Disheveled Digital Forensics: The Impact of Inconsistent Standards, Certifications, and Accreditation

Joshua S. Moulin

A Capstone Presented to the Information Technology College Faculty
of Western Governors University
in Partial Fulfillment of the Requirements for the Degree
Master of Science in Information Security and Assurance

November 15, 2014

Abstract

Technology and digital evidence are at the forefront of nearly every criminal, civil, and corporate investigation in the world. For the past thirty years digital evidence such as computers, cellular phones, tablets, servers, GPS devices, gaming consoles, storage devices, and network infrastructure devices have been forensically analyzed and presented in legal proceedings. In many cases digital evidence has been the "smoking gun" leading to successful convictions, lawsuits, employment terminations, and exonerations.

Although digital forensics has been recognized as a legitimate forensic science and has been utilized in the criminal justice system for the same length of time that DNA has, the discipline is anything but disciplined. Within the United States, any law enforcement agency, business, or individual can open a forensic "laboratory" and begin providing services without having to demonstrate even foundational knowledge, skills, or abilities. To further evidence this, within the law enforcement community alone there are only 67 digital forensic laboratories accredited to the ISO 17025:2005 standards for the nearly 18,000 law enforcement agencies in the country.

The lack of requirements for digital forensic practitioners to be certified in their discipline, be accountable to industry best practices and standards, or work out of accredited laboratories places the credibility of this forensic science in jeopardy. This paper will discuss the risks and impacts associated with unskilled practitioners who perform digital forensic analysis. Also included will be an examination of some legal cases that highlight the risks identified within the paper. Research and practical experience will be drawn upon to provide the reader with proposed solutions to improve the quality of the digital forensic discipline. Topics such as

forensic analyst training, proficiency testing, certification, best practices, policies and procedures, and laboratory standards and accreditation will be discussed.

The good news is that much of the work has already been done to identify digital forensic best practices and laboratory standards. This paper will provide a framework for digital forensic practitioners and managers to comply with best practices, standards, guidelines, and analyst certification and training within the discipline as well as minimum requirements that should be met before digital forensic evidence is allowed to be introduced into a legal proceeding.

Keywords: digital forensics, computer forensics, digital evidence, forensic laboratory accreditation, forensic certifications, digital forensic best practices

Table of Contents

Disheveled Digital Forensics: The Impact of Inconsistent Standards, Certifications, and Accreditation

Introduction

Digital evidence is being introduced in courtrooms and legal proceedings across the United States, often being presented as irrefutable. Many believe that digital devices do not lie; claiming that the evidence is either there or it is not. While it may be true that digital evidence is either there or it is not, the correct interpretation of that evidence is an entirely different issue. One incorrect assumption about how a particular file was discovered on a hard drive or which user was responsible for downloading data from the Internet could mean the difference in a business's future or a defendant's freedom. Many forensic analysts, particularly those found within law enforcement agencies, lack the necessary training, budgetary resources, administrative support, and knowledge to adequately perform digital forensics. Compounding the problem with law enforcement digital forensics specifically is the traditional rank structure and turnover of personnel, as well as a lack of understanding by many administrators. Beyond the certification and training shortfalls of many analysts, there is no rigor to a majority of forensic laboratories. Most of these "labs" do not comply with industry best practices or standards and nearly none are accredited to provide forensic services.

This capstone report examines the devastating results that untrained digital forensic analysts working outside of standards and best practices can produce. By reviewing actual legal cases that were impacted by improper digital forensics, research available on the subject, and personal experience, this capstone provides a suggested path forward and framework for digital forensic laboratories. The framework provides the reader with sufficient information on how to comply with industry best practices and place the necessary diligence within this forensic

science. This paper will also provide attorneys, judges, managers, and law enforcement administrators with information on what minimum standards should be in place to provide credibility to the forensic analyst, the digital evidence, and the laboratory.

Project scope

The scope of this capstone is primarily focused on three areas: digital forensic analyst training and certifications, digital forensic laboratory accreditation standards, and digital forensic best practices and policies.

While the focus area applies to all practitioners in digital forensics regardless of their affiliation or employer, the majority of the focus will be on law enforcement. This is because law enforcement has the most individuals practicing digital forensics and the opinions rendered by law enforcement forensic analysts have arguably the largest impact on society.

The scope also provides a framework that can be utilized by those in a position of authority over digital forensic laboratories and practitioners as well as the practitioners themselves. Since nationwide requirements for digital forensic laboratory accreditation and mandatory certification of analysts will take considerable time to implement, the intent of this capstone is to provide the reader with a litmus test when considering the admissibility or credibility of digital forensic evidence from a particular analyst or laboratory.

The usefulness and relevancy of this capstone to the few digital forensic laboratories that already hold International Organization for Standardization (ISO) 17025 accreditation is limited. This capstone is also not applicable to those companies or individuals that conduct digital forensics in the course of breach investigations and incident response only, where the results of the digital forensics are not intended to be presented in a court or used against any individuals.

Defense of the Solution

For the digital forensic discipline to progress and be treated with the level of respect it deserves within the scientific community, the changes outlined in this capstone must take place. Digital forensic examiners must be certified in their discipline and have the requisite education. Agencies and businesses performing digital forensics must have the proper policies, procedures, and standards to ensure the integrity of evidence and of their employees. Digital forensic laboratories must have proper practices and standards to meet a baseline of best practices in order to ensure evidence is handled properly.

Digital forensics is never going away and it is being used in exceptional ways to solve crimes, hold people accountable, and vindicate the wrongly accused. It has also been misused, presumable unintentionally, which puts the discipline in jeopardy of no longer being accepted as a science.

Much of the solution is already available to practitioners and those that manage digital forensic laboratories. Excellent certifications exist for analysts, standards have been developed for laboratory accreditation by the International Organization of Standardization (ISO), and many organizations have written digital forensic best practices. The issue is not a lack of available knowledge, but rather a lack of desire to be held accountable. The solution presented in this capstone is a framework that anyone practicing digital forensics should comply with in order to move the science forward into the well-respected discipline it should be.

Methodology Justification

The approach is to provide individuals with the necessary knowledge to understand what standards should be applied to digital forensics and how to ascertain if digital forensic laboratories and analysts are meeting industry best practices. The approach was selected because many non-technical people lack the understanding to inherently know whether or not the opinion of a digital forensic analyst is made on sound scientific methodology. This approach will outline the current problem, the causes of the problem, and then a framework to correct the problem and what the minimum standards are that a forensic laboratory and analyst should possess. Since most of these standards already exist it makes for an easy transition vice proposing something completely new.

Organization of the Capstone Report

The capstone report is segmented into the following key areas:

1. A brief history of digital forensics and how it is being used in criminal and civil litigation.
2. The problem background, which will discuss the lack of forensic standards, training requirements, laboratory accreditation, and how this has already led to failures in investigations.
3. Solutions for the problem including the availability of digital forensic analyst training, education, and certification, the availability of policies, procedures, and best practices, and the availability of laboratory accreditation programs for ISO 17025 forensic laboratories.

4. A framework presented on the minimum standards any individual, business, or agency performing digital forensics should meet and what others should expect of digital forensic analysts to ensure the integrity of the forensic discipline.

Systems and Process Audit

This capstone examined a number of systems and processes used in digital forensic science across the United States. Specifically, various policies and procedures, laboratory accreditation standards, forensic analyst certifications and educational training programs, and case law were reviewed. While many of these items exist, the implementation of both systems and processes vary greatly across the country.

Audit Details

The scope of this capstone audit was public and private digital forensic laboratories within the United States. The audit reviewed five court decisions that contained findings by a judge that were directly relevant to problems in forensic science, four of which were specifically about digital forensics. Three of the five cases were found as a result of media stories on the Internet that highlighted some problems with digital evidence during a trial. The full court decisions were found on the Internet and reviewed in their entirety to determine the legitimacy of the media claims as it pertained to the use or misuse of digital evidence. The other two cases were cited in research used in this capstone report and those cases were also obtained in their entirety and reviewed for relevancy. In order to be included in this capstone report, the court case had to indicate that forensic evidence was utilized in a criminal trial and that forensic evidence was either improperly handled, improperly interpreted, or both. The audit also reviewed research done in the area of the effectiveness of forensic science within the United

States, the maturity of the digital forensic science, and the available resources for digital forensic practitioners.

The audit found that digital evidence is being sought and examined in nearly every criminal case in the United States. The demand for digital forensic analysts and digital forensic laboratories is high, putting pressure on the limited resources that do exist. Nearly every crime imaginable has some tie to technology, such as tracking a person's whereabouts with a cellular phone or determining what user downloaded illicit images of child sexual abuse. This high demand combined with a lack of regulations for digital forensics has led to most public and private digital forensic labs to stand up some sort of "forensic lab" with no accreditation and sometimes with no certified analysts.

This trend is mainly due to a perceived lack of need to be regulated from both private and law enforcement digital forensic laboratories. Largely, the level of knowledge regarding digital forensics by judges and attorneys is low, allowing the testimony of digital forensic experts to go unchecked and unchallenged in many cases. As more attorneys receive training in digital forensics, cases are starting to come to light where digital forensic evidence was mishandled, incorrectly interpreted, or analyst credentials misrepresented. The cases highlighted within this capstone report as well as others found during research, validate the necessity for the framework offered herein.

Problem Statement

Computer forensics was coined in the early 1980's and by 1984 the Federal Bureau of Investigation (FBI) had started the first computer forensic team, originally called the FBI Magnetic Media Program (later called the Computer Analysis Response Team (CART)) (Kedziora, 2014). Similarly, the use of deoxyribonucleic acid (DNA) in criminal investigations

began in the 1980's as well, with the first DNA-based conviction in the United States in 1987 (Calandro, L, et. al, 2005). Despite the similar timelines of computer forensics and DNA forensics, the two disciplines have greatly departed in the structure surrounding these sciences.

When computer forensics first began the number of forensic analysis software tools were limited. Early forensic examiners learned a great deal about how files were written to disks and how file systems functioned. To recover deleted files, analysts had to manually re-link files together and carve them out of the unallocated space on a disk. Computer forensics was mostly used to examine computers or floppy disks in financial crimes and fraud cases and many of the current challenges did not exist. As technology has increased, so has the complexity of the forensic analysis of digital evidence. Mobility, encryption, rapidly changing hardware and software, multiple operating systems and file systems, cloud storage, the Internet of things, and large networks have dramatically changed the landscape of digital forensics.

As the examination of digital evidence began to encompass more than just computers, the name changed from computer forensics to digital forensics to better represent the discipline (Wikipedia, 2014). Digital forensic science is defined as the process used to acquire, preserve, analyze, and report on electronically stored information using scientific methods that are demonstrably reliable, verifiable, and repeatable, such that they may be used in judicial and other formal proceedings (SWDGE, 2014). Digital forensics focuses on the examination of all types of electronic evidence including computers, cellular phones, tablets, GPS devices, gaming consoles, servers, cloud computing, email repositories, network devices and logs, and peripheral storage devices such as USB drives and optical media.

Government agencies and private corporations have seen the benefit of digital forensics from convicting murders to proving employee misconduct. Many executives in law enforcement

and private corporations understand why digital forensics is important, yet lack the knowledge to understand the best practices that are needed for digital forensics to be successful and produce valid results. In a survey conducted by the SANS institute for digital forensic and incident response professionals, 25% of respondents were government forensic examiners most likely working for law enforcement (SANS, 2013). This group accounted for twice as many as any other industry classification surveyed.

The problem of a lack of standardization is particularly obvious within the law enforcement community. When standardization has been pushed on the digital forensic community in the past, primarily the law enforcement community has argued that digital forensics is more of an investigative tool than a forensic science. This argument was made to eliminate the necessity of education, certification, and accreditation. Digital forensics has been recognized by many organizations as a forensic science for years, the latest being the Scientific Working Group on Digital Evidence (SWGDE) officially naming it as a forensic science in September of 2014 (SWGDE,2014). Many in law enforcement believe that individuals performing digital forensics are synonymous with a traffic officer using a handheld radar: they understand how to use the tool (the radar), but cannot testify as to the science behind how radar works. This analogy has been used by law enforcement several times, saying that a digital forensic examiner should be trained in whatever software tool they are using for forensics, yet should not have to understand how the tool functions. This logic is woefully flawed and would never be accepted in any other forensic science. Imagine a DNA analyst testifying that they understand what buttons to push on their DNA sequencer, yet cannot testify to how it actually works. The DNA analyst would never be allowed to testify as an expert witness and that laboratory would probably never be used again. Unfortunately, law enforcement would like to

enjoy the benefits of introducing digital forensic evidence as scientifically acquired in courtrooms and render expert witness opinion testimony, yet in most cases they do not want to be held to the same standards as traditional forensic laboratories. It should be noted that a small subset of law enforcement agencies in the United States are doing an exceptional job at digital forensics by meeting best practices, however the majority are still falling behind.

Many law enforcement agencies are facing budget shortfalls, high turnover of personnel, and competing needs for resources. This often makes digital forensics a lower priority, reducing the resources available to implement best practices or send analysts to expensive forensic training. Additionally, because of the quasi-military rank structure used in law enforcement and the archaic way of managing promotions, officers who want to further their career often must leave a digital forensic position and go back to a uniformed position in order to advance. Many law enforcement agencies such as the San Jose, California Police Department have mandatory rotations of their personnel (USDOJ, 2007). This means that after a few years of specialized training in digital forensics, these officers are removed from the forensic unit and placed back onto the street in uniform. This is a perfect example of an agency (and many others are just like this) that does not view digital forensics as a science, but rather just another investigative tool. When a law enforcement digital forensic analyst becomes passionate about forensics and decides to make it their career path, in most agencies that law enforcement officer hits their glass ceiling. Most digital forensic analysts in law enforcement are police officers, deputies, and detectives; among the lowest paid members of a police department. After a few years of experience, law enforcement digital forensic analysts realize they can command significant salaries in the private sector doing much the same work and have chances for upward mobility in their career path while not having to be exposed to cases such as child pornography. A skilled law enforcement

digital forensic analyst could easily go from a salary at a law enforcement agency of $50,000 per year to a starting salary of $80,000 to $100,000 per year performing digital forensics for a private corporation. This is another factor in law enforcement's difficulty in attracting and maintaining proficient digital forensic analysts.

Despite there being some exceptional digital forensic analysts and laboratories in the United States, many of the individuals performing digital forensics are not true experts, finely honed in this science. Often the law enforcement officer who is the best in the department using Microsoft Word is selected to be the digital forensics "expert" in the department. Many of these officers self-teach themselves and are able to get a minimal amount of forensic hardware and software. Some of the officers will be allowed to go to a small amount of training and most will not obtain any certifications in the field. Some of the certifications that are obtained do not fully qualify them to conduct digital forensics. Law enforcement agencies have access to federally-funded digital forensic training like the Federal Law Enforcement Training Center (FLETC) Seized Computer Evidence Recovery Specialist (SCERS) training. This ten-day training session provides law enforcement with basic computer forensic training and the students leave with a computer designed to perform forensic analysis and copies of commercial forensic software, all at no cost to the law enforcement agency (FLETC,2014). While this is an excellent starting point, in many cases this will be the only training a law enforcement digital forensic analyst will receive. According to the syllabus on FLETC's website, the training does not discuss courtroom testimony, policies and procedures, laboratory standards, evidence storage, Mac forensics, Linux forensics, cloud storage, mobile phones, or networking (2014). It is understood that this course is a starting point, yet most who graduate from the program immediately begin conducting forensic examinations in criminal cases and testify as an expert with this limited foundational

training, and rarely have a peer or mentor at their home agency to supervise their work. This trend has produced what is commonly referred to as "Nintendo forensics" (Carvey, 2005) or "tool jockeys": that is digital forensic analysts that heavily rely on pushing buttons in forensic software programs and exporting the results of the programs with little to no thoughtful interpretation or validation of the data.

Of the nearly 18,000 law enforcement agencies in the United States (Law enforcement in the United States, 2014), every agency needs access to some form of digital forensic analysis services. Law enforcement agencies are left with a few choices when it comes handling digital evidence: contract with another agency, use a regional laboratory, contract with a private laboratory, perform the work in-house, or do not include digital evidence in any criminal investigation. Since there is only one accredited digital forensic laboratory in the United States for every 300 law enforcement agencies, most agencies decide to perform digital forensics in-house.

ASCDL/LAB added digital forensics to its disciplines for laboratory accreditation over ten years ago, in 2003. ASCLD/LAB is now accrediting digital forensic laboratories under the ISO 17025:2005 standards and currently there are 67 forensic laboratories in the United States accredited by ASCLD/LAB in the digital forensic discipline (American Society of Crime Laboratory Directors, 2014). Although there are other accrediting bodies for ISO 17025, none of them have a current accredited laboratory providing digital forensic services.

Of the 67 ISO 17025 accredited digital forensic laboratories in the U.S., seven of them are private labs. Of the seven labs, only one is a private business solely focusing on accepting evidence from external customers; the others are internal corporate labs (ASCLD/LAB, 2014). This significantly reduces the available options for criminal and civil defense attorneys to submit

evidence to a private laboratory for analysis. Digital forensic evidence is being examined by individuals across the nation with no standardization in how it is performed or what minimum level of education or experience a digital forensic analyst should possess. Certification and accreditation in digital forensics is completely voluntary and most view it as unnecessary and excessive. Several criminal cases, some of which received international attention, have highlighted improper conclusions made by digital forensic analysts. In other cases, digital evidence was never even allowed to be presented because of spoliation, or the mishandling of the evidence which rendered it inadmissible.

Having a laboratory accredited according to best practices such as ISO 17025 removes many questions about the quality assurance of the laboratory and the personnel performing work. Accreditation is not the be-all and end-all or a magic solution to issues plaguing the digital forensic discipline. Accredited laboratories have been known to have issues with their findings as well, the only difference is that the laboratory accreditation standards generally help bring misconduct to light. For example, in 2014 the Oregon State Police quietly closed down their handwriting analysis unit after conducting an internal review of allegations involving bias, sloppy work, and dishonesty (Denson, 2014). A report to the U.S. Congress said, "In the case of laboratories, accreditation does not mean that accredited laboratories do not make mistakes, nor does it mean that the laboratory utilizes best practices in every case, but rather, it means that the laboratory adheres to an established set of standards of quality and relies on acceptable practices within these requirements" (National Research Council, 2009).

Of the eight factors that have been correlated with erroneous criminal convictions, one of them is errors in forensic science (Gould, et. al., 2013). Nearly every investigation has some technology component, increasing the demands on digital forensic analysts and laboratories.

Despite digital forensics being a forensic science, it has been relatively untouched by the standards and regulations required of other more traditional forensic sciences such as DNA, fiber analysis, hair analysis, latent fingerprints, and ballistics.

According to the National Research Council (2009) there are three main challenges to digital forensics: the lack of a standardized certification program or agreed upon qualifications for digital forensic analysts, some agencies treating digital forensics as an investigative tool rather than a forensic science, and there is wide variability in the education, experience, and training of digital forensic analysts. As digital evidence is being submitted more and more frequently in courtrooms, the implications of the challenges identified by the National Research Council are becoming evident.

The lack of oversight in the digital forensic science community has led to poor court decisions and misrepresentation by digital forensic analysts. As bad precedence is created, more scrutiny will be placed upon digital forensics by the legal system. Digital forensics has solved amazing cases and there are many individuals who are superb forensic analysts, however none of that will matter if the discipline loses its credibility. In a quote given to NPR about another forensic laboratory scandal, forensic consultant Brent Turvey said, “The forensic science is not like any other community. It’s not beholden to anyone other than the police and prosecutors. The question is: Are we creating crime fighters, or are we creating scientists?” (Becker, 2014).

In 2014 a private digital forensic analyst conducting investigations for the defense bar in New Hampshire was convicted of a misdemeanor because she was found to have misrepresented her digital forensic qualifications (Concord Monitor, 2014). In 2007 another digital forensic analyst was convicted of perjury during a child pornography case in California after falsely claiming he had received several college degrees (Gaudin, 2007). Unfortunately, there is a long

list of forensic analysts in the United States who have been caught being untruthful about their credentials. This behavior calls into question the analyst's credibility and may lead to reopening all cases the analyst was involved in throughout their career. Accreditation and validation of forensic analysts would help stop this type of behavior from occurring.

The high-profile Casey Anthony murder trial is another example of a case that brought to light quality control issues in digital forensics. At issue in this case was contradicting information provided by two different forensic software tools. The state was attempting to prove that the defendant murdered her daughter with premeditation and one of the keyword hits located by law enforcement forensic analysts on a computer from the defendant's home was "chloroform." One of the forensic software tools reported the website containing the search hit for chloroform was visited 84 different times and the other software tool only reported one single visit (Wilson, 2011). The software tools were simply interpreting raw data from a Mozilla Firefox Mork database and using even free software tools, the forensic examiner could have reviewed this raw data themselves. Instead of immediately determining the cause of the discrepancy, law enforcement produced reports showing the conflicting results of the two software tools. In trial, the prosecution and digital forensic analyst chose to introduce the forensic report showing the chloroform website was visited 84 different times instead of the report indicating it had only been visited once. The defense was able to prove the state's interpretation (and that of the second software tool) was incorrect and in actuality the chloroform website was only visited once. The defense was able to show the 84 hits were for a different website altogether, MySpace.com. The defense attorney, Jose Baez, stated, "the state's computer forensic evidence involving chloroform research, a central element of their premeditation argument, was used to mislead the jury and that the flaws in that evidence infected their entire

case like a cancer." (Wilson, 2011). Craig Wilson, who wrote a detailed blog entry about this case and the forensic evidence introduced at trial is also the creator of the forensic software tool NetAnalysis. NetAnalysis also happens to be the first forensic tool used on the Casey Anthony evidence and produced the correct data interpretation. Wilson was able to obtain the actual evidence from Casey Anthony's computer and do his own forensic analysis, showing how the raw data could have been validated by law enforcement. In his carefully worded conclusion, Wilson stated, "Whilst it may not be possible to validate a tool, it is possible to validate the results against known data sets. If two forensic tools produce completely different results, this should at least warrant further investigation." (Wilson, 2011).

In this same case, the law enforcement analyst was incapable of extracting incriminating Internet search terms from the defendant's computer, which were later revealed by the defense computer forensic expert after the defendant was acquitted (Alvarez, 2012). Not every digital forensic analyst is going to find every single artifact on a computer, however when these two significant errors are combined it paints a picture of ineffectiveness. ISO 17025 accreditation standards of tool validation, peer reviewed work, and analyst education and certification requirements may have led to a different outcome.

In another case, a police detective in Cary, North Carolina deleted all data from a BlackBerry cellular phone and its Subscriber Identity Module (SIM) card that belonged to a homicide victim. The defense claimed the evidence was spoiled by law enforcement actions and that the smartphone contained exculpatory evidence for the defendant. During the testimony offered by the detective, he admitted to not being qualified to conduct digital forensic examinations, or even what a SIM card was, yet he was accessing the original digital evidence to perform an exam. An expert was later hired to review the testimony of the Cary Police detective

and attempt to reconstruct the actions taken by the police detective. The expert's opinion was that both the contents of the BlackBerry and the SIM card were deleted by the detective's actions and that the detective's actions were, "highly likely intentional." (Levitan, 2011). Digital evidence spoliation due to mishandling is becoming a growing problem.

The training provided to most law enforcement forensic examiners has remained relatively unchanged over the past ten years. With few exceptions, the core areas taught to forensic examiners include conducting post mortem or "dead box" forensic analysis on Windows based computers. Any advanced topics such as network forensic analysis, network protocols, mobile device forensics, Mac forensics, Linux forensics, RAM analysis, malware analysis, or live imaging all require additional advanced courses. Largely, law enforcement forensic examiners are ill-equipped to respond to network intrusion cases, complex network forensic needs, and other advanced cases. Forensic analysts working for federal government agencies or large corporations generally have more training and experience in the area of advanced technologies, especially in networking and intrusion investigations than law enforcement analysts.

As technology continues to rapidly change and evolve, digital forensic analysts must stay current on new techniques and tools available. While not new by any means, the acquisition and collection of Random Access Memory (RAM) of a running computer is still largely not done by law enforcement agencies when seizing a computer. RAM can contain massive amounts of relevant evidence which could be used to convict or exonerate an accused individual. Items such as open file shares, past and present network connections, logged on users, processes running on the computer, usernames and passwords, open files, clipboard contents, websites visited, search terms, and more can be recovered from RAM. Essentially, if a running computer has 8 gigabytes

(GB) of RAM installed for example and an investigator fails to obtain that 8 GB, then they have failed to preserve and obtain 8 GB of evidence. In most law enforcement cases, the digital forensic laboratory staff does not have the time or personnel resources to respond to every computer seizure in their jurisdiction; leaving it to police officers, detectives, and crime scene technicians to seize electronic evidence. Even though digital evidence has been used by law enforcement for thirty years, many police academies are still not providing even basic training to recruits about digital evidence. Many free tools exist that have been created by private companies and law enforcement that would allow police officers with limited knowledge to plug in a USB thumb drive, acquire the contents of RAM, and provide both the computer and RAM contents on the USB thumb drive to the forensic laboratory.

An argument could be made by attorneys that failing to acquire RAM is spoliation. Once the computer is powered off, the contents of RAM are volatile and will never again be available for collection in the same state they were when the computer was seized. With computer hacking, advanced malware, and cloud computing being prevalent, the contents of RAM are more important than ever before. There is malware being used to exploit computer systems that only reside within RAM, called memory resident malware, or non-persistent malware (Kornblum, 2013). Without obtaining the RAM, there may be no way of knowing if a system was compromised by malware or what information was flowing into or out of the digital device.

Malware is becoming more sophisticated with increasing evidence of malware being written to thwart reverse engineering attempts and zero-day malware and rootkits designed to evade detection by traditional anti-virus software. According to a study produced by Mandiant, only 54% of intrusions were caught with antivirus software (Mandiant, 2012). Many digital forensic examiners are not skilled in the area of malware reverse engineering, static malware

analysis, or dynamic malware analysis. This makes it extremely difficult for an untrained forensic analyst to render an opinion as to whether or not malware could have been responsible for activity found on a digital device during a forensic examination.

Highlighting an example of the danger of malware and unskilled forensic analysts is a 2013 California case. This case involved an individual that was found to have child pornography on his computer and was arrested and criminally charged for child pornography. The defendant took his computer to a Staples store because he believed the computer was infected with a virus. When a Staples employee booted the defendant's computer, the employee saw a screen pop up that said, "We Are Anonymous, We are Legion, You have been caught with Child Porn and have been reported to Interpol." Included with the banner were four thumbnail images of child pornography. The Staples employee contacted local law enforcement and reported the incident. The police took the computer and wrote a search warrant for it and then sent the computer to a United States Secret Service special agent who performed a forensic preview on the computer. The Secret Service agent located the four images of child pornography all contained within the temporary Internet files of the computer and all created on the hard drive on the same date within less than one minute of each other. This activity is completely consistent with all images being downloaded into cache from viewing a webpage in a browser. The law enforcement analyst found no other illegal images on the hard drive, no evidence the images were ever viewed after they were created on the hard drive, no evidence of search terms indicative of a user searching for child pornography, or any evidence to establish the defendant had knowingly possessed these images (D. Fairweather, personal communication, 2013).

The defendant adamantly denied involvement in child pornography after his arrest and said his computer was infected with a virus and his browser redirected to a child pornography

website. Law enforcement was quick to discount the "virus did it" defense, but the prosecuting attorney felt it necessary to re-examine the computer. It was not until the prosecuting attorney began looking at the facts of the case and asked for assistance, that it became clear this case is not a prosecutable case and the charges were dismissed.

Law enforcement digital forensic laboratories often do have a large backlog of cases which pressures them to perform haphazard examinations and get cases turned around quickly. The above mentioned case is a perfect example of the impacts of incorrect conclusions and unfortunately, is all too common. Law enforcement refers to this rapid analysis practice as "forensic previews" or "forensic triage" and is designed to obtain just enough evidence to support an indictment or criminal information and then the examiner moves on to another case. This practice may seem on paper to help reduce the backlogs of digital evidence, but lacks impartiality or scientific methodology. If a law enforcement forensic analyst's sole responsibility is to find evidence to support an arrest or indictment it eliminates any separation of duties and may become a self-fulfilling prophecy. This approach of looking solely for evidence to convict is exactly what Abraham Maslow meant when he said, "if all you have is a hammer, everything looks like a nail." Most agencies that practice this tiered style of triage forensics do not perform completely thorough forensic examinations on a digital device until a defendant has refused to accept a negotiated plea and a trial date is set. Agencies refer to this as trial forensics and this may be the only time a full analysis is completed on the evidence. Sometimes trial forensics occurs years after the initial filing of criminal charges against a defendant due to the slow moving justice system in the United States.

Many law enforcement forensic analysts wear multiple hats as both investigator and forensic analyst. In a recent unscientific survey conducted for law enforcement digital forensic

examiners, of the 26 agencies that provided information, 58% of the agencies allowed their forensic analysts to also maintain a normal investigative caseload (F. Helmcke, personal communications, 2014). The average ratio of law enforcement officers to digital forensic analysts in the survey was 181:1. Often these individuals are assigned to Internet Crimes Against Children (ICAC) units and act as the original undercover officer making a case, the interrogator and arresting officer of the suspect, and the forensic analyst. This lack of separation of duties is ripe for noble cause corruption.

As in the California case, when suspects are charged due to limited information found on a computer with no thorough analysis done to determine how the evidence got on the digital device or who may have been responsible for putting it there, innocent people may be accused. There is little more stressful or devastating to a person and their family than being falsely accused of a crime, especially most of the felony-level crimes involved with technology. An individual who is arrested for child pornography possession for instance, may very likely lose their job, may be removed from their home if they have children, may go into significant financial debt to mount a criminal defense, and may lose a spouse or other family members just from the allegation alone. With the age of the Internet media and law enforcement making a point to publically announce most arrests involving technology, even if a case is later dismissed or a defendant is acquitted, the original allegations will remain online forever. A person can never fully be whole again after suffering the effects of a false criminal accusation.

Law enforcement carries an enormous responsibility in this area of criminal investigations since many judges and attorneys do not understand digital forensics enough to effectively cross-examine government witnesses or identify when incorrect conclusions are made (Garett, B.L., & Neufeld, P.J, 2009). Particularly in cases that evoke emotional responses from

judges and juries, law enforcement can easily allow photographic and video evidence such as images of child pornography overshadow the highly technical aspects of digital forensics.

Short of other compelling evidence, no person should face criminal charges from digital forensics alone until a thorough analysis has been by a certified forensic analyst using validated forensic tools and operating in accordance with best practices and accreditation standards. In research it was found that some agencies do not even perform basic steps such as scanning a hard drive for malware before making an arrest. In one forum often used by digital forensic analysts, a law enforcement analyst wrote asking for advice in a child pornography case that was scheduled for trial. The law enforcement official admitted finding a virus on a computer seven years after the defendant was arrested for possession of child pornography and that the virus was capable of allowing a remote user to control the computer. The law enforcement official wrote, "So we are expecting the defense to try the old, 'The virus allowed someone else to put this CP [child pornography] on the computer.'" The law enforcement official also stated this would be the agency's first-ever trial for child pornography because, "all of the others have plead out" and further stated that, "This guy just didn't like the offer from the prosecution and is fighting it." These statements sum up the problem with digital forensics in law enforcement powerfully. At no time did the law enforcement official consider that the defendant may be fighting the charges because they are innocent and that the virus very well could have been responsible for the illicit material located. Obviously from the content of the communication, a thorough analysis was not conducted since the forensic analyst was asking for help on how to refute the virus defense and the virus was not found until seven years after the defendant was arrested.

The digital forensic discipline is at a pinnacle point in its life. The courts, higher education, and the scientific community are all pushing for the standardization of digital

forensics. The biggest resistance to this standardization is the practitioners themselves. Digital forensics may face a similar fate as that of the polygraph if standards are not followed: viewed only as an investigative tool, but not as a forensic science that is admissible in court.

Problem Causes

The overarching causation of this problem is the lack of identifying digital forensics as a forensic science by law enforcement agencies, private individuals, and corporations. Many excuses have been made by these groups as to why placing standards on digital forensics will reduce the effectiveness of digital forensics, however this has been disproven. Until standards are required by the federal government and/or individual states for the licensure of digital forensic practitioners and forensic laboratories, this problem will persist.

Contributing factors to the major cause is a lack of education for managers and executives as well as for judges and attorneys. Although managers and executives may not want to dedicate the resources necessary to achieve analyst certification and laboratory accreditation, if judges and attorneys begin requiring this level of professionalism, there would be no choice but to comply.

Regardless of whether laboratory accreditation is sought after applying this capstone's framework of best practices, the topic of forensic analyst training must be discussed by the laboratory. Analyst certificating in their field and annual proficiency testing is at the core of credible forensic science (National Research Council, p. 207-208). Allowing an individual, public or private, to refer to themselves as a digital forensic analyst without a certification in the field should never be allowed. At a minimum, an individual without a certification should have to be mentored and their casework reviewed by a senior, certified analyst while the junior analyst is seeking certification.

There are a host of certifications available for digital forensics by a wide range of organizations and businesses. It is important for judges and attorneys to have some awareness of certifications and what the requirements were to obtain the certifications. There are some certifications, such as the AccessData Certified Examiner (ACE) that is a 90-minute free test given online and only tests an individual's ability to properly use the AccessData suite of forensic software tools (AccessData, 2013). It is important for forensic analysts to have certifications in the tools they use, however the ACE certification does not make an individual qualified to perform digital forensic analyses. When judges and juries here that someone is a "certified examiner" such as with the ACE certification, a false assumption may be made that the person is able to render expert opinions as to digital evidence.

The SWGDE produced a document that provides excellent guidance on what a digital forensic practitioner should be certified to in order to demonstrate the necessary proficiency (SWGDE, 2009). There are a few certifications available that meet the suggestions provided by SWGDE which include the International Association of Investigative Specialists (IACIS) Certified Forensic Computer Examiner (CFCE) certification, the International Society of Forensic Computer Examiners Certified Computer Examiner (CCE) certification, the SANS Global Information Assurance Certification GIAC Certified Forensic Examiner (GCFE), the GIAC Certified Forensic Analyst (GCFA), and the Encase Certified Examiner (EnCE). It should be noted that the IACIS CFCE is currently the only digital forensic certification to be accredited by the Forensic Specialties Accreditation Board (FSAB). Several other certifications exist which are very good and include written tests and may be excellent to supplement the above-listed certifications, but lack true practical examinations. These additional certifications include, but are not limited to the EC-Council Certified Hacking Forensic Investigator (CHFI), and the

Digital Forensic Certification Board's Digital Forensic Certified Practitioner (DFCP). Many colleges are also starting to offer associates, bachelor's, and master's degrees in the area of information security and digital forensics. A forensic examiner with a bachelor's or master's degree from an accredited college would have sufficient training to be qualified as a digital forensic analyst, but annual proficiency testing would still be required.

Many believe that implementing more controls over digital forensics will lead to exponential increases to an already overwhelming backlog of digital evidence. The flawed logic is that the people arguing this are essentially saying they would rather produce hasty incomplete work than go through a scientific and controlled process. Yes, it may add some time to the average case, however based on experience, this time is minimal. The risks of false accusations, false convictions, the guilty going free, or the loss of credibility to the digital forensic discipline far outweigh any inconvenience of implementing industry best practices.

Business Impacts

The most significant consequences of this problem include innocent people being wrongly convicted, guilty individuals going free, or the loss of credibility for the digital forensic discipline as a whole. There are other similar consequences for digital forensics used to support non-criminal investigations as well, such as civil litigation and employee misconduct investigations.

The innocent being wrongly convicted is a well-known problem. According to the Innocence Project (2014) there have been 321 post-conviction exonerations through the use of DNA in the United States. In many of these cases, additional forensic sciences other than DNA were used to convict these innocent individuals.

The business impacts may become more severe for digital forensic practitioners who choose not to embrace the notion that digital forensics is a science. In 2014, Senator Patrick Leahy (D-Vt.) and Senator John Cornyn (R-Tx.) introduced new legislation to reform the use of forensic evidence in criminal cases. This legislation is in response to the 2009 report from the National Research Council, *Strengthening Forensic Science in the United States: A Path Forward.* If this legislation passes, any laboratory that performs forensic examinations of evidence to support a criminal case and receives federal funding must meet the requirements of the proposed law. The proposed law does include many of the topics in this capstone, including analyst certifications, laboratory accreditation, and establishment of best practices (Criminal Justice Reform Act, 2014). It is clear that this is the direction the courts and lawmakers want to take forensic science and if laboratories want to continue to receive federal funding, they will eventually have to comply.

Business certainly will be impacted if the lack of digital forensic standards continues to manifest itself in the courtroom. It is critical that those practicing digital forensics do everything in their power to ensure the forensic evidence is presented truthfully and credibly. If a judge were to make a ruling that a certain practice in digital forensics was unreliable, it would have an immediate ripple effect across the country and upon criminal cases everywhere. Such activity is already occurring in forensic science for many of the reasons addressed in this capstone. In a 2001 ruling, the Florida Supreme Court reversed convictions of a defendant who was convicted of murder, armed robbery, and armed burglary because of poor forensic science. The judge stated, “In order to preserve the integrity of the criminal justice system in Florida, particularly in the face of rising nationwide criticism of forensic evidence in general, our state courts both trial

and appellate must apply the *Frye* test in a prudent manner to cull scientific fiction and junk science from fact" (Ramirez v. State of Florida, 2001).

Cost Analysis

This capstone will provide forensic practitioners and those operating digital forensic laboratories with a framework to achieve compliance with industry best practices. Higher education degrees, digital forensic certifications, digital forensic standards, and laboratory accreditation standards all already exist, minimizing the time and resources needed to implement them.

The costs associated with the implementation of the framework provided by this capstone would be:

1. Time resources needed to customize best practices for the particular organization and obtain management support for implementation.
2. Training costs to send personnel to the necessary training in order for them to become certified in their respective area of the digital forensic science.
3. Accreditation costs if a laboratory chose to become an ISO 17025:2005 accredited laboratory.

The costs for a laboratory to implement the above measures vary greatly depending on the number of personnel and the present condition of the laboratory. It is estimated to cost a minimum of approximately $6,000 annually for training and certification maintenance of a single digital forensic analyst. This would provide the analyst with one forensic conference or two virtual training sessions. Annual proficiency tests for each analyst would cost an additional $300.00.

Accreditation costs also vary depending on the number of personnel assigned to the laboratory. There are a limited number of accrediting bodies for ISO 17025 laboratories, with the most well-known being the American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB). While this capstone does not advocate for mandatory accreditation for all laboratories, it does strongly recommend mandatory compliance with best practices even if full accreditation is not sought. The minimum amount a laboratory should expect to spend on initial accreditation is approximately $6,000. This amount includes accreditation fees and the first initial assessment conducted by the accreditation assessment team. Minimum annual accreditation fees would be approximately $4,000 and also depends on the size of the laboratory and number of forensic analysts.

Risk Analysis

At its core, the identified problem is the lack of inconsistent standards, certification, and accreditation in the digital forensic discipline. The manifestation of this problem is improper handling of evidence which could lead to misinterpretations and ultimately to wrongful convictions or the guilty going free. Nearly anyone anywhere can proclaim themselves to be a digital forensic analyst and there is nothing that prevents them from providing these services. The legal system and most professional organizations would not accept the opinion of a non-degreed individual with no relevant certifications who provides DNA analysis evidence out of a "lab" within their home office that has no accreditation or even policies and procedures. Yet, this happens every day with digital forensics.

Currently, there are no requirements in place to regulate individuals who are involved in the forensic analysis of digital evidence. Some states require private digital forensic analysts to become licensed private investigators (PI), but a PI license does not assure the forensic analyst

has any of the necessary knowledge, skills, or abilities to render correct scientific opinions. The PI licensure may help make someone seem more credible, but there is no accountability involved and only ensures a person has a clean background and knows the relevant state statutes dealing with private investigations. In 2008 the American Bar Association created a resolution urging state governments not to require PI licensing for digital forensic practitioners and instead to establish professional certifications or competency requirements for this science (American Bar Association, 2008).

Many private forensic analysts providing criminal and civil defense work have a traditional information technology (IT) background but because of the high rates paid to forensic experts, they claim their IT skills make them forensic experts. Criminal and civil defendants have little access to qualified digital forensic analysts and those that are qualified are extremely costly. This makes defending a case involving technology problematic.

In a report published by the American Bar Association, they identified similar risks with law enforcement forensic laboratories as a whole and stated, "crime laboratories and medical examiner offices should be accredited, examiners should be certified, and procedures should be standardized and published to ensure the validity, reliability, and timely analysis of forensic evidence (Achieving Justice: Freeing the Innocent, Convicting the Guilty, 2006). The likelihood of these risks being realized is extremely high and in most cases, they already have been.

Detailed and Functional Requirements

Numerous studies have been funded by the U.S. government as well as non-profit organizations examining forensic science within the U.S. Nearly all of the studies come to the same conclusion: something must change in forensic science. Digital forensics is starting to be heavily scrutinized. Federal legislation has already been introduced this year to insure that

forensic laboratories that receive any type of federal funding (including grant funding) comply with minimum standards and best practices. This legislation would impact all federal laboratories and many local, county, state, and private labs as well.

Beyond the impending legislation and pressure by the legal system, it is just the right thing to do. Anyone who may be providing evidence against another person, especially in the name of forensic science, should do everything in their power to ensure their findings are accurate and done according to industry recognized standards.

The requirements were identified to mitigate the problem presented in this capstone. Gaps were also examined in both the existing digital forensic science as well as the framework being presented in this capstone. Much of the requirements of this framework already exist, but have not been combined into a single source document such as the framework within this capstone.

Functional (end-user) Requirements

The requirements for end-users is an easy to understand framework of digital forensic best practices to include minimum qualifications for digital forensic analysts, laboratory standards and accreditation guidelines, and a minimum set of quality assurance policies and procedures. The details of what constitute minimum qualifications and training is in details provided in the next section. End-users must be able to easily understand the information and apply it to their digital forensic practice with limited financial and personnel resources. The end-user in this project is both a digital forensic analyst and the laboratory director or individual that has overall management responsibility for the lab. In some small companies or agencies, this individual may be the same person.

In order to comply with the functional requirements, end-users will have to dedicate adequate personnel and budget resources and make the implementation of the framework an official project within their organization. Depending on the size of the organization, a forensic analyst or lab director could have the role of project manager, or a true project manager could be assigned if available. Whoever is acting as project manager should review the framework provided within and the timelines and create a project plan, along with target dates, metrics, and major accomplishment dates to ensure the project is staying on track.

End-users will be responsible for following each of the implementation phases described in this framework plan and customizing the supplemental documents provided as part of the framework to fit their lab. Gaps that are identified when going through the implementation should have plans created for them. Examples might include sending analysts to training and obtaining certification or improving physical security of the lab.

If a lab wishes to obtain ISO 17025 accreditation then the culmination of this project should be obtaining that accreditation. Becoming accredited to ISO 17025 is prima facie evidence of compliance with this framework. If a lab does not seek external accreditation, they can still be in compliance with the ISO accreditation standards if all of the policies, procedures, and manuals are implemented as well as analyst training and certification requirements are met.

Detailed Requirements

The detailed requirements for digital forensic practitioners and laboratories are as follows:

1. The development of minimum education and training standards for individuals performing the forensic analysis of digital evidence.

a. Examples are provided within this capstone framework. It is recommended that individuals performing forensic analysis on digital evidence have a bachelor's or master's degree in a related subject (e.g., information security, computer forensics, digital forensics, information assurance, etc.), or maintain certifications which require peer reviewed practical analyses of digital evidence and written tests as well as a recertification requirement. Although not required, it is highly recommended that digital forensic analysts have a bachelor's degree, even if not in a related subject, to show competency in core subjects such as reading, writing, and math.

2. The development of quality assurance based policies and procedures that should be required for any laboratory performing digital forensic analysis.
    a. This framework provides all of the quality assurance policies, procedures, and manuals needed for a laboratory to be in compliance, as long as the lab's practice matches the written documents. Part of the accreditation process is to ensure that labs are meeting industry best practices and working to their own policies and procedures.
    b. The minimum policies, procedures, and manuals a laboratory should have include, but are not limited to:
        i. Technical manuals for all disciplines utilized in the laboratory (computer forensics, mobile device forensics, audio forensics, video forensics, etc.).
        ii. Training manuals for all disciplines utilized in the laboratory (computer forensics, mobile device forensics, audio forensics, video forensics, etc.).

iii. A validation manual for all forensic hardware and software to include validation whitepapers on all validations completed within the lab.

iv. An administrative policy manual / quality control manual which has the following core policies:

1. Interim directives, organization chart, training development, courtroom testimony, case assignments and triage, controls of materials and supplies, property and evidence control, evidence retention and destruction, physical security, fire safety, health and safety, news media relations, report writing, equipment testing and verification, reports and document storage/retention, storage of digital evidence, release of evidence, deviation of policies and procedures, proficiency testing, personnel records, complaints about the lab's quality system or personnel, and corrective actions.

v. Standardized forms for handling cases and evidence such as:

1. Technical glossary, chain of custody, consent to sanitize, evidence disposition, forensic report templates, checklists, service request forms, and testimony evaluation forms.

3. The adherence to best practices for digital forensic laboratories based upon ISO 17025 international standards. By implementing the above two steps and training analysts, this requirement will be met.
4. Recommendation for a mid-tier laboratory accreditation model that would allow single-person digital forensic laboratories to seek and obtain a form of accreditation.

   a. A gap was identified as part of the capstone project in the area of accrediting bodies for digital forensic laboratories. Achievement of actual ISO 17025 accreditation by one-person forensic labs may be nearly impossible with the current accreditation process. This project provides recommendations for already existing organizations that certify digital forensic analysts to consider creating an accrediting body as well.

5. Recommendation that regulations be put in place at the federal, state, or judicial system level that requires a minimum standard must be met before an individual can introduce digital forensic evidence in a legal proceeding.
   a. Without some regulation in place, most digital forensic laboratories will not expend the time or resources to meet this framework. This has already been proven by the lack of rigor public and private labs are putting themselves through and the lack of accredited laboratories for digital forensics. Until this problem becomes a business impact (e.g., labs cannot introduce their evidence in court unless standards are met) then it will not be taken seriously.

Existing Gaps

As discussed in this capstone report, the gap in digital forensic standards is wide. The vast differences in digital forensic laboratories range from a fully ISO 17025 accredited with degreed and certified forensic analysts to an individual with no formal training operating their forensic laboratory from their home garage (National Research Council, 2009). The framework in this capstone fills the gaps in forensic analyst's minimum training and education, minimum policies and procedures, and laboratory standards.

Without ensuring digital forensic analysts are properly trained and certified and that laboratories are not following best practices, the entire discipline of digital forensics is at risk. Hundreds of innocent people have been wrongfully convicted due to poor forensic evidence and an unknown amount of guilty people have walked free due to mishandling of forensic evidence. If digital forensic practitioners want to enjoy the reputation and respect they most certainly could achieve, laboratories must begin following the framework outlined in this capstone. Ultimately not following these capstone recommendations could mean increased scrutiny to digital forensics and a much more difficult time admitting digital forensic evidence into legal proceedings.

Project Design

Ensuring the soundness of digital forensics is the right thing to do for society and the criminal justice system in the United States. The capstone provides some core methods to ensure the successfulness of digital forensics as a scientific discipline and assurance that evidence is handled properly and that analysts demonstrate the knowledge, skills, and abilities to render scientific opinions.

The implementation of the framework proposed is not a large financial burden and ultimately will make any laboratory and analyst better. There are also intangible benefits with analyst certification and laboratory accreditation that improve business. For instance, when analysts are certified and laboratories are accredited, it takes a large amount of questions off the table from the opposing counsel. There is no question whether or not the laboratory has policies and procedures in place or if the analyst has been proficiency tested in their discipline. This level of professionalism and demonstrated ability leads to the forensic findings being challenged in court less often, saving the laboratory time and money. Meeting these standards and best

practices also opens up laboratories for additional business and grant funding that are only available to laboratories and personnel that meet this level of rigor.

The framework that is developed in this capstone includes a tested and validated implementation of best practices for digital forensic laboratories. The framework provides digital forensic practitioners (whether public or private) their management, and the legal system a guide to use when evaluating the competency of a digital forensic analyst or laboratory.

Scope

The scope of this capstone is primarily focused on three areas: digital forensic analyst training and certifications, digital forensic laboratory accreditation standards, and digital forensic best practices and policies.

The usefulness and relevancy of this capstone to the few digital forensic laboratories that already hold ISO 17025 accreditation is limited. This capstone is also not applicable to those companies or individuals that conduct digital forensics in the course of breach investigations and incident response only, where the results of the digital forensics will not be presented in a court or used against any individuals.

Assumptions

The assumption of this capstone is that the reader already has a fundamental knowledge of digital forensics as well as the criminal justice system. The intended audience is twofold: digital forensic practitioners and administrators that wish to enhance their forensic practice, and judges and attorneys who wish to better understand the standards to which digital forensics should be held.

Project Phases

The stages for a digital forensic laboratory to implement this capstone framework include:

1. Phase 1 – Audit. Whether a one-person digital forensics laboratory or a large multi-person operation, an audit must be conducted to provide a snapshot in time of the current operations. The audit should include: the current training, experience, and education levels of all staff, an inventory of all hardware and software used within the laboratory, a collection of all existing policies and procedures, all forms and documents used in the laboratory, and any metrics used to track case assignments, turnaround times, backlog, analyst workload, etc.
2. Phase 2 – Requirements gathering. Some of the items proposed in this framework should be considered mandatory, but others are discretionary. Additionally, forensic laboratories and their management or customers may identify other standards to be held accountable to. In this phase, the individual(s) who will be responsible for running this project should be identified and requirements are decided upon.
3. Phase 3 – Design. Once a baseline is established for existing operations and the requirements have been decided upon, the custom implementation of this framework can be created. This design phase will include the "look and feel" of the lab's implementation to include document templates, naming conventions, and communication with stakeholders and customers.
4. Phase 4 – Development. In this phase the responsible individual for implementing this framework will begin the actual development. The development will include writing additional policies and procedures or customizing those provided in this

framework, developing a training program and career ladder for forensic analysts to ensure they achieve the necessary certifications and training, creating workflows and forms to comply with the policies and standards being developed, and performing a gap analysis and budget for any equipment or construction that may need to be accomplished in order to comply with best practices and standards. It is important to involve as many practitioners as possible to achieve buy-in and not create this program in a vacuum.

5. Phase 5 – Quality assurance. A system must be developed to ensure the laboratory and its analysts are following the new policies, procedures, and standards. The quality assurance phase should include an education campaign for analysts and management on what the new standards and policies will include and affirmation from management that the new policies will be requirements of the laboratory. The quality assurance program should also be developed to include random checks of laboratory findings, administrative and technical reviews of analysis reports, courtroom testimony evaluations, and metrics to ensure compliance.
6. Phase 6 – Implementation. After the new policies, procedures, standards, and best practices have been drafted, reviewed, and approved and the program is ready for implementation, a date should be set to go live with the new standards. Since much of what is required within this framework are best practices and improve the overall quality of the forensic discipline, there is no reason why as new practices are reviewed, vetted, and approved that they cannot be implemented in a phased approach. The implementation date should be a date communicated with all staff that all policies and procedures are in place and must be followed from that point forward.

7. Phase 7 – Post implementation support. Someone within the laboratory should become the subject matter expert (SME) in this framework. The SME can provide support to staff within the lab and also should consider attending specific training in laboratory management and accreditation standards. Other laboratories that may have a more mature process can also be contacted for support and guidance as needed. Additionally, policies, procedures, best practices, and standards change as technology and case law changes, necessitating an annual review to ensure the laboratory is maintaining relevant practices.

Timelines

The timeline to implement this framework will vary depending on how much customization a laboratory does on the suggested program as well as the laboratory resources and staff. A complete program without this framework has been accomplished within small digital forensic laboratories within one year time. With much of the work done and provided to laboratories in this framework, it is suggested that a laboratory achieve the objectives within one year of beginning the process.

A recommended timeline is provided below for each step:

- Phase 1 – Audit. This phase should take approximately one month to complete.
- Phase 2 – Requirements gathering. This phase should take approximately three months to complete.
- Phase 3 – Design. This phase should take approximately two months to complete.
- Phase 4 – Development. This phase should take approximately two months to complete.

- Phase 5 – Quality assurance. This phase should take approximately one month to complete.
- Phase 6 – Implementation. This phase should take approximately two months to complete.
- Phase 7 – Post implementation support. Much of this is reoccurring annually, however developing the program should take approximately one month to complete.

Dependencies

Most phases are linear and will require the phased approach outlined above to be used. The implementation phase could be slow-rolled throughout the phases and as new policies are written, they could be implemented. This approach may be beneficial so staff will have more time to adjust to changes rather than having so many new changes all at once during the implementation phase. The major dependency will be on executive leadership support and also personnel resources to accomplish the work. This capstone report was developed in order to provide leadership with the reasons why this should be implemented as well as a template for forensic laboratories to hopefully reduce the resource needs for implementation.

Resource Requirements

With executive leadership support, this framework can be implemented by one person acting as the project manager within the one-year timeframe proposed. The resource requirements will include providing the identified individual with the time necessary to complete the work as well as placing an emphasis on other staff members to review draft documentation being created as part of the project. If full laboratory accreditation is sought, the laboratory will need to budget the necessary funding for accreditation application fees and onsite assessment fees. There may also be some budgetary impact to comply with best practices, such as

increasing physical security, alarm systems and monitoring, office supplies, etc. The laboratory will also need a mechanism to track metrics for compliance, which could be a custom created or commercial-off-the-shelf (COTS) software application or as simple as using a Microsoft Excel spreadsheet.

Risk Factors

Currently, there are no requirements in place to regulate individuals who are involved in the forensic analysis of digital evidence. Some states require private digital forensic analysts to become licensed private investigators (PI), but a PI license does not assure the forensic analyst has any of the necessary knowledge, skills, or abilities to render correct scientific opinions.

Many private forensic analysts providing criminal and civil defense work have a traditional information technology (IT) background but because of the high rates paid to forensic experts, they claim their IT skills make them forensic experts.

The major risks associated with not following the framework provided by this capstone is the conviction of the innocent, freeing of the guilty, and collapse of digital forensics as a recognized forensic science.

From a business perspective, implementing the framework in this capstone reduces liability and ensures the future success of digital forensics and the individual agency or corporation providing those services. There will come a point where non-certified forensic examiners and laboratories that cannot meet minimum standards will be excluded from rendering scientific opinions in legal proceedings. For those who did not choose to comply, their business model will have to change.

Important Milestones

The major milestones of implementing the framework include:

1. Approval from laboratory management to implement new policies, procedures, and best practices.
2. Completing the internal audit and acquiring all of the necessary data to baseline the services being offered by the laboratory.
3. Deciding on the design of the framework and what portions will be implemented in the project.
4. Creating a training program for digital forensic analysts.
5. Developing all necessary policies, procedures, forms, manuals, and templates.
6. Implementing new policies and procedures.
7. Development of metrics and a way to track metrics within the laboratory.
8. If seeking accreditation from ISO 17025, obtaining the status of an accredited laboratory.

Deliverables

The deliverables of this project is a complete turnkey solution for a digital forensic laboratory to create a quality assurance manual, technical manuals, a training program, and all necessary forms to prepare a laboratory for accreditation.

Methodology

The methodology behind this capstone project is to enhance the discipline of digital forensics by giving forensic laboratories a framework to achieve compliance with industry best practices. The approach is nothing new and many forensic laboratories around the world have used the approach proposed in this capstone project successfully. The uniqueness of this capstone is that it provides a digital forensic laboratory, large or small, with all of the necessary information and tools to comply with industry standards and best practices.

This capstone project understands that actually achieving ISO 17025 accreditation by some laboratories may not be possible, depending on the accrediting body used to achieve accreditation. For example, ASCLD/LAB adds additional restrictions above and beyond that of ISO 17025 before it accredits a laboratory. Some of the additional restrictions may make it very difficult for a one-person digital forensics laboratory to achieve accreditation. Other accrediting bodies that require meeting just the ISO 17025 standards however may be achievable by a one-person laboratory.

This capstone project understands there is a gap in the United States for accreditation of smaller digital forensic laboratories. It is recommended that a vendor-neutral independent accreditation body that is already involved in certifying digital forensic analysts consider also creating an achievable laboratory accreditation model based upon the ISO 17025 standards. Organizations such as the International Society of Forensic Computer Examiners (ISFCE), the International Association of Computer Investigative Specialists (IACIS), or the Digital Forensic Certification Board (DFCB) are all excellent choices to undertake such a task. The most obvious choice would be the DFCB since it was originally designed by the National Institute of Justice (NIJ) and the National Center of Forensic Science. The DFCB created a certification known as the Digital Forensic Certified Practitioner (DFCP) trying to fill a gap identified of a lack of vendor-neutral certifying bodies (DFCB, 2014).

Approach Explanation

The capstone provides some core methods to ensure the successfulness of digital forensics as a scientific discipline and assurance that evidence is handled properly and that analysts demonstrate the knowledge, skills, and abilities to render scientific opinions.

The implementation of the framework proposed is not a large financial burden and ultimately will make any laboratory and analyst better. There are also intangible benefits with analyst certification and laboratory accreditation that improve business. For instance, when analysts are certified and laboratories are accredited, it takes a large amount of questions off the table from the opposing counsel. There is no question whether or not the laboratory has policies and procedures in place or if the analyst has been proficiency tested in their discipline. This level of professionalism and demonstrated ability leads to the forensic findings being challenged in court less often, saving the laboratory time and money. Meeting these standards and best practices also opens up laboratories for additional business and grant funding that are only available to laboratories and personnel that meet this level of rigor.

Digital forensic laboratories have only three approaches when it comes to meeting industry best practices: 1) achieve ISO 17025 accreditation, 2) meet the ISO 17025 and other industry best practices without actually obtaining accreditation, and 3) not meet best practices or obtain accreditation.

Approach Defense

Demonstrating core competency in digital forensic science should be non-optional. The framework proposed in the capstone to ensure forensic analyst certifications, standardized policies and procedures, and laboratory best practices and accreditation will provide the solution necessary to ensure digital forensics remains a well-respected forensic science. More importantly, the framework will help prevent miscarriages of justice and will get laboratories ready for the reality of federal regulations in the future.

The approach proposed in this capstone is nothing new and has been validated by those laboratories that are already seeking accreditation. This framework however is designed to give

laboratories that do not have the resources to actually obtain accreditation, to still meet the same standards.

If a laboratory was not accredited, yet fully complied with this framework, the laboratory would be able to sufficiently show compliance with industry best practices. It is not uncommon for counsel to subpoena a forensic laboratory's policies, procedures, training records, and validation manuals. By complying with this framework, a forensic laboratory would be able to immediately answer such a subpoena and build credibility.

Project Development

- Phase 1 – Audit. Laboratory staff should approach this phase by collecting all relevant information available from the laboratory and staff.
- Phase 2 – Requirements gathering. In this phase a single point of contact (POC) should be identified to lead this project. The executive leadership must fully support this project and understand the benefits to the organization.
- Phase 3 – Design. In this phase, the customized framework adapted for the laboratory will be designed. This will include the look and feel of the framework.
- Phase 4 – Development. Now that the POC has identified gaps and opportunities for improvement within the laboratory as well as items that the laboratory is not currently doing that is recommended in this framework, the development work can begin.
- Phase 5 – Quality Assurance. Quality assurance is at the core of this entire capstone project. The methodology used in this capstone and in digital forensic lab accreditation as a whole is ensuring that a laboratory's practices match their policies. Quality assurance will need to be accomplished to make sure the lab has integrity.

- Phase 6 – Implementation. Once all of the drafts have been approved and above steps completed, it is time to begin implementation. Some of the items can be implemented during the course of development, but do not have to be. This is primarily a laboratory management decision.
- Phase 7 – Post implementation support. The SME who created the customized framework as well as management will be responsible for post implementation support. If the laboratory is considering formal ISO 17025 accreditation, most accrediting bodies require the laboratory to be working to their standards for at least one year prior applying for formal accreditation.

Hardware

No new additional hardware should be needed to comply with this capstone project unless a forensic laboratory does not have basic digital forensic equipment. At a very high level, the type of hardware that most laboratories need in order to conduct digital forensics includes, but is not limited to:

- Hardware writeblockers.
- Computer forensic workstations.
- Computer forensic laptops.
- Loose hard drives or a Network Attached Storage (NAS) device or Storage Area Network (SAN) device.
- Network infrastructure equipment such as switches and routers.
- Servers.
- Mobile device forensic platform (e.g., Cellebrite, .xry, susteen, etc.).
- A connection to the Internet.

- Miscellaneous cables and connectors.
- Tools to disassemble computers and related equipment.

Software

Very little software will be needed solely to comply with this framework; however a digital forensic laboratory should have a minimum amount of software available. This software is listed below:

- Main forensic software for analysis (FTK, Encase, SIFT, BlackBag, X-Ways, etc.).
- Operating systems (Windows, Mac, Linux, Server).
- Microsoft Office suite (Word, Excel, PowerPoint, Outlook, etc.).
- EDMS software.
- Various digital evidence forensic tools.

Tech Stack

The layers of services provided by this framework are both administrative and technical controls used to enhance the quality of the digital forensic science. Administrative controls include the creation of new policies and procedures, validation of forensic software, compliance with international standards on forensic laboratory management, and a quality assurance process. Technical controls include the use of specific computer hardware and software as well as writeblocking devices.

Architecture Details

The architecture of this capstone project is designed to provide a forensic laboratory with a turnkey solution which reduces the need for costly consultants and a tremendous amount of time. This project does not require architected computer hardware necessarily, but more of an

architected framework. The framework is designed to be easily imported into an existing or new laboratory and implemented.

Resources Used

The largest resources expended in implementing this project would be in manpower. One organized individual could perform everything outlined in this project within the year timeline given, it has been done in laboratories that achieved accreditation. Some consumables will be expended, such as office supplies, ink, CDs and DVDs, paper, and binders. There may be some funds needed to purchase the necessary office supplies. Depending on the condition of the forensic laboratory using this framework, some expenses may be identified such as the need for more physical security, upgraded forensic hardware or software, and an EDMS solution. Because each laboratory is different and has different physical designs, there is no way to predict the costs that may be associated with this.

By providing so much of the required documents, templates, and project plan in this framework, it would be expected that one person spending ten hours per week for one year could easily bring a laboratory into full compliance with industry best practices or be ready for an accreditation assessment team. If the employee tasked with this project is not the lab director, then the lab director should plan on spending two to five hours per week on this project as well, meeting with the employee responsible for implementation and reviewing work.

The person(s) responsible for implementing this project should be experienced digital forensic analysts who possess the experience necessary to comply with the requirements and understand how to customize them to fit the needs of the specific laboratory. It is suggested that the responsible individual acting as the project manager have at least two years fulltime experience in digital forensics and possess formalized training and preferably certifications in the

digital forensic field. If a non-technical project manager is running the project, then much of the administrative tasks can be done by the project manager and a subject matter expert (SME) with the same qualifications as outlined above should be selected to review the project manager's work and also act as the technical lead.

Final Output

The tangible final output of this project will be multiple new documents created such as policy manuals, validation manuals, technical manuals, and forms.

The intangible outputs from this project are many. The reduction in risk for the laboratory is a key intangible benefit. Since the laboratory will be complying with industry best practices and international standards, the likelihood of a mistake or improper handling of evidence significantly reduces. Recognition and legitimacy as a professional competent laboratory also comes with this project. For labs that can attest to meeting ISO 17025 standards, it may open the door for additional funding sources from the federal government or other businesses. Laboratory management and organization executive leadership can also have peace of mind that the laboratory is operating as a true forensic science laboratory should.

Quality Assurance

The ultimately quality assurance check for this project is achieving accreditation by an ISO 17025 accrediting body. For those labs that do not pursue actual accreditation, then internal audits and management assessments would be required to ensure compliance.

Quality Assurance Approach

The most compelling quality assurance approach is for a laboratory to become an accredited ISO 17025 laboratory. By becoming accredited by an accrediting body, it provides proof that the laboratory has been assessed by outside and independent assessors and their

quality assurance program has been validated. As already discussed in this capstone report, achieving accreditation may not be possible for all labs. Nonetheless, even if actual accreditation is achieved, there is no reason why a lab cannot put into place the items in this framework and be compliant with the intent of the 17025 standards, thus raising the level of competency and professionalism of their laboratory. Many small digital forensic laboratories now have absolutely no policies or procedures, let alone most of what is provided in this capstone report framework.

If another accreditation option became available as recommended in this paper providing access to accreditation by smaller laboratories, than onsite assessments and validations can be conducted to ensure compliance with standards.

This framework is a quality assurance centric approach and is designed to raise the standards within a digital forensic laboratory. The framework is based upon reviewing the ISO 17025 standards document and ensuring that the best practices and standards identified by ISO and the forensic community have been translated directly into this framework. When implemented, this framework insures that quality assurance is in the forefront of all laboratory activities.

By complying with the standards in this framework, digital forensic analysts are certified and annually proficiency tested, digital forensic hardware and software are independently verified, evidence is handled correctly and chain of custody can be tracked for each item submitted to the laboratory, materials used on casework are validated and controlled, analysts must meet a minimum standard before being allowed to work on actual evidence, documents are controlled and tracked in a centralized repository, and structure and formalized is embedded into

all processes the lab performs. Each of these areas is critical to the success and quality of product produced by a laboratory.

In any case, this framework will assist laboratories of any size to comply with best practices and standards in order to prepare for the inevitable and much needed legislation that will require forensic laboratories to be accredited at some level.

Solution Testing

This solution has been successfully implemented in several forensic laboratories across the United States and has resulted in obtaining ASCLD/LAB accreditation for a laboratory (ASCLD/LAB, 2009). The lab that achieved ASLCD/LAB accreditation as a result of implementing this framework was only a two-person law enforcement laboratory. At the time it received accreditation, it was the only non-federal standalone digital forensic laboratory to be accredited in the nation. The laboratory received nearly a perfect score in the accreditation process and had no significant findings during the onsite assessment.

Additionally the policies, procedures, and manuals created as part of this framework have been tested in courts within the United States and held up to all scrutiny they were subjected to.

Implementation Plan

This capstone project involves the implementation of a framework that has already been created and tested. The implementation of the framework was discussed already in this capstone project under methodology, but is provided here with greater detail.

- Phase 1 – Audit. Laboratory staff should approach this phase by collecting all relevant information available from the laboratory and staff. The information collected should include, but not limited to:
    - Job descriptions for all positions.

  - Curriculum Vitea's for all staff members.
  - Copies of all training records, transcripts, and certifications for staff members.
  - Copies of all memorandums of understanding (MOU), service level agreements (SLA), and contracts.
  - Annual budget for the laboratory.
  - Laboratory organization chart.
  - Existing policies, procedures, technical manuals, and forms.
  - Existing metrics for the laboratory to include:
    - Average case turnaround time.
    - Caseload per analyst.
    - Annual cases being submitted and type of cases (e.g., homicide, child exploitation, etc.).
    - Number of devices examined.
    - Quantity of digital evidence examined (in GB).
  - Laboratory mission statement and core values.
  - Complete hardware and software inventory used for digital evidence forensics.
- Phase 2 – Requirements gathering. In this phase a single point of contact (POC) should be identified to lead this project. The executive leadership must fully support this project and understand the benefits to the organization. The POC should obtain the following requirements:
  - Interview management and senior management to identify any current gaps or issues with the forensic laboratory that could be addressed as part of implementing this framework.

- Interview administrative staff and forensic analysts to identify any gaps, suggestions, particular subject matter expertise, and other items that may be helpful with the project. Individuals expressing an interest in assisting with the project and/or have a particular expertise should be utilized.
- Survey customers to identify deficiencies and opportunities for improvements. Look for issues other than slow turnaround times and backlogs of evidence, focusing on process improvements such as report quality, testimony quality, and the level of confidence customers have with the work of the laboratory.
- Review the framework included in this capstone and identify what processes will be included in the laboratory's enhancements and make work assignments as necessary. Begin to track the requirements, timelines, and POCs for each assignment for weekly status briefings.
- Review state licensure laws and any other legal regulatory agency to ensure that the laboratory will comply with all necessary laws and regulations.
- Compare the existing policies and procedures with the requirements outlined in this framework. Conduct a gap analysis and anything that is insufficient, move to the remaining phases (design, development, etc.). Items of particular interest in include chain of custody, evidence handling and storage, physical security, reporting, forensic tool validation, and courtroom testimony.

- Phase 3 – Design. In this phase, the customized framework adapted for the laboratory will be designed. This will include the look and feel of the framework. The methodology for this step includes:
  - Design a standardized report template for forensic findings within the laboratory.

  - Design a standardized technical manual format.
  - Design a standardized quality assurance manual format.
  - Design a standardized policy and procedure format.
  - Design a training program for forensic analysts.
  - Design a repository to store forensic reports that enables security and version control.
  - Design a standardized template for laboratory forms.

- Phase 4 – Development. Now that the POC has identified gaps and opportunities for improvement within the laboratory as well as items that the laboratory is not currently doing that is recommended in this framework, the development work can begin. The development phase methodology includes:
  - Drafting of new policies and procedures based upon recommendations within this framework and feedback obtained during the interviews.
  - Developing new practices such as tool validations.
  - Develop any missing metrics and begin tracking metrics immediately.
  - Develop minimum training and education standards for forensic analysts and create a career path for analysts to achieve minimum standards if they are not already in compliance.
  - Develop budgetary needs and requests for anything that will require financial resources to implement.
  - Develop a quality assurance manual.
  - Develop technical manuals for each discipline used within the lab (e.g., computer forensics, audio forensics, video forensics, mobile device forensics, etc.).

  - Develop workflows for different best practices.
  - Develop a training program to teach staff the reasons behind new changes and how to remain in compliance.
  - Develop an annual management assessment and internal audit plan to ensure compliance with standards.
  - Develop new forms as identified in the gap analysis.
  - Develop a secure evidence storage area if not already in place, including auditing of access and chain of custody.
  - Develop laboratory mission statement and core values if not already in place.
  - Develop a forensic tool validation process and document findings. The National Institute of Standards and Technology (NIST) has great resources for tool validation whitepapers and forensic images to use for testing.
  - Develop forensic reporting templates for standardization.
  - Develop digital storage for forensic evidence.
  - Develop a document repository with version control as an Electronic Document Management System (EDMS). There are free open source tools available or a product such as Microsoft SharePoint will work very well.

- Phase 5 – Quality Assurance. Quality assurance is at the core of this entire capstone project. The methodology used in this capstone and in digital forensic lab accreditation as a whole is ensuring that a laboratory's practices match their policies. Quality assurance will need to be accomplished to make sure the lab has integrity. The specific items to accomplish a quality assurance program include:

- An annual management assessment to review work and ensure it is being done in accordance with the laboratory's new quality system.
- Annual assessment of a random sampling of digital forensic reports to ensure the conclusions of the analysts is made with sound forensic methodology and is backed by sound work.
- Ensure there is a system in place for customers to report issues and complaints about the quality system of the laboratory.
- Ensure accusations regarding ethical violations are immediately reviewed and that an ethical code of conduct has been established within the laboratory.
- Ensure a process exists that can track all cases performed by each analyst as well as the equipment used for each examination. If there are concerns about a particular piece of equipment or analyst, all potentially effected cases can be quickly identified.
- Perform occasional reviews of forensic analyst's courtroom testimony. If there is only one analyst, send surveys to judges and attorneys to rate the performance of the forensic analyst.
- Use metrics to ensure forensic analysts are working as expected and within industry standards.
- Ensure forensic software is validated upon each new major revision.
- Ensure forensic hardware is validated annually.

- Phase 6 – Implementation. Once all of the drafts have been approved and above steps completed, it is time to begin implementation. Some of the items can be implemented

during the course of development, but do not have to be. This is primarily a laboratory management decision. To implement this framework, the laboratory should:

- Issue a policy statement to the laboratory indicating that the new quality system is now in place.
- Require mandatory reading for the newly generated documents, insuring staff has read and understands the new processes.
- Initially, review work more frequently to ensure items are being done in accordance with new standards.
- Make available all of the new information within the EDMS.
- Communicate to stakeholders and customers about new changes.

- Phase 7 – Post implementation support. The SME who created the customized framework as well as management will be responsible for post implementation support. If the laboratory is considering formal ISO 17025 accreditation, most accrediting bodies require the laboratory to be working to their standards for at least one year prior applying for formal accreditation. Other tasks for this phase include:
  - Annual refresher training for all personnel on standards and policies.
  - Annual management reviews and internal audits.
  - Annual review of all forms, documents, policies, procedures, manuals, and practices to ensure they are still relevant.
  - Reviewing any complaints or suggestions made about the lab's quality system.

Strategy for the Implementation

Digital forensic laboratories have only three approaches when it comes to meeting industry best practices: 1) achieve ISO 17025 accreditation, 2) meet the ISO 17025 and other

industry best practices without actually obtaining accreditation, and 3) not meet best practices or obtain accreditation.

Phases of the Rollout

The rollout of this project is done in seven phases: 1) internal audit, 2) requirements gathering, 3) design, 4) development, 5) quality assurance, 6) implementation, and 7) post implementation support.

The internal audit phase has been identified as taking one month to complete and includes a gathering of existing information and material. There is no acceptance test of this phase. The next phase involves obtaining the requirements of implementing the suggested framework within the organization. The requirements are gathered from internal and external stakeholders and are expected to last three months. This phase's acceptance test would include leadership approval that the requirements are accurate and complete. The third phase is the design phase and is expected to take two months to complete. This phase will require a number of document templates to be created and will require acceptance testing from the laboratory director. The fourth phase involves the actual development of the framework as it is customized to the laboratory. This will require frequent communication with lab staff and management and final acceptance test by the laboratory director of all policies and standards created. In the fifth phase, the quality assurance plan should take a month to complete. An individual within the lab should be identified as the lab's quality manager, however in small laboratories this may be the same person as the lab's director. Acceptance testing of all quality assurance activities will be required from the lab management. The sixth phase will last two months and involves the actual implementation of all the work done to this point. This will be the culmination of the work and put the policies, procedures, and standards into action. In order for this phase to occur,

acceptance testing must be obtained for all of the previous phases and a date selected by lab management to move forward with the implementation. The final phase is post implementation support, which does not have a time frame associated with it as it is an ongoing activity. This may involve internal audits, management assessments, and reviewing the quality system of the laboratory. There is not an actual acceptance test for this phase.

Details of the Go-Live

This capstone framework project would be considered fully implemented when one of two items occur: either the laboratory is accredited by an ISO 17025 accrediting body, or upon the completely of phase six (implementation phase). The capstone framework is considered implemented when all new policies, procedures, and manuals are in place and direction has been given from management to begin using the new quality system.

Dependencies

Most phases are linear and will require the phased approach outlined above to be used. The implementation phase could be slow-rolled throughout the phases though as new policies are written, they could be implemented. This approach may be beneficial so staff will have more time to adjust to changes rather than having so many new changes all at once during the implementation phase. The major dependency will be on executive leadership support and also personnel resources to accomplish the work. This framework was developed in order to provide leadership with the reasons why this should be implemented as well as a template for forensic laboratories to hopefully reduce the resource needs for implementation.

Deliverables

The deliverables of this project is a complete turnkey solution for a digital forensic laboratory to create a quality assurance manual, technical manuals, a training program, and all necessary forms to prepare a laboratory for accreditation.

Training Plan for Users

Laboratory staff as well as some stakeholders will need to be trained during this process. It is recommended to make an announcement to all internal and external customers that the laboratory is going to be improving its quality assurance system (or perhaps seeking accreditation) and as a result, some items will change. For external customers, the noticeable change will most likely be the look of forms and reports and possibly the thoroughness of results.

A training session should be provided early on with the internal staff, providing them with details of why moving toward standardization and best practices is necessary for the laboratory and the forensic discipline. This training should be done by the laboratory director or other executive leadership member.

The next step in training would most likely be provided by the POC designated to manage the project of implementing the framework. This individual will need to begin training sessions on new standards, policies, procedures, and documents that are being developed and solicit input from staff members.

At the conclusion of the development phase, an entire training session should be conducted for the entire staff on the new policies and procedures as well as the expectation of the staff members to adhere to the new practices. A formalized way of making suggestions and complaints about the quality system should also be discussed.

Risk Assessment

The risk to a digital forensic laboratory is much greater by not implementing this framework than by implementing it. This capstone framework was developed to mitigate much of the risk currently being realized in the United States.

Of most concern with implementing this project will be the amount of administrative time it will take during the one-year rolled implementation approach. If the POC used to run this project is also a forensic analyst, there is a potential that their caseload will suffer due to the time demands of this project. This may cause an increase to case turnaround times and backlog.

Quantitative and Qualitative Risks

There is no known way to assign a quantitative risk analysis to the implementation of this framework because the probability and business impact for each laboratory will be different. Mainly, the caseload and staffing will dictate how much impact the implementation will have, disallowing a fixed value to the risk. The only quantitative risk that could be associated with the implementation of the framework is a risk to budget. It is possible that some overtime expenses for non-exempt employees could be incurred during the implementation of the project to balance administrative work with the ability to continue casework. The amount of overtime that should be budgeted is estimated to be $10,000.

There are, however quantitative risks associated with not implementing this framework by a laboratory. Laboratories are at greater risk for civil liability and lawsuits if their results are flawed and improperly presented in a legal proceeding due to a lack of quality assurance or training. Laboratories that are found incompetent by a judge or other person of authority may lose credibility, reputation, and the ability to testify in court. Any of these findings would immediately impact business and could result in a complete shutdown, much like what was seen in the Oregon State Policy handwriting analysis unit discussed previously.

If laboratories are not able to present their findings in a legal proceeding, the scope of work they can compete with is quickly limited since most forensic cases are initiated to be used in a legal proceeding. Labs that do not meet minimum standards for both the laboratory quality

assurance system or analyst training and competency are also not generally eligible for federal grant funding or assistance. There are some federal grants available for state and local law enforcement agencies for forensic support, but even before mandatory legislation has been passed, most of these grants require the lab to be accredited in order to receive these funds.

Labs that do not obtain accreditation or at least have the ability to show they are meeting industry standards by implementing this framework have the possibility of being shut down until an outside audit can be done. Closing the doors of a lab until it is audited by an outside agency sometimes happens when the quality of the laboratory is called into question. A decision to suspend a laboratory can either come from inside the organization or from outside, such as from a judge. It can be extremely costly to bring in expert consultants to audit the laboratory, interview personnel, and review casework and all the while the laboratory is unable to accept new work. Brining in expert consultants for a review of this magnitude would cost an estimated $50,000.

Qualitatively speaking however, based on research and experience there is a medium likelihood that lab turnaround times will increase as a result of changing practices and collateral duties being assigned to analysts as part of the enhancement process. This increase is expected to stabilize once the laboratory is working to new standards.

In some areas, the implementation of this framework will help streamline many aspects of the laboratory, reducing the turnaround time risk identified above. As consistency and clear procedures become second nature, the quality of analysis will improve as will the expectations of each analyst. When analysts understand the procedures that must be followed for each case, it allows them to work to those procedures and create workflows, allowing them to build in efficiencies.

Cost/Benefit Analysis

With the exception of some office supplies and potentially overtime pay for non-exempt employees working on this project, this project can be implemented without cost. Because the low cost of implementation, there is not a risk of cost overrun in this project. There is a cost risk associated with not implementing the framework. The risks are of digital forensic analyst being found incompetent in a legal proceeding or a laboratory that is found to be mishandling evidence. These risks certainly would have significant financial implications as it would most likely require outside reviews and consulting services. Some grant funding from the federal government is also only available to forensic laboratories that are accredited, giving them a financial edge over non-accredited laboratories.

Risk Mitigation

If turnaround times begin to be a concern due to the workload of this capstone project, than the schedule could slip to mitigate that concern. An additional mitigation could be the hiring of a consultant to create this program for the forensic laboratory. Because a majority of the work could be done virtually, the consultant costs should not include a great deal of travel, lodging, or per diem costs.

This framework was actually designed to be a risk mitigation strategy itself. The largest risk to implementing this is turnaround time increasing and the potential for overtime expenses not to exceed $10,000. Depending on a lab's budget, they could also decide to budget additional overtime funding to help with turnaround time while implementing this framework. By budgeting approximately $20,000 of overtime funding, it would allow analysts to work overtime on specific cases to get the case analysis and reports completed.

From experience, it is known that at times agencies submit a large amount of evidence to a forensic laboratory in cases. Often, these cases get resolved through the plea negotiation process or the focus of the case becomes narrower. Since evidence can often sit in a forensic laboratory for months before being processed and case agents forget to notify a lab of case status changes, it is recommended that labs create a system to contact case agents prior to performing analysis on any case. If cases in the laboratory no longer need analysis performed, the evidence can be returned to case agents and the cases closed, reducing the backlog and turnaround time for the lab.

Because a majority of the risk is associated with not doing the project instead of implementing the project, it is recommended that lab directors make it known that this framework is going to be implemented and first start with the quality assurance manual. Most attacks against a laboratory's qualifications will be around analyst experience and certifications and written policies and procedures for the lab. It would be recommended to start sending analysts to training as soon as possible if that is determined to be a need as well as start on the administrative and quality assurance manual implementation first.

Post Implementation Support and Issues

The majority of the work in this capstone project is the initial design, development, and implementation. Once the project is approved, the documents are written, and the staff is trained the maintenance of the project is minimal.

Post Implementation Support

In order to be achieve ISO 17025 accreditation, a lab must perform least three audits annually of the forensic laboratory. While not all laboratories will achieve actual accreditation, these audits should be done in any forensic laboratory regardless of accreditation status. These

audits are done to perform internal management assessments of the most critical aspects of a forensic lab and to ensure documentation is still relevant.

One audit is an annual audit and inventory of the evidence storage space. This audit ensures that all evidence is accounted for and a random sampling of evidence items is chosen to ensure all necessary documentation and packaging requirements are met. Secondly is a management assessment of the overall quality system. This assessment reviews any complaints or suggestions made to the system, annual metrics, budget needs, laboratory functionality, and the effectiveness of policies and procedures. The last audit is a review of all documentation to ensure that policies and procedures do not become stale and that new technologies, techniques, and case law are incorporated where appropriate. If a laboratory seeks formal accreditation then annual onsite assessments may be required to ensure external oversight of compliance.

Post Implementation Support Resources

The largest resource needed will be time. The laboratory director and POC will need to spend time reviewing the effectiveness of the quality system and ensuring compliance. Secondly, if digital forensic analysts do not possess industry standard certifications then funding may be needed for them to obtain those certifications.

Courses are offered by organizations such as ASCLD/LAB to learn how to prepare a laboratory for an accreditation assessment. Whether a laboratory chooses to seek formal accreditation or not, this training provides excellent information on how to comply with best practices.

Maintenance Plan

The maintenance plan for this project is based upon an annual time table. A proposed schedule for maintenance within one year is shown below:

Task	Q1	Q2	Q3	Q4
Evidence Room Audit	X		X	
Management assessment of lab's quality system				X
Internal audit of compliance with lab policies		X		
Internal audit of effectiveness of polices and standards	X			

Conclusion, Outcomes, and Reflection

This project is unlike anything available for digital forensic laboratories today. Many of the resources can be located in various locations, but no other like resource could be located on the Internet which provides public and private digital forensic laboratories with the justifications and path forward to enhance the quality of work being conducted by their laboratories.

Project Summary

This project began as an answer to a worrisome trend in digital forensics; the lack of consistent standards, analyst certifications, and laboratory accreditation. Several criminal cases were reviewed that showed how errors in the analysis of digital evidence can impact the justice system. In each case the causation of the errors all boiled down to a lack of standards, analyst qualifications, or laboratory best practices. This capstone project was created to help digital forensic laboratories, small or large, meet industry best practices.

It is unsettling that a person without any degree or certifications in digital forensics can create a "lab" using forensic hardware and software that they have never independently validated and offer themselves as experts. That the findings from a "forensic lab" such as this could mean the difference in someone's freedom or even their life is staggering, yet this is happening every day across the United States. Both public and private individuals are claiming to be digital forensic experts with no oversight and unfortunately a majority of lawyers and judges lack the technical knowledge to adequately challenge them.

The information contained in this capstone report along with the deliverables gives anyone the justification and materials to implement a solution in order to comply with standards such as ISO 17025 and industry best practices. In some cases, all an agency or corporation would need to do would be place their logo on the forms and policies provided and they would be on their way to compliance as long as the content of the documents were followed in practice.

Much of the digital forensic community desires to have their evidence seen in court as forensically sound and bulletproof, yet do not want to go through the rigors that other traditional forensic sciences have done to prevent evidence spoliation and other mishandling and misinterpretations. The digital forensic community and managers of digital forensic laboratories must realize that digital forensics is a science and the risks of non-compliance is far too great. If any digital forensic analyst ever found themselves in a position where digital evidence was being used in a legal proceeding against them, they would absolutely want that digital evidence processed in the best forensics lab with the most skilled analyst who meets certain standards. Defendants also should have access to knowledgeable, skilled, and certified digital forensic analysts working in accredited laboratories. We owe this level of treatment to all accused parties.

Deliverables

Included with this capstone project are multiple deliverables that have been prepared for any digital forensics lab to customize. These deliverables were successfully used in a law enforcement digital forensic laboratory to achieve ASCLD/LAB accreditation as well as within a federal agency focusing on national security. These deliverables have been audited many times and used in actual practice with excellent results. The deliverables include policies, procedures, technical manuals, and forms.

Outcomes

This project has been successfully implemented on two occasions for both accredited and non-accredited laboratories. On one occasion the framework was implemented which led to one of the most unique digital forensic laboratory accreditations of its time by ASCLD/LAB. The second occasion was implementing the framework for a federal agency that performs digital forensics and incident response in both classified and unclassified environments. Both implementations were huge successes and have been used by other agencies as an example of industry best practices.

Some argue that this framework requires too much administrative overhead, to which I disagree. It is different than what most digital forensic analysts are used to, but unfortunately that is because most are not using the level of structure necessary. There is no doubt, using this framework is a different way of doing business, but it is in accordance with best practices and standards. Yes, it requires additional work and some extra steps, however analysts and managers can enjoy the peace of knowing the laboratory is operating as a true forensic laboratory should be.

Reflection

I spent eleven years in law enforcement, the last seven were as the commander of a digital forensic laboratory I founded. I now work with the federal government as a defense contractor, supervising cybersecurity and forensic operations. In both cases I have put myself and my teams through the rigor of this framework and it made us better for doing so. During my tenure I have conducted digital forensic analyses in hundreds of criminal and civil cases and my forensic findings have withstood challenges and peer review. I have been qualified as an expert in both federal and state courts.

Although digital forensic laboratory accreditation was not required when I was in law enforcement (and still is not), I decided it was the right thing to do and became the only laboratory of its kind accredited to that level in the United States. I know that laboratories, large or small, can achieve these standards. Anyone performing forensics in a case that can lead to someone being convicted of a crime should *want* to meet these requirements. We should all remember that any of us are one accusation away from being a defendant.

The most disappointing thing I realized during the research for this capstone report is how much additional research there is available to digital forensic laboratories, yet the amount of bad cases is increasing. Between federal legislation being introduced and multiple reports generated about the significant problems in forensic science, most would think that laboratory managers and executives would immediately want to begin fixing the problems. Instead we see court cases like the Casey Anthony case and the Cary North Carolina case where digital evidence was mishandled, misinterpreted, or both.

Since digital forensics is constantly changing and difficult for many to understand, it is even more incumbent upon practitioners to go above and beyond to ensure evidence is handled

and analyzed correctly. When a jury takes everything coming from a forensic "expert" as absolute fact, especially in light of most attorneys being unable to effective cross examine the digital forensic witness, the responsibility to be truthful and accurate is enormous.

It is my desire that this capstone report serves as a wakeup call to individuals who can make a positive influence such as lawyers, judges, law enforcement executives, and private corporations. This capstone report not only raises a problem, but provides a solution. I hope digital forensic laboratories review this content and use the deliverables contained within to improve themselves, their laboratory, and the digital forensic community.

References

AccessData Corporation. (2013). ACE Study Guide. Retrieved from https://ad-pdf.s3.amazonaws.com/ACE%20Study%20Guide%20Aug%202013.pdf

Alvarez, L. (2011). Software Designer Reports Error in Anthony Trial. *The New York Times*. Retrieved from http://www.nytimes.com/2011/07/19/us/19casey.html?_r=1&

American Bar Association Criminal Justice Section Innocence Committee. (2006). *Achieving Justice: Freeing the Innocent, Convicting the Guilty.* Chicago, IL: American Bar Association.

American Bar Association. (2008). Resolution Regarding Computer Forensics. Retrieved from http://www.americanbar.org/groups/science_technology/pages/forensicresolution.html

American Society of Crime Laboratory Directors / Laboratory Accreditation Board (2014). *Accredited Laboratory Index*. Retrieved from http://www.ascld-lab.org/accredited-laboratory-index/

Becker, D. (2014, January, 3). Despite Scandals, Nation's Crime Labs Have Seen Little Change. *NPR*. Retrieved from http://www.npr.org/2014/01/05/259392234/despite-scandals-nations-crime-labs-have-seen-little-change

Calandro, L., Reeder, D. J., Cormier, K. (2005). *Evolution of DNA Evidence for Crime Solving – A Judicial and Legislative History.* Retrieved from http://www.forensicmag.com/articles/2005/01/evolution-dna-evidence-crime-solving-judicial-and-legislative-history

Carvey, H. (2005, December 22). The age of "Nintendo forensics." Retrieved from http://windowsir.blogspot.com/2005/12/age-of-nintendo-forensics.html

Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council. (2009). *Strengthening Forensic Science in the United States: A Path Forward.* National Crime Justice Reference Service.

Denson, B. (2014). Oregon State Police close handwriting lab after investigation of bias, sloppiness. *The Oregonian*. Retrieved from http://www.oregonlive.com/politics/index.ssf/2014/02/oregon_state_police_quietly_cl.html

Digital forensics. (2014). Retrieved from http://en.wikipedia.org/wiki/Digital_forensics

Digital Forensics Certification Board. (2014). *What is the DFCB?* Retrieved from http://www.dfcb.org/about.html

Federal Law Enforcement Training Center (FLETC). (2014). *Seized Computer Evidence Recovery Specialist.* Retrieved from https://www.fletc.gov/training-program/seized-computer-evidence-recovery-specialist-scers

Garrett, B.L., Neufeld, P.J. (2009). Invalid Forensic Science Testimony and Wrongful Convictions. *Virginia Law Review*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1354604

Gaudin, S. (2007). Bogus Computer Expert Goes From Witness to Federal Prisoner. *InformationWeek.* Retrieved from http://www.informationweek.com/bogus-computer-expert-goes-from-witness-to-federal-prisoner/d/d-id/1054952?

Gould, J. B., Carrano, J., Leo, R., Young, J. (2013). *Predicting Erroneous Convictions: A Social Science Approach to Miscarriages of Justice*. National Crime Justice Reference Service.

Henry, P., Williams, J., Wright, B. (2013). The SANS Survey of Digital Forensics and Incident Response. *SANS Institute,* 5.

Innocence Project. (2014). *DNA Exonerations Nationwide.* Retrieved from http://www.innocenceproject.org/Content/DNA_Exonerations_Nationwide.php

Kedziora, M. (2014). Computer Forensics History. Retrieved from http://www.forensics-research.com/index.php/computer-forensics/computer-forensics-history/

Kornblum, J. (2013, March 12). Memory Analysis and the Ongoing Battle Against Malware. Retrieved from http://www.dfinews.com/articles/2013/03/memory-analysis-and-ongoing-battle-against-malware

Law Enforcement in the United States. (2014). Retrieved from http://en.wikipedia.org/wiki/Law_enforcement_in_the_United_States

Levitan, B. (2011). *Telephone Expert's Report In the Matter of State v. Bradley Cooper, Case No. OCA 08-3863*. Retrieved from https://justiceforbradcooper.files.wordpress.com/2011/11/blackberry_report.pdf

Mandiant. (2012). *M-Trends 2012: An Evolving Threat*. Retrieved from http://marketing.mandiant.com/mtrends2012-sm

Ramirez v. State, 810 So. 2d 836 (Fla. 2001).

Scientific Working Group on Digital Evidence (2014). *Digital and Multimedia Evidence (Digital Forensics) as a Forensic Science Discipline.* Retrieved from https://www.swgde.org/documents/Current%20Documents/2014-09-05%20Digital%20and%20Multimedia%20Evidence%20%28Digital%20Forensics%29%20as%20a%20Forensic%20Science%20Discipline

Scientific Working Group on Digital Evidence (2009). *Position on the National Research Council Report to Congress Strengthening Forensic Science in the United States: A Path Forward.* Retrieved from https://www.swgde.org/documents/Current%20Documents/2009-09-17%20SWGDE%20Position%20on%20the%20NAS%20Report

Timmins, A. (2014). Computer investigator pleads guilty to misrepresenting credentials. *Concord Monitor*. Retrieved from http://www.concordmonitor.com/home/10505029-95/computer-investigator-pleads-guilty-to-misrepresenting-credentials?print=true

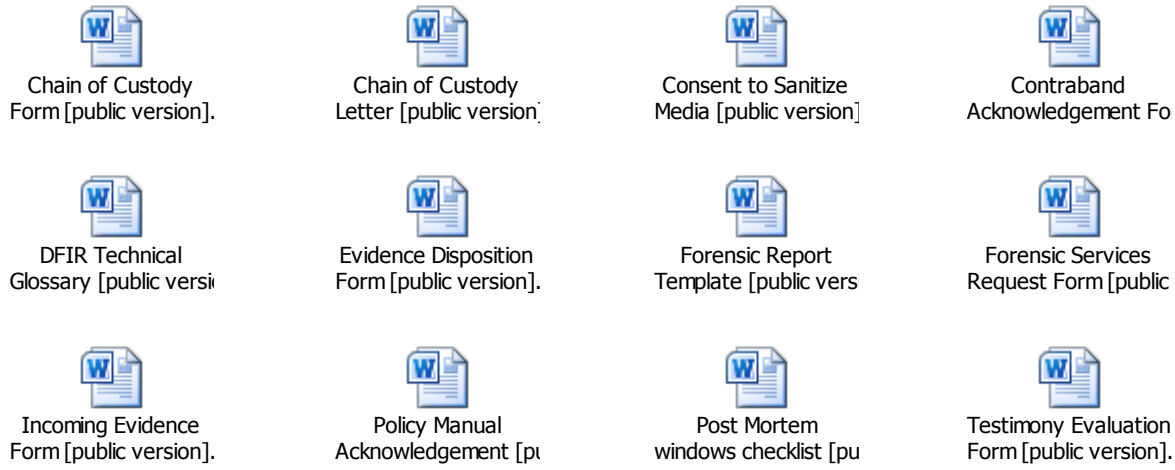
United States Congress. (2014). *Criminal Justice and Forensic Science Reform Act.* Retrieved from http://www.leahy.senate.gov/download/leahy-cornyn-forensics-bill_-as-introduced-alb14200

United States Department of Justice. (2007). *Community Oriented Policing Services, Promoting Effective Homicide Investigations.* Retrieved from http://www.cops.usdoj.gov/Publications/promoting%20effective%20homicide%20investigations.txt

Wilson, C. (2011, July 11). Digital Evidence Discrepancies – Casey Anthony Trial. Retrieved from http://www.digital-detective.net/digital-evidence-discrepancies-casey-anthony-trial/

Appendix A:

Appendix A contains embedded Microsoft Word documents of many of the standard forms a digital forensic laboratory should be using.



*** Note – To download these files from this PDF version, visit http://www.JoshMoulin.com ***

Appendix B:

Appendix B contains an embedded Microsoft Word file of an example technical manual for a forensic and/or incident response laboratory.

*** Note – To download these files from this PDF version, visit http://www.JoshMoulin.com ***

Appendix C:

Appendix C contains an embedded Microsoft Word file of an example validation manual for a forensic laboratory including multiple example validation papers.

CIRT Validation Manual [public versior

*** Note – To download these files from this PDF version, visit http://www.JoshMoulin.com ***

Appendix D:

Appendix D contains embedded Microsoft Word files of an example training manuals for a forensic laboratory.


Computer Forensics Training Manual [publ


Video Forensics Training Manual [publ


Mobile Device Forensics Training Ma

*** Note – To download these files from this PDF version, visit http://www.JoshMoulin.com ***

Appendix E:

Appendix E contains an embedded Microsoft Word file of an example policy and quality assurance manual for a digital forensic laboratory.

Forensic Lab Quality Manual Example [pub

*** Note – To download these files from this PDF version, visit http://www.JoshMoulin.com ***