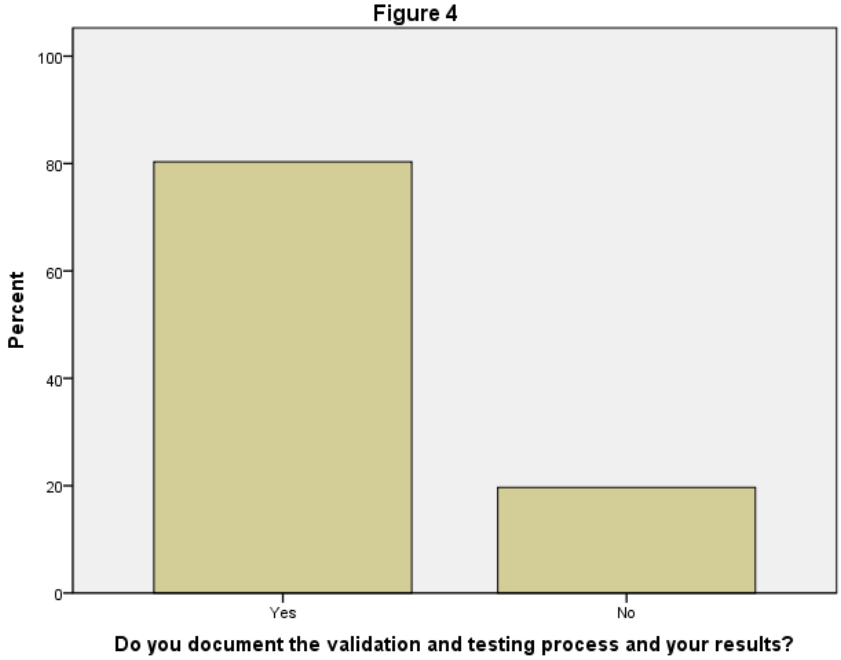
Figure 3



Hours per month spent on validating and testing Digital Forensics tools.

80.3% document the validation and testing process and their results, leaving 19.7% that do not. A majority of the response stated that they either kept an electronic log or a written log for documentation of their validation and testing process (See Figure 4).

Figure 4



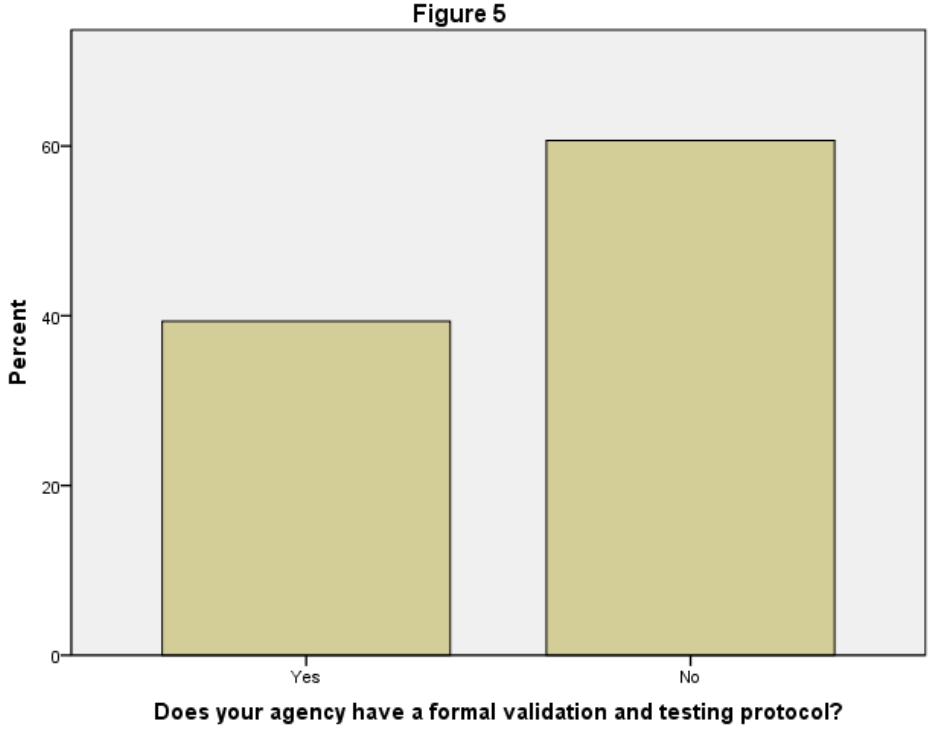
Validation and Testing Protocol

39.3% of respondent's agency has a formal validation and testing protocol and 60.7% stated no (See Figure 5). When asked to briefly describe protocol the responses given varied extremely and lacked detailed. Some stated that their protocols where proprietary, while others only provided limited details on their policies. Most respondents whose agencies do not have a formalized validation testing protocol stated that they use known data sets and/or hash values to validate results.

46.4% indicated that each examiner performs testing and validations, while 35.7% have it assigned to one individual. 17.9% selected other, two examiners stated that they have a group or

team testing. Five examiners stated that they use a combination of the two options, and two examiners stated it is assigned to someone in their unit.

Figure 5



Respondents perform validation and testing, 62.5% when new tool updates are released, 10.7% answered biannually, 8.9% quarterly, 7.1% answered monthly, 7.1% answered annually, 3.6% answered weekly. The respondents that selected other are stated that they perform validation testing before each case, standard tools are not re-validated, perform validation and testing as needed while working a case, and in the event of a system boot failure.

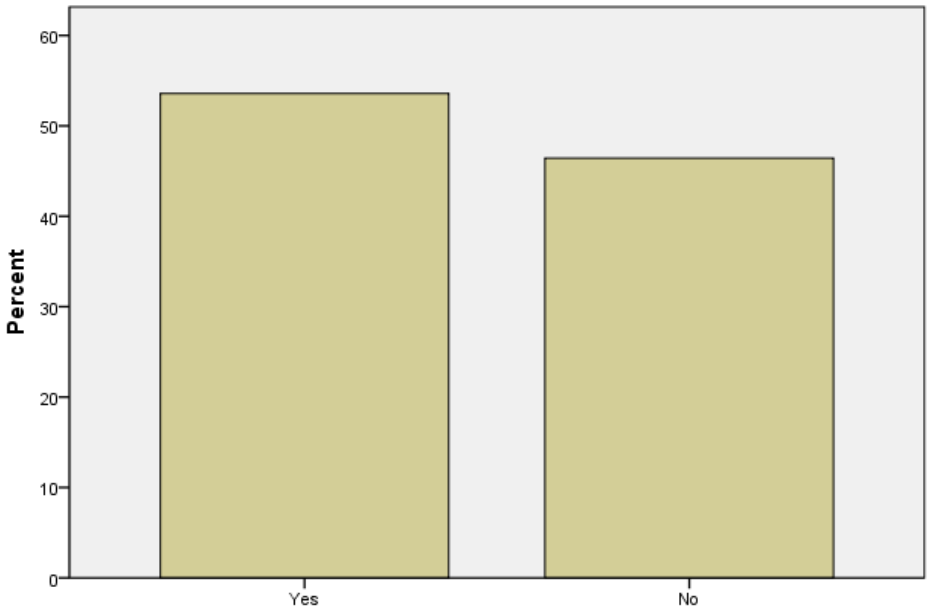
53.6% validate and test each function, if the Forensic Tool performs several different functions, while 46.4% do not (See Figure 6). Time, case load, and the amount of tools along with their updates, were obstacles and limitations when performing validation and testing of digital forensics tools. Also, a few stated that data sets were issues.

If they are not performing validation and testing of your digital forensic tool, why not? Examiners answered that,

- "Validation and testing of our digital forensic tools is not imposed by our organization."
- Cellebrite: We don't have the resources to test each cellular phone with a similar model that is not evidence. For this we use visual validation, and observe data viewable on the device and compare it to what Cellebrite provides, If there's a discrepancy, photos of the phone are submitted as a complementary report."
- "When tools are already validated by another two well know labs, we don't validate it again."
- "I validate my results, not my tools."
- "Time frame reliability of manufacturer expected results."
- "Lack of priority placed on task by management."

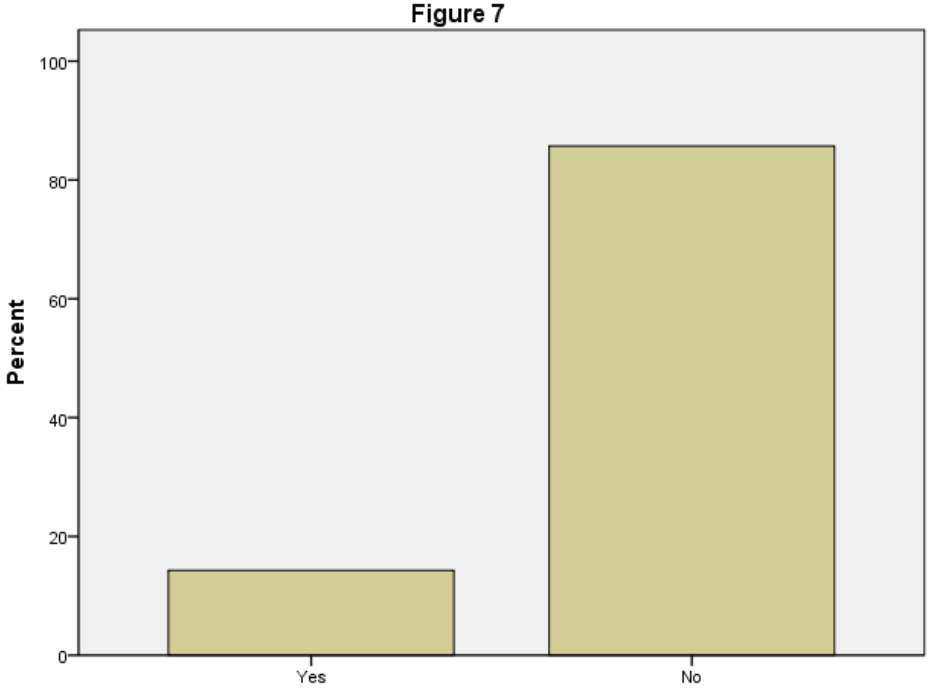
14.3% of respondents had been asked in court about their validation process and 85.7% had not been asked (See Figure 7). One examiner stated that they have had their validation manual subpoenaed by the defense on two occasions. The examiner thought the defense was expecting for them not to have one, and after it was discovered the case was resolved.

Figure 6



If the forensic tool performs serveral different functions, do you validate and test each function?

Figure 7



Have you ever been asked in court about your validation process?

Discussion

Introduction

As time goes on, more electronics contain digital information that may be of evidentiary value. Digital forensic labs across the United States are tasked with the workload of the growing amount of evidence and also with building the accreditation for the field. There is little information on the validation and testing procedures of digital forensic labs in the United States. Validation and testing practices and protocols need to be researched, documented, and reported.

Discussion

The purpose of this study was to provide a description of the current state of validation and testing procedures that digital evidence examiners perform in their labs in the United States. Currently, there is not a scientifically accepted protocol in place for the validation and testing procedures of digital forensic software. Data was collected from digital forensic examiners. The data collected provided information on how examiners are performing these vital validations and testing procedures on their digital evidence software.

A survey was used to collect the data and information for this study. Surveys have multiple advantages that make them optimal for this study. One advantage is that the survey is easy to access. An online survey can be taken at any time from any computer. This means there are no restrictions as to when the survey can be taken. Likewise, if the respondent does not feel comfortable taking the survey at work, he or she can access it at home. There are other advantages to online surveys; for example, they are inexpensive, confidential, and make collecting and organizing data easier.

For the digital forensic field to progress, people need to know where the field is standing in its validation and testing procedures currently. There are many digital forensic labs across the United States that perform testing for a variety of institutions. However, there are no standard policies and procedures that all the labs perform for validation and testing. Each lab has its own policies and procedures when it comes to validation and testing.

The first research question was, "What is the current state of validation and testing of digital forensic tools in the United States?" Most of the examiners surveyed stated that they do perform validation testing. Scientific Working Group on Digital Evidence (SWGDE) states, "Validation testing is critical to the outcome of the entire examination process" (Evidence, Scientific Working Group on Digital Evidence, 2009, p. 2). However, in this study, 95% of the respondents performed validation testing, but 5% did not. This is significant since validation testing not only affects the processes of testing itself, but also affects the outcome from the testing.

SWGDE also expresses, "Failure to implement a validation program can have detrimental effect" (Evidence, Scientific Working Group on Digital Evidence, 2009, p. 2). However, 39.3% of the respondents' agencies have a formal validation and testing protocol, and 60.7% stated that they do not. SWGDE states that implementing a validation program is important "to ensure the integrity of the components utilized in the forensic process" (Evidence, Scientific Working Group on Digital Evidence, 2009, p. 3). If there is no validation program or protocols in place for the examiners to follow, then the examiners do not have direction on items like when to perform the validation testing, what data to use for the testing, all the tools and their functions that should be tested, how to document the testing, and so on. It seems that most examiners do

perform validation testing and create their own data sets for the testing, but there are not any policies and procedures in place to regulate any of the testing.

It is crucial for all computer forensic examiners to perform validation testing. Examiners must meet Daubert's standards if they want their evidence and testimony to stand in court. Also, testing their digital forensic tools will ensure that the tools are working properly. If the forensic tool is not working properly, then the results could be inaccurate. This could change the outcome of the results of a case. Examiners should never rely on the manufacturer of the tool to make sure that the tool is performing its functions accurately.

To regulate testing, set policies and procedures should be in place. These policies and procedures will tell the examiner how often the testing should be performed. SWGDE suggests, "Validation testing should be performed whenever new, revised, or reconfigured tools, techniques or procedures are introduced into the forensic process" (Evidence, Scientific Working Group on Digital Evidence, 2009, p. 3). In fact, 62.5% of the respondents stated that they were performing validation and testing when new tools are updated or released.

Policies and procedures for the labs should state that validation testing should be performed often enough to ensure the integrity of the tools and their functions, but not enough to cause the examiner unnecessary stress and time. This should be every other month unless a new tool is released or updated; then, testing should be performed at that time. A new or updated tool would not be allowed to be used until the testing has been performed, the tool passes the test, and the process has been documented. Also, there should be more research into how often validation and testing should be performed to see what would be the optimal occurrence for accuracy of testing. This could be weekly, monthly, yearly, or only when updates are available. Also,

policies and procedures should provide detailed information on how the examiner will perform the testing. This would provide cohesion between all the examiners in the agency.

SWGDE declares, "Validation testing should be applied to all tools, techniques and procedures utilized in the performance of digital forensics" (Evidence, Scientific Working Group on Digital Evidence, 2009, p. 2). Surprisingly, 53.6% of respondents validate and test each function, if the Forensic Tool performs several different functions, while 46.4% do not. It was shocking that a large amount, at 46.4%, of respondents were not testing each function. The examiners cannot be certain that each function is working properly unless they are being tested. Therefore, every function that performs several different functions should be tested individually.

The agency should state, in their policies and procedures, acceptable data sets for the examiner to use to perform the testing. Most respondents stated that they created their own data sets for testing. Policies and procedures should state the designated data sets for the examiners to use. These data sets would be specifically created and designated for validation testing. The data sets would be created by the lab itself until there is a regionally or nationally accepted data set designated for validation and testing. The created data sets would be approved before use to make sure the created data set is accurate. Designated data sets would also be beneficial because they would save the examiner time by not having to make their own data sets for testing. Policies and procedures would also provide documentation on how the testing is performed.

The examiners should also have training on the programs that they use to perform the examinations. Some of the programs have their own training that offers the examiner to be certified using their program. Training would be periodical to keep the examiners up to date with new tools, software programs, and equipment. The policies and procedures would list the several levels of training.

SWGDE advocates that "the validation testing shall be documented in detail to enable independent replication and shall be written before testing begins" (Evidence, Scientific Working Group on Digital Evidence, 2009, p. 5). Remarkably, 80.3% document the validation and testing process and their results, leaving 19.7% that do not. A majority of the respondents stated that they either kept an electronic log or a written log for documentation of their validation and testing process. An examiner should not only document, but also keep a backup of the document. This may be in the same form as the original document or in a different form. For example, one document may be on a USB drive, while the other is on a server designated by the digital forensic lab, or one document may be on a USB drive, while the other is a paper copy kept in a designated spot by the digital forensic computer lab. This documentation could be used in court if there was a question about the testing process.

The courts may not be familiar with the methods and practices of the digital forensic examiners. There is also limited research on the methods that examiners employ. The programs used to perform the validation testing, such as Forensic Tool Kit, are generally accepted by not only the digital forensic examiners, but also by people outside of the digital forensic community. Due to the fact that the programs are regularly used to perform the examinations, they are considered reliable. The programs used to perform digital forensic examinations have error rates associated with them, but it is impossible to associate an error rate with each examiner who performs the examination. This leaves the error rate with an unknown factor, so it is impossible to give an exact error rate for the process as a whole. In this survey, 14.3% of respondents had been asked in court about their validation process, and 85.7% had not been asked. One examiner stated that they have had their validation manual subpoenaed by the defense on two occasions.

The examiner thought the defense was expecting them not to have one, and after it was discovered, the case was resolved.

The second research question was, "What primary methods are used to validate and test digital forensic tools by digital forensic labs and examiners in the United States?" Most of the examiners used Forensic Tool Kit (FTK) or Encase for their examinations. Some of the other popular answers were WinHex, SPADA, HexEditor, X-Ways, and Linux. According to the examiners surveyed, 95% stated that they perform validation testing on their digital forensic tools. The results also showed 90.2% use standardized data sets to perform their validation testing.

Forensic Tool Kit (FTK) and Encase are two primary tools used by digital forensic examiners for their examinations. This is significant because it shows that most examiners use the same equipment to perform their examinations. It is also important to use more than one tool to validate and test to make sure the tool results are accurate. Policies and procedures should state which equipment and programs will be used to examine evidence. This could also help the examiner to have a set direction to follow, or if they are not sure what to use, it will provide information on what tools or programs are the most beneficial to use on the digital evidence item. The examiner should also have the operations manuals and other documentation for all equipment and software used by the examiner available to them (Evidence, Best Practices for Computer Forensics Version 2.1, 2006, p. 5).

Largely, the examiners perform their own validation testing on their digital forensic tools. Since most agencies do not have policies and procedures set in place about validation testing, it is left up to the examiners. It is important for examiners to perform validation testing on their

forensic tools. This information shows that most examiners do perform validation testing on their tools; however, there are still some examiners who are not performing testing. Policies and procedures for these labs should state that validation should be performed by the examiner to make sure that the software programs are working properly. There should be someone other than the examiner to perform an examination on the digital forensic software. This other person performing the check would help lower the chance of human error. This could be someone designated by the lab or, possibly, someone hired from outside. This other examiner would also provide the documentation, along with the results on the testing they performed. The majority of the examiners use standardized data sets to perform validation testing. Examiners prefer the method of using standardized sets of data to test their digital forensic tools. There are pre-created data sets, or examiners can create their own data sets.

The third and final research question was, "What barriers do examiners face to validate and test their digital forensic tools?" Respondents stated that time, case load, and the number of tools, along with their updates, were some obstacles and limitations when performing validation and testing of digital forensics tools. Also, a few stated that data sets were issues.

Case load and the number of tools and updates are two aspects of a single obstacle: time. Standing policies and procedures may help with the obstacle of time. If the digital forensic labs had set policies and procedures to follow, it might eliminate some of the guessing for the examiners. Policies and procedures would state who performs the testing, when to perform the testing, what data sets to use, and how to document. If the labs had a designated day and time period that they performed the testing, the examiner would not have to try to find time to fit in the testing. Most labs have large workloads, which keep the examiners very busy. The obstacle of a large case load will never be eliminated because of the growing number of items containing

evidence of digital forensic value. However, designated data sets may be able to help with the obstacle of tools along with their updates. Some examiners are making their own data sets, which takes time. If the examiners had designated data sets, it might help with testing the tools. The examiner would be able to test the functions more quickly and more accurately with known data sets.

Recommendation for Future Research

Future research may use methods of contacting digital forensic examiners to participate other than the IACIS listserve, to give a broader sample of examiners. The broader sample of examiners might be beneficial by adding more to the survey.

Future research might also want to make more of the questions require answers on the survey. An online survey can be constructed so that the examiner must give an answer before he or she can move on to the next question. The disadvantage of making the examiner answer more questions is that he or she might not feel comfortable with the answer and exit the survey.

The examiners might be able to provide more detailed information on the barriers that digital forensic examiners face. This information could be beneficial to finding specific solutions to help the examiner with the barriers to improving the testing processes. Also, private sectors in digital forensics may have different barriers and methods for validation testing. Researching private sectors may provide different information than from other agencies.

Conclusion

A majority of the digital forensic examiners in the United States did perform validation testing. It was good to find out that the examiners across the United States were performing the testing, even if it proved to be difficult for them due to lack of time and large workloads.

However, surprisingly, most of them stated that they do not have set policies and procedures to perform this task.

The lack of set policies and procedures is a large issue, not only for the examiners, but for digital evidence as a field. Some of the examiners follow their own made-up policies and procedures without any real guidance about what they should be. This can cause issues in acquiring accreditation for those labs.

The digital forensic examiners also stated that they are creating their own data sets to perform their validation testing. This should also be designated in policies and procedures. If the examiners had a specific set of testing data, it would make testing easier and simpler for them to perform. This could also save the examiner time by providing a designated set of data.

If nationally accepted policies and procedures were in place, it would help the digital forensic labs and examiners. The set policies and procedures would help the lab acquire accreditation. Also, they would help the examiners in many ways. One way they would be helpful is by saving the examiner time. He or she would have set procedures in place to follow for his or her examinations.

References

American Society of Crime Laboratory Directors Laboratory Accreditation Board. (2012, July 26). *ASCLD/LAB Accredited Laboratories*. Retrieved July 28, 2012, from American Society of Crime Laboratory Directors Laboratory Accreditation Board: http://www.ascld-lab.org/labstatus/labstatus.html

Beckett, J., & Slay, J. (2007). Digital Forensic: Vailation and Verification in a Dynamic Work Enviroment. *40th Hawaii INternational Conference on System Science*, 1-10.

Bianchi, R. P., & Pollitt, M. (2006). Digital Evidence. In A. Mozayani, & C. Noziglia, *The Forensic Laboratory Handbook Procedures and Practice* (pp. 79-90). Totowa: Humana Press Inc.

Bradburn, N. M., Sudman, S., & Wansink, B. (2004). *Asking Questions.* SanFrancisco: Jossey-Bass.

Evidence, S. W. (2009, January). *Scientific Working Group on Digital Evidence.* Retrieved March 23, 2010, from SWGDE Recommended Guidelines for Validation Testing Version 1.1.

Evidence, S. W. (2009, October 27). *Scientific Working Group on Digital Evidence*. Retrieved May 22, 2010, from Scientific Working Group on Digital Evidence: http://www.swgde.org/index.html

Feder, H. A., & Houck, M. M. (2008). *Succeeding as an Expert Witness.* Boca Raton: CRC Press .

Guo, Y., Slay, J., & Beckeet, J. (2009). Validation and Verification of computer forensic software tools-Searching Function. *Science Direct*, 1-11.

Johnson, T. (2006). Challenges to Digital Forensic Evidence. In T. Johnson, *Forensic Computer Crime Investigation.* CRC Press.

Nardi, P. (2003). *Doing Survey Research.* Boston: Pearson Education, Inc.

Nardi, P. M. (2003). *Doing Survey Research.* Boston: Pearson Education Inc.

Salant, P., & Dillman, D. (1994). *How to Conduct Your Own Survey.* New York: John Wiley & Sons, Inc.

Scribner, H. (2008). Rigorous Analysis of the Class Certification Expert: The Roles of Daubert and the Defendant's Proof. *Review of Litigation*, 71-130.

Specialists, T. I. (2010, March 20). *Home: About Us*. Retrieved 09 20, 2010, from IACIS The International Association of Computer Investigative Specialists: http://www.iacis.com/home/about_us

Technology, N. I. (2008, December 18). *National Institute of Standards and Technology.* Retrieved March 23, 2010, from The CFReDS Project: www.cfreds.nist.gov

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

Wilsdon, T., & Slay, J. (2005). Digital Forensic: Exploring Validation, Verification & Certification. *First International Workshop on Systematic Approaches to Digital Forensic Engineering*, 1-8.

Appendix A

Current state of Validation and Testing of Digital Forensic Tools in the United States

1 Gender _____M _____F

2 Age _____

3 What type of agency do you work for? Local _____County_____ State_____ Federal_____Private_____

4 What is your job title? _____

5 Do you have a digital evidence machine? Yes _____ No_____

6 What operating system does the computer use? (example: Windows 7, Windows Vista)_____

7 What digital evidence program do you use? (example FTK, Encase)_____

8 Do your digital forensic examiners validate and test their tools? Yes _____ No_____

9 Are these tests performed by one individual or does every examiner perform their own testing?_____

10 Does your agency have a formal protocol to vaildation testing? Yes _____ No_____

11 If so briefly describe protocol

_____

_____

_____

_____

12 How often are test performed? (example: weekly,Quarterly, Annually, Receive New Version) _____

13 Do you test each function or the program as a whole? _____

14 What data is used to perform the test? _____

15 Where did you get the data? _____

16 How much time does it take you to complete the validation testing? _____

17 What tools do you use to validate your results?

18 What limitations do you have in performing validation testing?

_____

_____

_____

19 Do you document the process and your results? Yes _____ No_____

20 How do you document your results?

_____

_____

_____

21 If not performing validation testing, why not?

_____

_____

_____

22 Have you ever been asked in court about your validation process? Yes _____ No_____

23 Recommendations?

_____

_____

_____

_____