January 2015

Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies

Teri A. Flory
Purdue University

Graduate School Form 30
Updated 1/15/2015

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Teri Ann Flory

Entitled

DIGITAL FORENSICS IN LAW ENFORCEMENT: A NEEDS BASED ANALYSIS OF INDIANA AGENCIES

For the degree of Master of Science

Is approved by the final examining committee:

Eugene H. Spafford
Chair

Glenn G. Sparks

Marcus K. Rogers

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Eugene H. Spafford

Approved by: Eugene H. Spafford 11/30/2015

Head of the Departmental Graduate Program Date

DIGITAL FORENSICS IN LAW ENFORCEMENT: A NEEDS BASED ANALYSIS OF INDIANA AGENCIES

Submitted to the Faculty

of

Purdue University

by

Teri A. Cummins Flory

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

December 2015

Purdue University

West Lafayette, Indiana

ACKNOWLEDGEMENTS

I would like to acknowledge the assistance I received from my advisor, Dr. Eugene Spafford, and committee members Dr. Marcus Rogers and Dr. Glenn Sparks, and for all of their advice and guidance.

Further, I wish to acknowledge my husband, Christopher Flory, for his patience, support, guidance, and understanding during this process.

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

LIST OF ABBREVIATIONS

CERT	Computer Emergency Readiness Team
CSIS	Center for Strategic and International Studies
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FLETC	Federal Law Enforcement Training Center
IC3	Internet Crime Complaint Center
ILEA	Indiana Law Enforcement Academy
ISTS	Institute for Security and Technology Studies
IPAC	Indiana Prosecuting Attorneys Council
ISP	Indiana State Police
NCFI	National Computer Forensics Institute
NCFTA	National Cyber-Forensics and Training Alliance
NIJ	National Institute of Justice
NW3C	National White Collar Crime Center
PERF	Police Executive Research Forum
PWC	Pricewaterhouse Coopers
TWGECSI	Technical Working Group for Electronic Crime Scene Investigation
USSS	United States Secret Service

ABSTRACT

Flory, Teri A. MS Information Assurance and Security, Purdue University, December 2015. Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies. Major Professor: Dr. Eugene Spafford.

Cyber crime is a growing problem, with the impact to both businesses and individuals increasing exponentially, but the ability of law enforcement agencies to investigate and successfully prosecute criminals for these crimes is unclear. Many national needs assessments were conducted in the late 1990's and early 2000's by the Department of Justice (DOJ) and the National Institute of Justice (NIJ), which all indicated that state and local law enforcement did not have the training, tools, or staff to effectively conduct digital investigations (Institute for Security and Technology Studies [ISTS], 2002; NIJ, 2004). Additionally, there have been some studies conducted at the state level, however, to date, none have been conducted in Indiana (Gogolin & Jones, 2010). A quick search of the Internet located multiple training opportunities and publications that are available at no cost to state and local law enforcement, but it is not clear how many agencies use these resources ("State, Local, & Tribal" for FLETC, n.d.; https://www.ncfi. usss.gov). This study provided a current and localized assessment of the ability of Indiana law enforcement agencies to effectively investigate when a crime that involves digital evidence is alleged to have occurred, the availability of training for both law enforcement officers and prosecuting attorneys, and the ability of prosecuting attorneys to pursue and

obtain convictions in cases involving digital evidence. Through an analysis of the survey responses by Indiana law enforcement agencies and prosecutors' offices, it is evident that Indiana agencies have improved their ability to investigate crimes with digital evidence, with more than half with employees on staff who have attended a digital forensic training course within the past five years. However, a large majority of the agencies still perceive their abilities to investigate crimes with digital evidence in the mid-range or lower. The results support the recommendation that a comprehensive resource guide needs to be made available that the agencies can use to locate experts, obtain assistance with standard operating procedures, learn about free training courses, and find funding opportunities to increase their capabilities in investigating crimes involving digital evidence.

CHAPTER 1. INTRODUCTION

Cybercrime has continued to grow year after year, with 2015 continuing that trend (PricewaterhouseCoopers [PWC], CSO Magazine, Computer Emergency Readiness Team [CERT], & United States Secret Service [USSS], 2015). Of the respondents to the annual U.S. cybercrime survey[1], 79% stated they had a security incident within the past 12 months, the highest percentage ever in the annual surveys (PWC et al., 2015). Cybersecurity incidents are investigated both by internal company security, but also externally by law enforcement to determine whether a criminal act has occurred, or if attribution is possible. For an effective investigation, it is necessary that law enforcement have the capability to thoroughly analyze any evidence retrieved.

The level of investigative capability has been reviewed previously in needs assessments and analyses conducted on issues of digital forensics and law enforcement agencies (ISTS, 2002; NIJ, 2004; Hickman & Peterson, 2004). However, many of these were completed during the late 1990's and early 2000's, with only a few reports being published in 2010 and 2013 (Gogolin & Jones, 2010; Henry, Williams, & Wright, 2013). While it is not clear why this large publication break exists, it is well documented that the prevalence of technology use during the commission of a crime has increased (Weiner-Bronner, 2014). The current paper discusses the past state of digital forensics

[1] This survey is conducted annually by PricewaterhouseCoopers, CSO magazine, the CERT Division of the Software Engineering Institute of Carnegie Mellon University, and the U.S. Secret Service

investigations in the United States, and seeks to determine the status of the current training levels and abilities of Indiana law enforcement agencies to investigate crimes involving digital evidence and prosecuting attorneys to prosecute those crimes.

The study was conducted via survey because of the desire to obtain self-reported capabilities of the agencies and the lack of regular data maintained by those agencies that could have been analyzed to determine the same information. Surveys were distributed to Indiana law enforcement agencies and prosecuting attorneys offices, inquiring into the perceptions and capabilities of Indiana law enforcement. The surveys asked the agencies about topics including whether the Indiana agencies have an on staff digital forensics expert, if the agencies have access to an outside expert that can be utilized in these investigations, if any officers have attended training, and the agencies' perception of their own effectiveness in investigating digital crimes. Additionally, a pilot study that was previously conducted assisted in preparing the current larger scale needs analysis. The concept of digital investigations is described in many different terms throughout the previous research, including the terms electronic evidence, mobile phone evidence, computer evidence, computer crime, cyber crime, or computer forensics. The current paper uses the term digital evidence, with the intent to encompass all of the aforementioned terms.

The research question for the study is as follows: what are the current training levels, needs, and perceptions of abilities of law enforcement agencies and prosecuting attorneys in the State of Indiana when investigating and prosecuting crimes involving digital evidence?

The paper is divided into seven sections, with Section 2 discussing the relevant literature on the issues such as previously conducted needs analyses, and training opportunities and expertise available. Section 3 describes the methodology used in both the pilot study and full study, and Section 4 discussing the results of the study. Section 5 is the Discussion section which analyzes the results, Section 6 provides the limitations of the study, and Section 7 concludes the paper.

CHAPTER 2. LITERATURE REVIEW

The focus of the majority of the previous research conducted has been on the national ability to investigate digital crime. While there have been a few studies conducted on the abilities of agencies within states, none of these specifically looked at Indiana law enforcement agencies. Additionally, most studies review only the law enforcement aspect of digital investigations, and do not analyze the issue from the perspective of prosecuting attorneys' ability to successfully prosecute crimes involving digital evidence, or at what training abilities are currently available. The accessibility of training issue is important to analyze to help determine whether the training shortcomings noted in the needs assessments during 2002 and 2004 have been resolved (ISTS, 2002; NIJ, 2004; Hickman & Peterson, 2004). Further, the knowledge and ability of prosecuting attorneys in the field of digital evidence are a necessary step in successfully pursuing cybercriminals, as without the appropriate skills and training, any arrest and investigation by law enforcement into a crime involving digital evidence could be wasted. This might lead to the possibility of the alleged perpetrator being released from any liability for his actions.

2.1 Prevalence of Digital Crime, and Impact on Society

The first question that must be answered is whether digital evidence investigation expertise is needed. This study is unnecessary if there is not a problem of crime that includes digital evidence. Public, financial, and information industries were listed as the tope three industries affected by data breaches (which are included in cybercrime and require investigation of digital evidence) in 2015 (Verizon, 2015). The estimated annual direct and indirect costs of cybercrime for the global economy, as calculated by Intel Security at McAfee, was more than $400 billion in 2014 (Center for Strategic and International Studies [CSIS] & McAfee, 2014). Cybercrime incidents in the year prior to June 2014 affected more than 40 million Americans (CSIS & McAfee, 2014). Clearly there is a prevalence of crimes in our society that include digital evidence.

The Internet Crimes Complaint Center (IC3), which is an entity within the U.S. Federal Bureau of Investigation (FBI), received complaints in 2014 that totaled over $800 million dollars. This center received approximately 22,000 complaints monthly (FBI, 2014). It is estimated that only 10% of victims report their crimes directly to IC3, which could translate to an underinflated figure of $800 million, as mentioned earlier in the FBI report (FBI, 2014). Auto fraud was the most reported type of crime, followed by government impersonation email scams, intimidation/extortion scams, and real estate fraud. The investigation of these types of crimes is typically initiated by a call to a local law enforcement agency (FBI, 2014). Indiana ranked 18th in the percentage of crimes reported to IC3, meaning that approximately 4,470 complaints came from the state for the year (FBI, 2014). When looking at the aforementioned financial numbers reported by IC3 and CSIS, the types of crimes most regularly reported, and the fact that Indiana had

thousands of complaints last year, it is evident that local law enforcement agencies' ability to investigate crimes involving digital evidence is paramount. Conducting sound forensic investigations can lead to the arrest and prosecution of cyber criminals and increases the potential for retrieving some of the stolen assets for the victims.

2.2 State of Labs, Training, and Accessibility for Law Enforcement in the U.S. from Previous Studies

The Institute for Security and Technology Studies (ISTS) at Dartmouth College conducted a three-part study during 2001 and 2002 that consisted of a web-based survey, personal interviews with cyber-attack investigators, and a presentation of findings at a conference for additional feedback. The purpose of the study was to conduct a needs assessment for law enforcement in the area of cyber attacks, with a goal to create a national research and development plan to meet the assessed needs (ISTS, 2002). The ISTS (2002) study specifically focused on the investigative process, emerging technologies, national data and information sharing, law enforcement specific development issues, and training. When asked about satisfaction with tools and software available for examining a compromised machine or network, 41% of the respondents either disagreed or strongly disagreed that they were satisfied with the available tools and software. The lack of availability for the tools because of funding, training, or lacking essential needs was noted as the main reason for this dissatisfaction (ISTS, 2002). Law enforcement officers were much more satisfied with the tools available for finding an entity linked to an IP address, with 52% of the respondents answering that they agreed or strongly agreed to satisfaction in this area (ISTS, 2002).

Encryption, wireless technologies, and steganography were noted as emerging technological issues that restrained an investigator's ability to successfully conduct an investigation (ISTS, 2002). Of the 48% of the respondents who indicated dissatisfaction with the tools used in detecting and recovering data hidden by steganography, 63% indicated this was because of a lack of tools available for this task (ISTS, 2002). An additional concern noted by law enforcement officers was the inability to communicate with other cyber-attack investigators during real time investigations, as there were often different jurisdictions involved in these crimes (ISTS, 2002). Most respondents indicated they depended on their personal network of contacts when attempting to conduct investigations that may cross into other jurisdictions. Further, they identified a need to have technological resources to facilitate, and even help coordinate, cyber-attack investigations (ISTS, 2002).

An additional concern raised by respondents was the ability of new tools to work quickly enough because of there being a broad range of skill levels of investigators. Some investigators are only comfortable with utilizing point and click tools, while others regularly rely on command-line-based tools (ISTS, 2002). Only 11% of the respondents had completed a full course of academic study in a computer field, and 90% of respondents believed that there was an urgent need for additional training (ISTS, 2002).

In addition to the needs assessment on law enforcement conducted by ISTS in 2002, Hickman and Peterson (2002) at the U.S. Department of Justice conducted a needs assessment on the 50 largest crime labs in the country. They found that the respondent labs had a backlog of 142 computer crimes related cases at that time (Hickman & Peterson, 2002). The amount of computer crimes each year has continued to grow, and

this backlog is much greater now (Casey, Katz, & Lewthwaite, 2013). Further, in a 2004 report to Congress on the status of forensic science services, it was specifically noted that digital evidence analysis had a manpower shortage (NIJ, 2004).

The National Institute of Justice (2004) report to Congress also touched on training for both novices and experienced personnel, and recommended that minimum standards should be established for each forensic discipline, with required testing to confirm minimum competency. Additionally, the study included feedback from the forensic community requesting that Federal forensic training programs be expanded to address emerging issues of electronic crime (NIJ, 2004). As previously mentioned, a lack of manpower was also discussed, which was partially attributed to the highly trained officers in this area leaving the public sector and instead working for private companies, based upon the higher pay and shorter hours (NIJ, 2004).

In addition to requesting more training, there was a recommendation of an increase of forensic education programs at colleges and universities (NIJ, 2004). Many forensic educational programs that were established at the time of the report had a lack of funding, resources, laboratory space, and personnel (NIJ, 2004). To assist in this process, the Technical Working Group on Education through the National Institute of Justice created guidelines for forensic educational programs, including curricula for undergraduate and graduate programs and a recommendation that the schools work with forensic science laboratories (NIJ, 2004).

The 2004 report to Congress further stated that a baccalaureate degree in natural science, forensic science, or a closely related field, should be a minimum requirement for compliance with accreditation standards along with an individual need for hands on

training within the specific forensic science discipline in which that individual will be working (NIJ, 2004). This report was clear in its recommendations that relevant education was paramount to effectively conducting forensics examinations.

Unlike more traditional forensic work such as DNA testing, most digital evidence investigation is not completed in a crime lab, but instead in the field or in law enforcement agencies (NIJ, 2004). Crime laboratories for digital evidence investigation are limited by the costs associated with staying current with technology and maintaining training for the employees at the lab (NIJ, 2004). As technology changes, the labs must continually update their hardware, software, and employee training. Therefore, most of the analysis is conducted by officers, who often receive training from organizations, universities, or software companies. These officers are not currently required to engage in any specific number of continuing education hours to maintain a certification, as there is currently no nationally recognized certification (NIJ, 2004).

Stambaugh et al. (2000) discussed the needs of law enforcement to combat electronic crime, and indicated that one of the particular concerns is the gap that existed between the technologies and training available to law enforcement and the advanced technologies that were being used by the cyber criminals. In their paper, the authors analyzed the data collected by the NIJ in a 1998 study, and reported the key findings were that greater awareness of electronic crime should be made for all stakeholders, including attorneys and judges. Additionally, and more relevant to this study, the authors noted that local and state agencies felt unprepared when it came to training, equipment, and staff to meet any current or future needs in investigating electronic crimes (Stambaugh et al, 2000). The following two issues were prevalent throughout the study:

first, progress must be accomplished quickly, and second, progress must be accomplished in a coordinated and centralized manner (Stambaugh et al., 2000). The sense of urgency was based on the increasing pace that new technology was being developed and that the offenders were keeping up with the new technology while law enforcement lagged behind (Stambaugh et al., 2000).

In a study conducted by Rogers and Seigfried (2004) that inquired into the top issues related to computer forensics, respondents most frequently reported the issue of education/training and certification. The least reported issue was lack of funding (Rogers & Seigfried, 2004). The study was a voluntary survey of individuals interested in computer forensics, and asked the single question of what the respondents believed were the five top issues related to computer forensics (Rogers & Seigfried, 2004).

One of the few studies conducted between 2004 and 2010 was completed by Rahul Bhaskar (2006), and was written after the negative federal, state, and local governmental response to the destruction caused by Hurricane Katrina. The author compared that response to the likelihood that a digital Hurricane Katrina could occur. He surveyed personnel in 530 midwestern law enforcement agencies and found that only a small number of them had even a basic understanding of computer forensics (Bhaskar, 2006). Additionally, the study found that individual organizations thought it difficult to respond to incidents because of the limited knowledge of computer forensics within law enforcement and the lack of legal personnel, such as prosecuting attorneys, that are trained in computer forensics law (Bhaskar, 2006). The author identified the key elements of computer forensics as identification, preservation, analysis, and presentation, and stated that the lack of performing these tasks uniformly across agencies caused an

uncertainty in the ability to ensure that digital evidence would withstand the scrutiny of trials (Bhaskar, 2006). Further, the lack of legal experts who are trained to prosecute digital crimes often caused many cases to not be prosecuted (Bhaskar, 2006).

Another study on forensics expert employment at law enforcement agencies was conducted by the West Virginia University College of Business & Economics (2008). This study found that less than 60% of law enforcement agencies surveyed reported having at least one individual that worked directly on forensics. However, almost 85% of the responding agencies reported performing digital evidence investigations, and these investigations were regularly performed outside of a traditional forensics laboratory environment (West Virginia University, 2008). This study was conducted as a follow-up to the Census of Publicly Funded Forensic Crime Laboratories, in 2002 and 2005 (West Virginia University, 2008).

While it appears that most digital evidence investigations do not occur in formal labs, it is still important to review the capabilities of these labs. Certain investigations with a high level of technical difficulty are likely to still be conducted in a formal laboratory environment, such as those run by the State Police agencies or Federal Bureau of Investigations. Many forensics labs have faced an increase in both the amount of cases as well as an increase in the amount of data that needs to be analyzed (Casey et al., 2013). The Casey et al. (2013) study reviewed digital forensic processes, and the authors determined that there are ways to increase the speed with which investigations are completed, but that the workflow process had to be reviewed as a whole, and not as individual parts. Law enforcement agencies that are using forensic labs have an interest in these investigations being completed quickly and efficiently to ensure that evidence is not

lost and that cases are pursued in a timely manner (Casey et al., 2013). The results from the current study show that many Indiana agencies do not have the ability to conduct investigations involving digital evidence, and it is not unreasonable to believe that these agencies use forensic labs such as those discussed in the study conducted by Casey et al., (2013).

Henry, Williams, and Wright (2013) at the Sans Institute conducted a survey of forensic examiners working in both private industry and government. Almost half (47%) of government personnel reported that mobile devices are involved in more than 10% of their cases (Henry et al., 2013). The results of the survey indicated that the likelihood is greater for government personnel, as opposed to private industry, to investigate mobile devices in addition to more traditional desktop computers (Henry et al., 2013).

Respondents to the Henry et al. (2013) survey also indicated the following five challenging areas in digital forensics;

1. Legal issues of ownership and privacy;
2. Lack of standards and tools;
3. Lack of skills, training, and certification;
4. Lack of established policy; and
5. Lack of visibility

The final recommendations of the white paper were for all forensic and legal professionals to stay current on the latest cases and practices in digital forensics (Henry et al, 2013).

One state specific study analyzed Michigan law enforcement needs and abilities through a survey sent to all of the Sheriff's Departments in the state (Gogolin & Jones, 2010). The authors found that 42% of the agencies contacted did not have a computer crimes unit, and 37% of reporting agencies that did have a computer crimes unit had one

for less than four years (Gogolin & Jones, 2010). Many agencies in the State turned the investigation and evidence of computer crimes over to the Michigan State Police, which had a backlog of between one and two years (Gogolin & Jones, 2010). One creative agency had law enforcement collect the computers, but the investigation was handled by deputized volunteers who typically were technicians that did not have any other law enforcement training, and were employed in the private sector in an information technology position (Gogolin & Jones, 2010).

Approximately half of the responding Michigan law enforcement agencies had an individual on staff that had received training in collecting and storing digital evidence, and two agencies reported that they conducted digital investigations, even though no one on their staff had received any training on how to properly conduct a digital investigation (Gogolin & Jones, 2010). In addition, no agency reported having more than three primary investigators working on digital crime, even though some of the agencies reporting served populations of between one and two million people (Gogolin & Jones, 2010). Further, 73% of all investigators received 5 days or less of annual training on digital evidence, and a majority of the investigators were also assigned other, more traditional, types of cases to investigate (Gogolin & Jones, 2010).

One important aspect that has not yet been discussed is the ability of patrol officers in digital evidence investigations. They are typically the first responders to any criminal complaint, and they must know how to effectively ask the necessary questions, control the scene, and collect any relevant evidence. These issues were analyzed by Bossler and Holt (2011) in a survey conducted with patrol officers Charlotte, North Carolina and Savannah, Georgia. They were asked about their beliefs on who should be

responsible for investigating cybercrimes and their perceived abilities to investigate cybercrime (Bossler & Holt, 2011). Almost half of the respondents had no opinion on whether cybercrime was being taken seriously enough in law enforcement, and nearly 73% believed that cybercrime should be dealt with by a special unit (Bossler & Holt, 2011). This is concerning considering that patrol officers are the initial ones who might flag, or request, that a case be assigned to a special unit. The lack of knowledge on whether cybercrime was being taken seriously enough by law enforcement could indicate a lack of knowledge on the subject in general, and the belief that a special unit should be assigned could be a reason that necessary training on digital evidence is a lesser priority for this group. This could limit the knowledge of patrol officers on how to handle digital evidence appropriately at a crime scene, which directly impacts the effectiveness of an investigation with digital evidence.

The issue of properly handling digital evidence was reviewed by Bulbul, Yavuzcan, and Ozel (2013). They stated that digital evidence must be properly handled to ensure a timely, valid, and accurate presentation to a court. It is possible for digital evidence to be altered, damaged, or destroyed through improper handling, and therefore it is important for any law enforcement officer or staff who might handle any digital evidence to have training and education to ensure that the evidence is admissible in court (Bulbul et al., 2013). In this article, the authors furthered this idea by offering a model as a guideline for practitioners in this area to help ensure admissibility (Bulbul et al., 2013).

2.3 State of Prosecutions of Crimes Involving Digital Evidence

Even if officers are properly handling digital evidence, and a thorough investigation is completed, the prosecuting attorneys must be able to effectively present

the evidence in court for a successful conclusion to a case. In the previously mentioned study conducted by Bossler and Holt (2011), the authors also questioned the patrol officers on their perceptions of prosecution of cybercrime, and the officers overwhelmingly agreed that there needed to be more prosecutions of cybercriminals. As early as 2001, 42% of all local prosecutors, nationwide, had prosecuted a computer related crime under their state laws (Brenner & Schwerha, 2002). The largest percentage of crime involved in this grouping was child pornography, however, credit card/bank card fraud and theft of intellectual property were also included in the results (Brenner & Schwerha, 2002). Computer crimes that do not meet the criteria of federal laws (such as a required dollar amount of fraud or number of images in child pornography) regularly fall to local prosecutors to pursue (Brenner & Schwerha, 2002).

To be effective at prosecuting crimes involving digital evidence, local prosecuting attorneys must have a minimal level of knowledge in computers and information technology (Brenner & Schwerha, 2002). Funding for training of prosecutors in this area was also noted as a concern, as most prosecutors offices are funding by local municipalities, and the costs associated with these types of training opportunities are likely prohibitive to most small communities (Brenner & Schwerha, 2002).

The concerns noted by Brenner and Schwerha were from 2002, and many technological advances have been made since that time. Additionally, as is noted later in this paper, many training opportunities are now available in the area of digital evidence. Unfortunately, according to data conducted during a workshop presented by the Priority Criminal Justice Needs Initiative by RAND Corporation and the Police Executive Research Forum (PERF), the lack of understanding by prosecutors of digital evidence is

still a great concern (Goodison, Davis, & Jackson, 2015). Law enforcement regularly works with their local prosecuting attorneys when ensuring they are complying with search and seizure restrictions and chain of custody concerns during the course of investigations, and the realm of digital evidence is no different (Goodison et al., 2015). Police and prosecutors must coordinate on these cases to increase efficiency on the types of data searched, understand the evidence involved, and ensure that all legal requirements of disclosure to the defense are met. If prosecutors do not understand the digital evidence, these tasks become much more difficult to complete (Goodison et al., 2015).

2.4 Use of Federal or State level Expertise

The State of Indiana established a cybercrime unit within the Indiana State Police (ISP) in 1998 (Cybercrime and Investigative Technologies Section, 2015). This cybercrime unit assists with investigations where digital media is an "integral part of the crime" (Cybercrime and Investigative Technologies Section, 2015). It is comprised of six sergeants who conduct digital forensics evidence retrieval and 28 digital media recovery specialists throughout the state for on-scene computer previews (Cybercrime and Investigative Technologies Section, 2015). The ISP also has a Crimes Against Children Unit that focuses solely on investing crimes involving the possession and distribution of child pornography, which regularly involves digital evidence (Cybercrime and Investigative Technologies Section, 2015).

Additionally, the FBI has many tools that can be utilized by state and local law enforcement, including the National Cyber Investigative Joint Task Force, Cyber Task Forces, Infraguard, the Strategic Alliance Cyber Crime Working Group, and the Cyber Action Team (Cyber Crime, 2015). However, only the Cyber Task Forces, National

Cyber-Forensics & Training Alliance, and Infraguard work regularly with local agencies, and provide opportunities or assistance with current digital investigations (Cyber Crime, 2015). Unfortunately much of this assistance is through training and information sharing, and does not include regularly retrieving digital evidence unless the case is of interest to the FBI for other reasons, such as federal prosecution or national security (Cyber Crime, 2015).

Finally, the National White Collar Crime Center (NW3C) which is a non-profit organization comprised of state, local, tribal, and federal law enforcement agencies, provides support for the prevention, investigation, and prosecution of high-tech and economic crimes. Specifically, they provide technical assistance to local agencies upon request that are investigating white collar or high-tech crimes (NW3C, 2015).

2.5 Current Training Opportunities and Availability for Indiana Law Enforcement

In the State of Indiana, new law enforcement officers must attend a Basic Training course taught at the Indiana Law Enforcement Academy (ILEA) (Basic Training – Tier I for ILEA, n.d., para. 1). This academy consists of over 600 training hours in areas such as criminal and traffic law, firearms, emergency vehicle operations, physical tactics, and human behavior (Basic Training – Tier I for ILEA, n.d., para. 1). There is no mention of any digital or technology based investigations in any of the training course materials, so it appears that new law enforcement officers in Indiana enter this career with no formal training in digital investigations, or identification, collection, or preservation of digital evidence (Basic Training – Tier I for ILEA, n.d.). A review of in-service training courses offered at the academy also revealed that there are no digital or cyber investigation opportunities available for Indiana law enforcement officers to attend

after their basic course if they have an interest in the subject matter (Inservice Training for ILEA, n.d., para. 1). For a sworn law enforcement officer in the State of Indiana to receive digital forensics training, he or she must attend a course at a University, or one conducted by federal agencies or private companies.

The Purdue University Cyber Forensics Laboratory, located in West Lafayette, Indiana, provides two different training courses for local, state, and federal law enforcement officers (Law Enforcement Training Courses, Purdue University, n.d., para. 2, 3). The available courses include a three-day Basic Digital Investigations course and a one-day Basic Evidence Seizure and Imaging course (Law Enforcement Training Courses, Purdue University, n.d., para 2, 3). An additional course on Macintosh Forensics is currently being developed (Law Enforcement Training Courses, Purdue University, n.d., para 4). These courses are open to law enforcement officers, judges, and prosecuting attorneys, and are scheduled by demand (Law Enforcement Training Courses, Purdue University, n.d., para 1).

A federal training opportunity for law enforcement, prosecuting attorneys, and judges is at the National Computer Forensics Institute (NCFI). The NCFI opened in 2008 as a joint venture between the Alabama Office of Prosecution Services and the United States Secret Service Criminal Investigative Division with the goal of providing training for state and local investigators on digital evidence and cyber crime investigations, and is located in Hoover, Alabama ("About" for NCFI, n.d., para. 1, 2). This training is provided at no cost for state and local law enforcement, judges, and prosecuting attorneys ("About" for NCFI, n.d., para. 7). Courses are offered on an almost weekly basis at a facility specifically designed, built, and dedicated to this training, and the courses range

in topics from Basic Computer Evidence Recovery Training to Advanced Mobile Device Examiner ("Courses" for NCFI, n.d., "Schedule" for NCFI, n.d.).

Training is also provided at no cost to State and local law enforcement agencies at the Federal Law Enforcement Training Center (FLETC) ("State, Local, & Tribal" for FLETC, n.d., para. 1). Some relevant courses include Computer Network Investigations Training and Digital Evidence Acquisition Specialist Training ("Training at FLETC" for FLETC, n.d.). These training courses are offered throughout the year, with a master calendar posted on the agency's website ("Training at FLETC" for FLETC, n.d.,; "Training Calendar" for FLETC, n.d.). It is not known if the training opportunities available at FLETC or the National Computer Forensics Institute have long waiting lists, but from a review of both of the agencies' websites, it does not appear that any additional requirements exist for attendance beyond being a member of law enforcement (https://www. fletc.gov; https://www.ncfi.usss.gov/ncfi).

The Technical Working Group for Electronic Crime Scene Investigation (TWGECSI), working with the U.S. Department of Justice, National Institute of Justice, published a Guide for First Responders for electronic crime scenes (TWGECSI, 2001). This publication was one part of a full guide that was created to assist state and local law enforcement agencies with the growing number of crimes involving digital evidence (TWGECSI, 2001). This first publication consisted of approximately 80 pages of reference materials, ranging from the question of what is electronic evidence to a 30 page listing, by state, of technical resources that are available nationwide (TWGECSI, 2001). These guides were made available, at no cost, on the website of the National Institute of

Justice (TWGECSI, 2001). It is not known if the agencies surveyed in the current study have taken advantage of these training offerings or publications.

As mentioned previously, the FBI has a National Cyber-Forensics and Training Alliance (NCFTA) that deals with transnational cybercrime, and brings together local agencies, academia, federal law enforcement, and private industry (Cyber Crime, 2015). However, the NCFTA is considered an international alliance that is used to help protect cyberspace for individuals worldwide, and does not have a local focus on cyber crimes, so it is not considered as a viable training opportunity in this paper (Cyber Crime, 2015).

Another agency that was previously mentioned also provides training to law enforcement in the area of cyber crime. The National White Collar Crime Center (NW3C) provides training to law enforcement in the areas of computer forensics and cyber and financial crimes investigations. These training opportunities are offered in many different locations throughout the United States as well as online (NW3C, 2015). Finally, the NW3C also provides Whitepapers and publications at no cost on relevant areas of cyber crime and digital investigations (NW3C, 2015).

A comprehensive review of this literature suggests that many national studies were completed in the early part of the decade, but recently, most needs analyses have been conducted on a small scale, such as the study by Gogolin and Jones (2013). Further, there are many free training opportunities and educational resources available to state and local law enforcement agencies in the United States. The leads to the question presented in this study, which is what are the current training levels, needs, and perceptions of abilities of law enforcement agencies and prosecuting attorneys in the State of Indiana when investigating and prosecuting crimes involving digital evidence.

CHAPTER 3. METHODOLOGY

A total of three surveys were conducted, two for law enforcement agencies and one for prosecuting attorneys. The first survey for law enforcement was sent during a pilot study, and the second law enforcement survey and the prosecuting attorneys' surveys were modified based upon the results of the pilot study. These two revised surveys were sent to a larger number of agencies. The results of each are discussed in turn.

3.1 Pilot Study

As previously mentioned, a pilot study was conducted in November 2014 on this issue. Indiana has approximately 570 law enforcement agencies, and for the pilot study, a random number generator was utilized to select 30 of those agencies to participate in a survey. The pilot study consisted of a nine-question survey with voluntary participation, and the only potential identifying information collected was the size of the agency responding. An application for research was submitted to the Purdue University Institutional Review Board (IRB), and the response received from the IRB stated that the study was exempt from review. The findings of the pilot study affected the methodology used in the full study, and therefore the results of the pilot study are included the methodology section of this paper.

The questions on the pilot study survey inquired into the size of the responding agency, whether the agency had a digital forensics expert on staff, and if so, whether that individual was employed solely in that capacity. If the agency did not have a digital forensics expert on staff, the survey inquired into the reason, with the answer options limited to an expert is not needed, a lack of funding, or other. Further, the survey inquired into whether the agency had hired outside expert assistance for digital investigations, whether that assistance cost the agency financially, and how that outside assistance was located. Finally, the pilot study questioned whether these agencies had officers who attended digital forensics training, and how each agency ranked its own ability to effectively investigate a case involving technology.

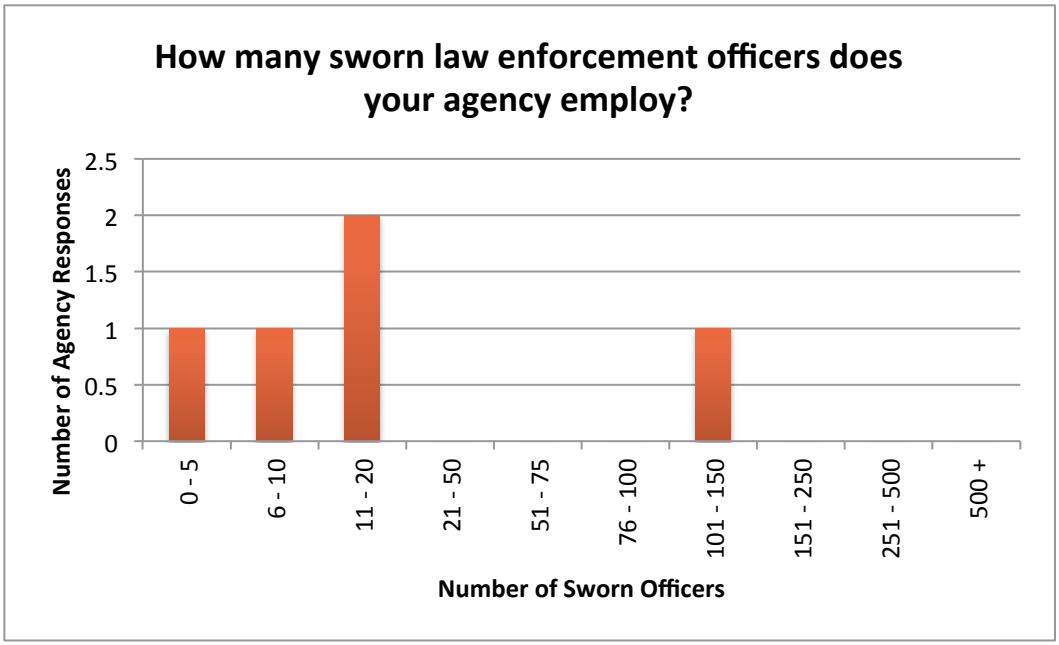
Through Internet searches and telephone calls to the randomly selected agencies, email addresses were collected. A total of 24 addresses[2] were successfully collected out of the 30 agencies selected. Email invitations were sent to these 24 agencies with a link to take the survey. Two invitations were returned as incorrect email addresses. After the initial invitation, only four emails were opened and one survey was completed. One week later, a reminder email was sent to the non-responding agencies. A total of ten of the email invitations were opened, seven of the surveys were started, and one more survey were completed, for a total of five complete survey responses. The data from the pilot study is based upon those five responses.

[2] One interesting discovery during this process by the researchers was the large number of Indiana law enforcement agencies that still do not have websites or basic contact information available via the Internet.

3.2 Pilot Study Results

The five responding agencies varied in size from very small to fairly large when counting the number of sworn law enforcement officers. The size of the responding agencies is noted in table 3.1.

Table 3.1: Number of Sworn Officers Per Responding Agency

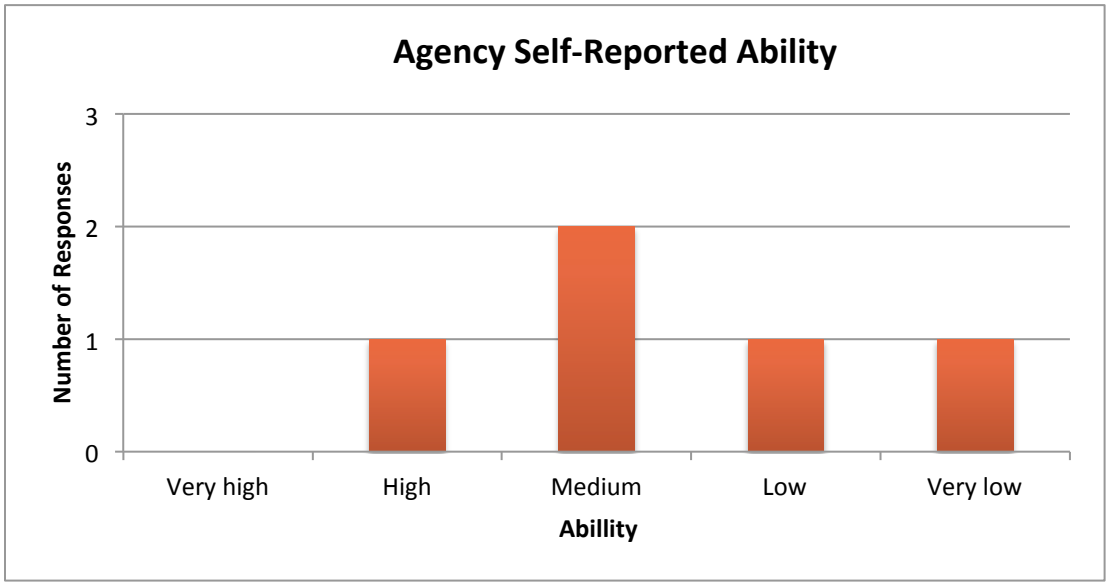


None of the responding agencies employed a full time digital forensics expert, and even though the response size was extremely small, this response was somewhat surprising. Four of the agencies responded that there was no funding to employ this type of expert, and only one indicated that there was no need to hire an expert of this type. Three of the responding agencies had previously sought outside assistance for a digital forensics investigation, and out of those three agencies, only one had to pay for that outside assistance. One of those agencies used another law enforcement agency to find that outside expert assistance, with the other two respondents indicated “other” as a means for locating this assistance.

Two of the five respondents (40%) had an employee in their agency attend digital forensics training. Interestingly, even with the lack of having a forensics expert employed, using outside experts, or attendance at training courses, the agencies' ratings of their own ability to effectively investigate a case involving digital evidence were higher than expected.

The results of the question regarding agency perception of ability to investigate crimes with digital evidence are summarized in Table 3.2. The mean response to the question of an agency's ability to effectively investigate was 3.4, which was directly between the "Medium" response and the "Low" response. So even with these higher than expected self-reported abilities, overall, the ability of these agencies to investigate cases involving digital evidence was still medium to low.

Table 3.2: Agency Self-Reported Ability



The results of the pilot study provided certain expectations for the full study. Indiana agencies were not expected to have the tools, training, knowledge, or capability to effectively investigate crimes with digital evidence. Further, it was obvious that certain

questions were lacking, such as the number of training opportunities employees had attended, the perceptions of prosecuting attorneys, and whether it is perceived that there has been a change in the incidence of crimes involving digital evidence.

3.3 Full Study Methodology

It became apparent during the preparation of the pilot study that it was extremely inefficient to attempt to obtain the email addresses of all 570 law enforcement agencies in addition to the 92 prosecuting attorneys' offices in Indiana. The law enforcement survey was also redesigned, to include questions on the areas of the number of training courses attended, the perceptions of local judges, juries, and prosecuting attorneys' understanding of digital evidence issues, whether there is a perceived increase or decrease in the incidence of digital evidence, and an extra "other" question that allowed a written in response for any information that was deemed relevant to the survey and that the respondent believed was important for the study.

Additionally, a similar survey was designed for the prosecuting attorneys' offices, with questions related to the admission of evidence during trial, the training of staff, and the perceptions of judges, juries, and local law enforcement abilities to work with digital evidence. Both questionnaires are included in Appendices A and B. The surveys were created on the Qualtrics survey system, which has a built in email system that provides information on whether the email was successfully delivered to the recipients, and allows a subsequent mailing to only those participants who have not yet responded.

Once the surveys were fully designed, the task of collecting the email addresses of the relevant law enforcement agencies in Indiana was begun. The State is designed with

one Sheriff's Department in each county (92 total), one[3] Prosecuting Attorneys' Office in each county (91 total), and many local city and town law enforcement agencies.

In the interests of reaching as many agencies as possible while also attempting to ensure a full representation of the agencies in the State, the decision was made to contact each sheriff's department and prosecuting attorneys' office directly to obtain email addresses. To contact as many local city and town law enforcement agencies, the Indiana Chief of Police Association sent out the survey link to its membership (189 agencies) in its weekly informational email. To obtain the email addresses of the sheriff's departments and prosecutors' offices, a quick Internet search was conducted on each agency. If an email address was not located through that search, the agency was contacted by telephone advising the basics of the survey and requesting an email address. Approximately five days after the first attempted contact with the agency, any non-responding agency was re-contacted, again explaining the study and requesting a contact email. Of the 92[4] sheriff's departments, one would not supply an email address over the telephone, and nine more did not respond to messages left, leaving a total of 83 email addresses collected. Upon distribution, nine of those 83 addresses bounced, meaning a total of 74 sheriff's departments should have received the link to the survey. An initial message was sent to these 74 departments with the link to the survey, and if they did not respond, a follow-up email was sent 14 days after the original email containing the survey information and link

[3] There are actually 92 counties in Indiana, but Dearborn and Ohio Counties have one Prosecutors' Office that they share. All other counties have their own Prosecutors' Office.

[4] The Indiana State Police were also added in to this group, so the total agencies directly contacted via email was 83.

was sent. Between these two messages, a total of 14 surveys were completed, for a response rate of 19%.[5]

The same process was conducted for the prosecuting attorneys' offices, with one office not willing to provide an email address, and four offices not returning messages left requesting an address. A total of 89 emails were initially sent, with a reminder survey sent to non-respondents approximately 13 days later. Six of those emails with the survey links hard bounced, leaving the email successfully distributed to 83 prosecutors' offices. A total of 18 surveys were completed, for a response rate of the Prosecuting Attorneys' Survey of 21.7%.

As noted earlier, there were an additional 189 local law enforcement agencies that had the email distributed to them via a weekly email received from the Indiana Chief of Police Association. Information about the survey and link were included two separate weekly emails sent out two weeks apart, and a total of 12 responses were received from this method. When adding these 12 responses to the 14 Sheriff's Department responses, the total response rate[6] for the law enforcement survey was only 9.9%.

The survey questions used in this study were based upon the information sought in previous needs assessments that have been conducted and reviewed by the author. Further, the author is a licensed attorney with experience working in criminal law, and many of the questions for the prosecuting attorney's offices were based upon this personal experience and discussions with current prosecuting attorneys. Finally, the

---

[5] The researchers would like to thank the Indiana Chief of Police Association for agreeing to include this information in their weekly emails. While the response rate was small, it still provided a more diverse sample than would have otherwise occurred.

[6] The number of 74 total Sheriff's Departments where delivery of the email was presumed was added to the 189 Chiefs of Police where delivery was presumed, for a total potential sample size of 263.

answers that were received in the full study were mostly expected, based upon the results of the pilot study. This similarity provides support for the reliability of the results of the full study.

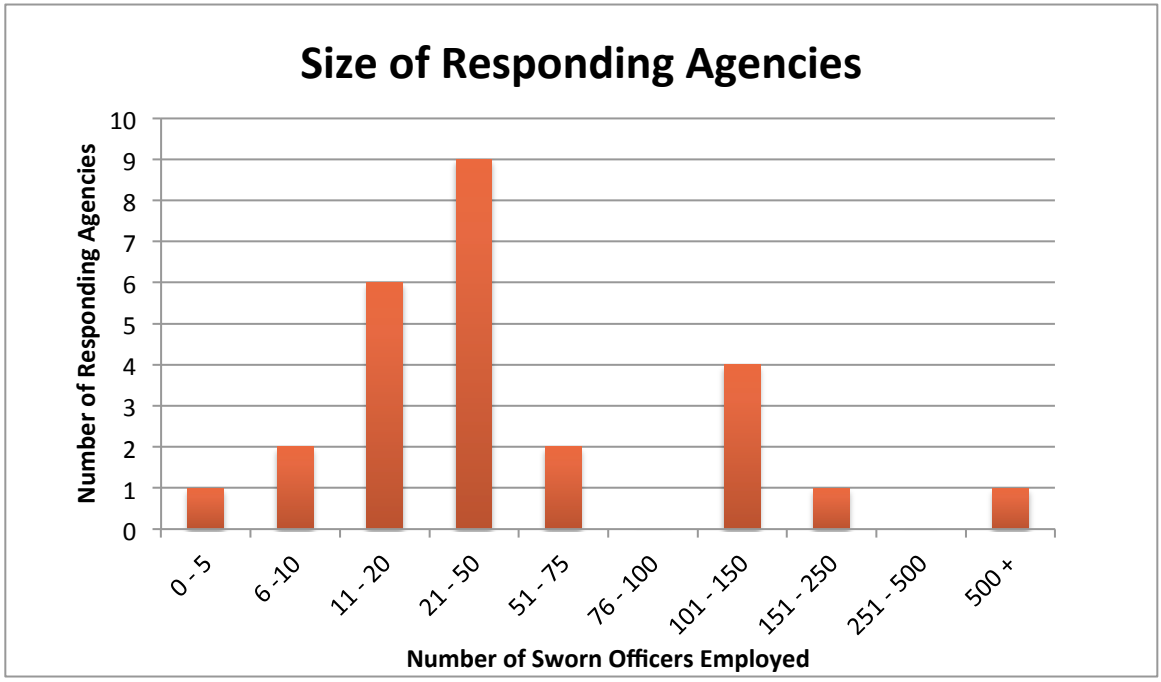
CHAPTER 4. RESULTS

The results of both the Law Enforcement Survey and Prosecuting Attorneys' Survey are discussed in turn. Additionally, the data from pilot study is compared to the data from the Law Enforcement Survey, with explanations attempted for any observed variations in results.

4.1 Law Enforcement Survey

A total of 26 agencies of varying sizes responded, but a majority (58%) of them employ between 11 and 50 sworn officers. Breaking this down further to allow better comparison with the pilot study shows that six of the agencies employ between 11 and 20 and nine of the agencies employ between 21 and 50 officers, for a total of 23% of the responding agencies employing between 11 and 20 sworn officers and 35% of the responding agencies employing between 21 and 50 sworn officers. In the pilot study, 40% of the responding agencies employed between 11 and 20 sworn officers, which is a much smaller average agency size than responded to the full study. The results of this question are displayed in Table 4.1, but the great takeaway from this response size versus the pilot study is that a greater percentage of the responding agencies in the full study have more sworn officers, meaning they likely have greater access to resources for more specialized training and investigations.

Table 4.1 Number of Sworn Officers Employed



A total of ten of the responding agencies employ an individual considered an expert in the field of digital forensics, but seven of those ten experts have other assigned duties as well. Of the 16 agencies that do not have a digital forensics expert employed, 80% responded that lack of funding was the reason. A total of 22 responding agencies[7] have sought outside expert assistance with a digital forensics investigation over the past five years, but 20 of those 22 hiring agencies did not have to provide compensation for that expert assistance. This expert assistance was typically located through referrals from other law enforcement agencies, or by using experts from other agencies, which could explain why compensation was typically not required.

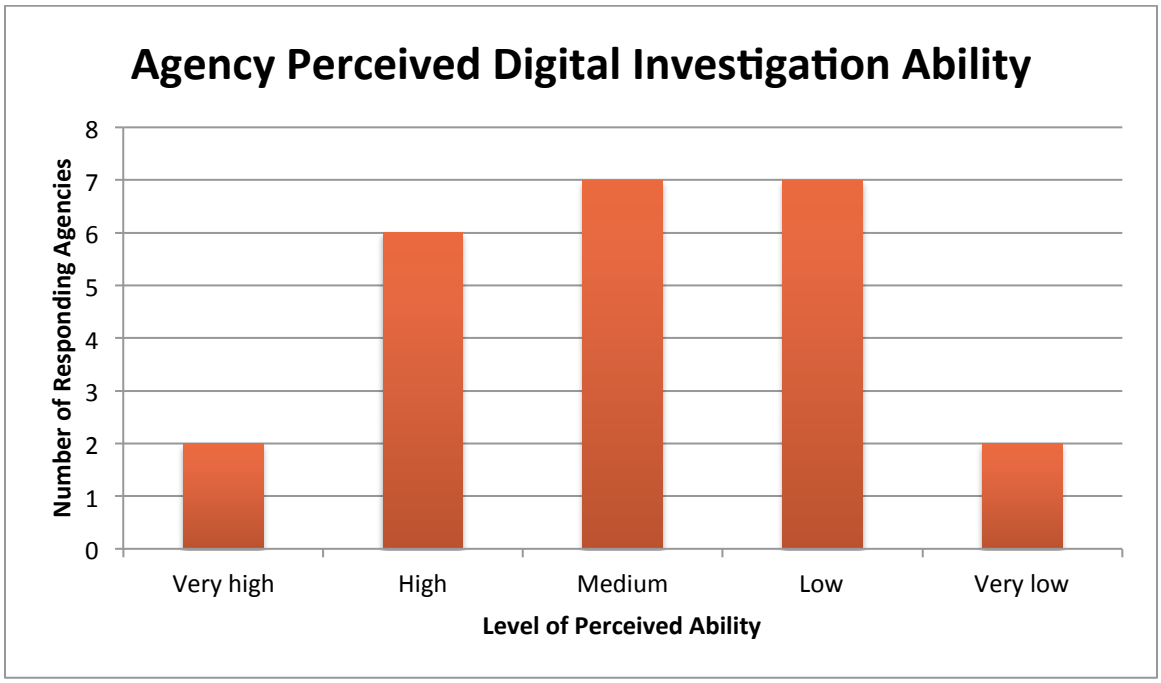
[7] Only 25 agencies responded to this and the following questions on employee training

When questioned about attendance at digital forensics training course in the past five years, 15 agencies (60%) responded that their employees had attended such training, with seven of those 15 attending six or greater training courses over that five year period. This is a greater percentage than was found in the pilot study, where only 40% of the respondents had an employee who had attended digital forensics training. Additionally, in the full study, six of those 15 agencies have an employee on staff who has obtained a formal degree or certification related to digital forensics. This means that of the 25 agencies potentially able to respond to this question, 24% do have an employee with a formal degree or certification related to digital forensics. The reasoning given by agencies that have not had an employee attend training on digital evidence was a lack of funding available for this training (6 responses), the time of job requirements prohibit attendance at a digital evidence training course (3 responses), and a lack of interest from employees on staff (2 responses). One agency reported insufficient manpower to employ someone in this area under this question.

Similar to the pilot study, the agencies were asked their perceptions of their ability to effectively investigate a crime involving digital evidence. As shown in Table 4.2, of the 24 respondents, 14 perceived their ability to be medium or low, with another two perceiving an ability of very low. In comparison with the pilot study where 80% of the respondents perceived their ability to be medium, low, or very low, only 67% in the full study perceived their ability to be medium, low, or very low. A further question that assists in understanding this difference is that 52% of respondents in the full study believed their office had adequate resources to effectively conduct an investigation into crimes involving digital evidence. So as previously noted, the difference between the

results pilot study and the full study in agency perceived ability can be explained by the number of larger agencies, with more experts on staff and more resources available, who participated in the full study. Additionally, as a reminder, only 40% of the agencies in the pilot study had an employee who had attended digital forensics training, compared to 60% of the responding agencies in the full study with employee attendance at digital forensics training, which could also have a great impact on an agency's perceived ability of investigation.

Table 4.2 Agency Perceived Ability to Investigate a Crime Involving Digital Evidence



The responding law enforcement agencies were also questioned on their perceptions of local prosecuting attorneys to present digital evidence, and 38% of the respondents perceived these abilities to only be somewhat effective, while 33% perceived the abilities to be moderately effective. Surprisingly, 13% of the responding law enforcement agencies perceived their local prosecuting attorneys' abilities to present

digital evidence at a hearing or trial to be extremely effective. Additional questions were asked about the perceived abilities of local judges to understand digital evidence and its admissibility at trial and the abilities of juries to understand digital evidence when it is presented at trial, with 79% percent of respondents believing the Judges' abilities are medium or high, and 80% of respondents believing the Juries' abilities to understand are medium or high.

While these numbers are interesting, none are truly important unless it is actually necessary for law enforcement to have the ability to investigate crimes involving digital evidence. Of the responding agencies in the full study, 100% reported that the number of crimes involving digital evidence that their agency has investigated in the past five years has at least remained steady, and 84% of the agencies reported that the number of investigations has increased. This large majority of agencies that have had an increase in digital evidence investigations indicates that it is important for law enforcement agencies in Indiana to have this knowledge and ability. An additional question that may provide some level of assurance to those concerned inquired into the ability of officers and evidence technicians in the responding agencies to identify, collect, and preserve digital evidence. A total of 67% of respondents rated their ability as either very good or good, and an additional 25% rated their ability as fair. Only 8% perceived their officers' and technicians' digital evidence identification, collection, and preservation abilities to be poor.

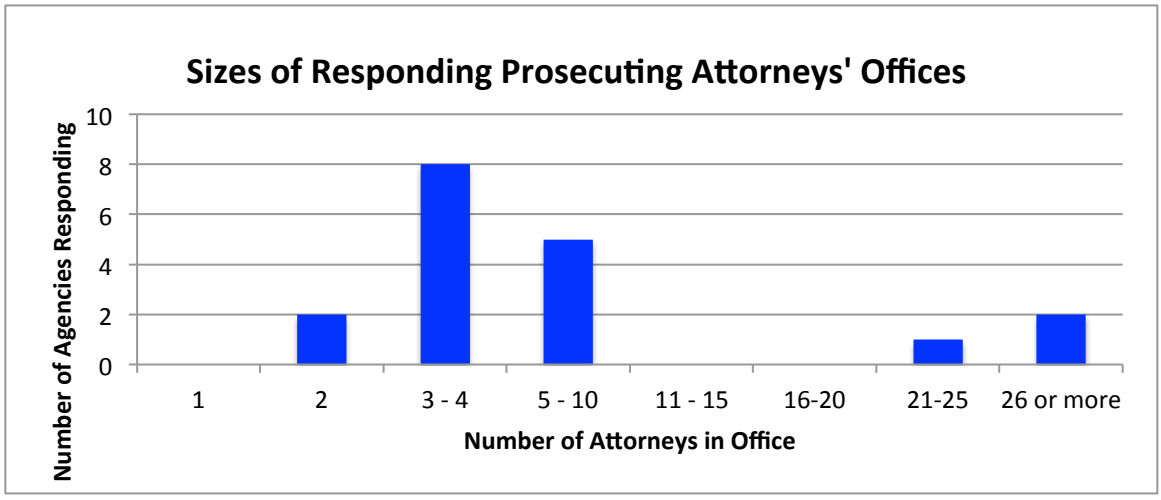
However, there is concern that many of these perceptions may be overinflated, as only 46% of the responding agencies have a standard operating procedure regarding the identification, collection, and preservation of digital evidence, and 67% expressed a

concern related to their ability to collect digital evidence from the cloud or the internet of things. Finally, the law enforcement respondents were granted the opportunity to express any other concerns related to the area of digital evidence, and the comments noted are listed in Appendix B.

4.2 Prosecuting Attorneys Survey

The population of an Indiana county is typically reflected by the number of attorneys employed in a prosecutor's office, so it was important to the researcher to have this data in the survey responses. A total of 44% of the responding offices employ between three and four attorneys, and an additional 28% of the responding offices employ between 5 and 10 attorneys. For example, a county with a population of approximately 45,000 employed a total of four prosecuting attorneys[8]. Since 83% of the responding offices had 10 attorneys or less, this indicates that the responding prosecuting attorneys' offices are from relatively low population counties. The results are displayed in Table 4.3, and should be recalled while reviewing the remaining survey responses.

Table 4.3 Sizes of Responding Prosecuting Attorney Offices



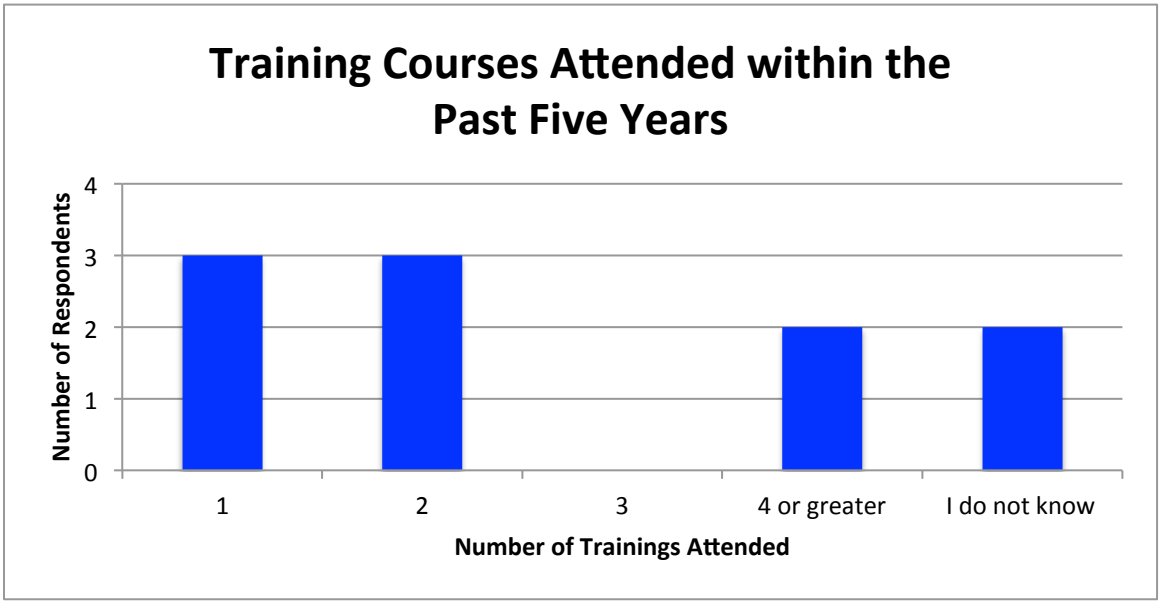
[8] The researcher previously worked at a county of this size, and used first hand knowledge of that county to provide this information.

The next inquiry was whether the office had received investigations in the past five years that included digital evidence, and 17 of the respondents answered in the affirmative. Further, 83% of the respondents' offices had presented digital evidence at a hearing or during trial in the past five years. To help prepare for that presentation of digital evidence, the attorneys typically worked with the submitting officer or investigator (73%), attended training (27%), or worked with an outside expert (27%). Certain agencies reported no need for additional training (20%) and another 20% conducted self-research, utilized their IT department, or another attorney in the officer.

Only 17% of Indiana prosecutors' offices have hired an expert to assist their attorneys in presenting digital evidence in court over the past five years, and all respondents indicated they found this expert through a referral from law enforcement. Contrary to the law enforcement responses, 100% of the prosecuting attorney offices that hired an expert compensated that expert for his or her services. When asked about the success of their office in presenting digital evidence in court, 80% of the respondents perceived that their office has been successful as measured by the outcome of the cases.

Training in the area of digital evidence is perceived to be just as important for attorneys as law enforcement officers, and 56% of the responding offices had at least one employee attend a training on digital investigations or cyber crime within the past five years. Of the offices with one employee attending training, the response rates were evenly spread with regard to the total training courses attended. These results are shown in Table 4.4.

Table 4.4 Number of Training Courses Attended within the Past 5 Years



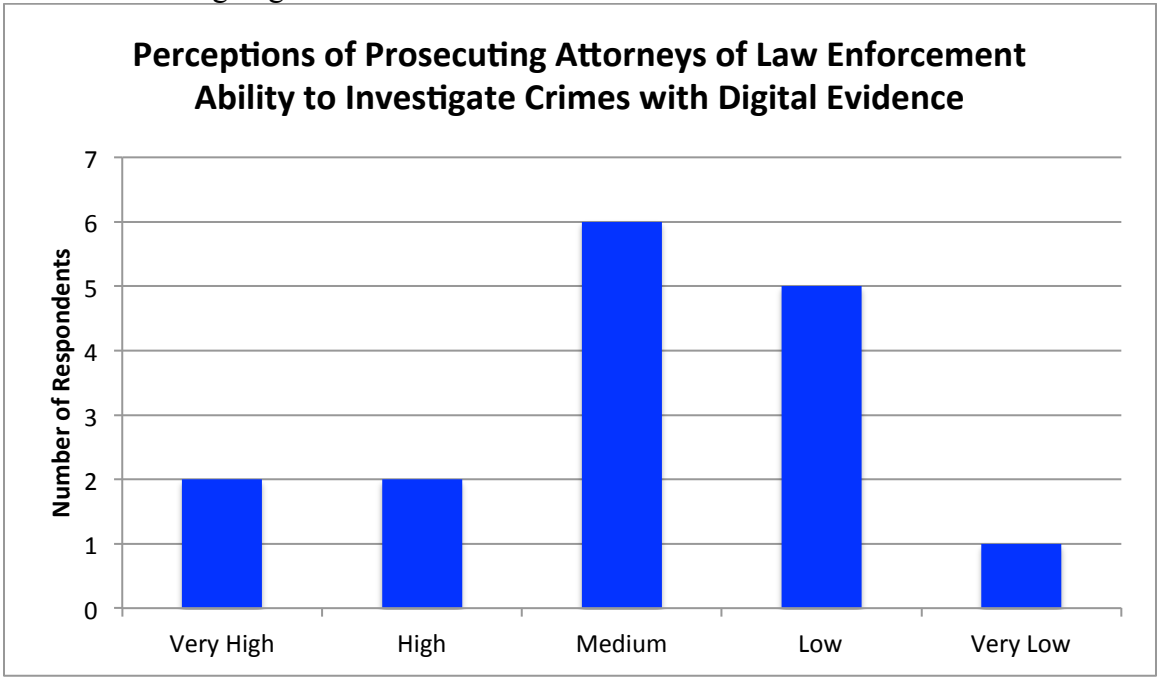
While it is important that the prosecuting attorneys' offices have had employees attend digital evidence related trainings over the past five years, only 20% of the offices reported having an employee with a formal degree or certification related to digital evidence, 60% responded that they do not have such an employee, and 20% responded that they do not know if such an employee is on staff. Additionally, 78% of the respondents with employees attending training courses over the past five years had attorneys attending those courses, while 44% of those with employees attending trainings over the past five years had investigators who had attended those courses.

An additional concern is the condition of any digital evidence submitted to prosecutors' offices by investigators, and 50% of the respondents indicated that a moderate or substantial amount of additional effort is needed to prepare evidence as submitted from law enforcement for a hearing or trial. Only 13% responded that minimal effort is required to prepare the evidence for court. Conversely, 69% of respondents did

indicate they were confident in using the digital evidence, in the condition as submitted by law enforcement, without any further preparation for trial.

The prosecuting attorneys were also asked to rate their perceptions of the ability of local law enforcement agencies to investigate crimes involving digital evidence, and the results are included in Table 4.5. As can be seen, the overwhelming majority (75%) of respondents perceive that their local law enforcement agencies abilities to investigate crimes involving digital evidence are medium, low, or very low.

Table 4.5 Perception of Prosecuting Attorneys of Local Law Enforcement to Investigate Crimes Involving Digital Evidence



Interestingly, 75% of respondents believed that their judge's understanding of issues pertaining to digital evidence and its admissibility at trial was either medium or high, and 87% of respondents believed that local juries' abilities to understand digital evidence when presented was either medium or high. When asked about the incidence of cases that involve digital evidence over the past five, 87% of the prosecuting attorneys

perceived either an increase or a significant increase in the rate of change. Finally, the prosecuting attorneys were presented with the same opportunity to provide comments they believe to be relevant to this study, and those are listed in Appendix B.

CHAPTER 5. DISCUSSION

As noted in the Literature Review, there is a concern about both the abilities of law enforcement to investigate crimes with digital evidence, backlogs in digital forensics crime labs, and capabilities of the investigators in those labs. Because of these backlogs and the nature of digital forensics investigations, it makes sense that law enforcement agencies would move as much of digital investigations in house as is possible. Without having a digital forensics investigator on staff, this is nearly impossible. Responses from current digital forensics investigators in both government and private industry reported as recently as July, 2013, that the lack of standards and tools, and more importantly, the lack of skills, training, and certification, are a challenge (Henry et al., 2013).

The results of the full study indicate that Indiana law enforcement agencies and prosecuting attorneys have a greater capability to conduct investigations of crimes involving digital evidence than was shown in the pilot study. This conclusion is based upon the greater number of agencies with employees that have attended a digital evidence training course. While only 38% of the responding agencies employed an individual considered to be a digital forensics expert, 60% of the responding law enforcement agencies and 56% of the prosecuting attorneys' offices had at least one employee that had attended training on digital forensics within the past five years. Of the 60% of law

enforcement agencies that had an employee attend digital forensics training, 40% of those respondents have someone on staff with a formal degree or certification in a field related to digital forensics. This indicates that a majority of the agencies have some minimal level of ability regarding investigations involving digital evidence, and some have an even greater level of expertise with employees that have related certifications or degrees. Unfortunately the question did not differentiate between certifications or degrees, which are two substantially different levels of knowledge, and this information could have provided a greater level of understanding of the agencies' capabilities. The 60% digital forensics training attendance rate in the full study is greater than the 40% reported in the pilot study. However, as previously noted, the responding agencies in the pilot study were smaller, and may have fewer resources. Further, the methodology of contacting the participants was different between the pilot study and full study, which may have led to selection bias, and is further discussed in the limitations section.

Of interest to the author is that of the 40% of law enforcement agencies without an employee on staff that has attended digital forensics training; 67% responded that lack of funding is the main reason. Conversely, when asked about whether the offices have sufficient resources to investigate crimes involving digital evidence, 52% of the respondents reported that yes, they do have sufficient resources. The agencies appear to be separating training from resources available, and could be considering digital forensics tools and outside agencies in the resources question. Additionally, as previously discussed in this paper, there are many free resources and training opportunities offered by multiple different agencies and organizations. It is unknown if these agencies are

unaware of the free training opportunities, but providing information on these resources should be a priority for associations and organizations involved with law enforcement.

Participating agencies perceive a fairly low ability to investigate crimes involving digital evidence, with 29% perceiving their ability to be medium, 29% perceiving their ability to be low, and 8% having a very low perception. When reviewing these numbers from a capability standpoint, 62% of responding agencies believe they have at least a medium, high, or very high ability to investigate crimes with digital evidence. The response from the prosecutors was very similar, with 64% of respondents perceiving law enforcement's ability to be medium, high, or very high. However, the prosecutors responded that they did not regularly have confidence in the digital evidence received by their offices from law enforcement, with 69% of respondents being only confident or moderately confident (a mean of 3 out of 5) that the evidence will not need additional work prior to presentation in court. This is important to pursue further, as a lack of perceived ability may inhibit officers from pursuing investigations into these areas.

Some lingering questions that remain and are not addressed by this study are the prevalence of crime with digital evidence in Indiana that is not pursued by law enforcement because of this perceived lack of ability, and what else is needed for law enforcement to increase their perceived ability in investigations of this nature. There may be cases of cyberstalking or hacking into social media accounts when the victims are referred to civil resources with no criminal investigation because of the lack of training. Additionally, the training courses that employees have attended may not have been thorough enough to increase the perceived capabilities of law enforcement to investigate crimes with digital evidence. Or it could be as simple as a need for more employees to

attend basic digital forensics evidence training to increase the baseline of knowledge in these agencies. These issues should be further pursued by future research.

As to the ability of prosecuting attorneys, judges, and juries, the law enforcement agencies ranked them higher, with 54% of prosecuting attorneys' offices deemed at least effective in introducing digital evidence, 81% of judges having at least a medium ability to understand digital evidence admissibility, and 80% of juries having at least a medium ability to understand digital evidence presented at trial. When asked the same questions about judges and juries, the prosecuting attorneys' perceived abilities of 75% and 87% respectively. It is revealing that the respondents from both surveys have greater perceptions of the ability of non-law enforcement to understand these detailed, and sometimes confusing, technological issue than they do of law enforcement to actually investigate them.

An interesting finding was that only 9% of law enforcement agencies that hired an outside expert provided compensation to that expert, while 100% of the prosecuting attorneys' offices provided compensation to a hired expert. This could be because the outside expert sought by law enforcement came from a different law enforcement agency, while the expert hired by the prosecutors came from the private sector or academia, which typically do require compensation.

Both groups agreed that the incidence of crimes involving digital technology has increased over the past five years, with 87% of prosecuting attorneys and 84% of law enforcement agencies reporting an increase. Overall, it appears that Indiana has made strides from the national needs analyses that were conducted at the turn of the century. However, there is still a great amount of training expertise that will be needed if the

prevalence in crimes that involve digital evidence continues to increase as it has over the past five years.

This current study has many limitations, one of which is the sample size. Future research should be conducted that contacts every law enforcement agency in Indiana, inquires into the whether there are investigative needs not being met for the citizens of Indiana, and pursues the question of why agencies do not seem to be aware of the availability of free training opportunities. Further, many of the questions used metrics such as very high, high, medium, low, and very low, which could be interpreted differently by the respondents. Some may have better abilities than others; yet answer with a lower ranking based upon a different idea of what is considered a medium ability.

Additionally, it is likely that the respondents from the Indiana Chief of Police Association already are interested in the area of digital investigation, and may have a greater interest in ensuring that their office remains apprised of new investigative techniques. The mere fact that the specific Chiefs are members of this association already indicates an increased level of interest in receiving information deemed relevant to the occupation, as their membership includes a weekly email from the association. This could mean that smaller agencies without the capabilities, that were included in the random sample of the pilot study, were not notified of the full study survey because they are not members of the association. A selection bias could also be present in the respondents' interest when reading the link in the email; if they are already interested in the area of digital evidence, they might be more likely to respond to a survey on the subject. This greater interest may also mean a greater importance is placed on the area of digital evidence retrieval, collection, preservation, and analysis within these responding agencies.

It is also not clear how many hours of digital evidence training the officers have participated in, and whether that training was a one time only event or takes place on an annual basis. The study by Gogolin and Jones (2010) specifically asked about the amount of annual hours devoted to digital forensics training, and that is a question that could be included in future studies in Indiana. This study only inquired into the number of training courses attended over the previous five years that all employees may have attended. Further, there were no follow up questions in the current study on why each agency perceived its ability to investigate crimes involving technology as low, medium, or high, or what else, beyond resources, might be needed to improve their abilities. While funding was noted as a reason for non-attendance at training courses, 52% of respondents indicated they do have the necessary resources to conduct effective investigations of crimes involving digital evidence. More detailed questioning on this subject could explain more clearly what each agency perceives its needs to be in this area. These answers could range from funding, availability of officers, increases in technology and the inability to maintain training to meet the new technologies, or just a lack of a desire for further training on these types of investigations as there are other, more pressing needs.

Another area that is not clear is how often Indiana law enforcement agencies investigate crimes involving digital evidence, or whether investigations have not been conducted due to a lack of ability. The responses indicate that the prevalence of crimes involving digital evidence has increased over the past five years, but the baseline of the incidence of digital evidence involved crime from five years ago is unknown. This information could assist in determining the necessity of further training, funding, or a

greater focus in the area of digital evidence investigations for Indiana law enforcement agencies

There are some recommendations to help meet some of the lingering concerns about agency capabilities that are secondary the results of this study. One recommendation for both law enforcement and prosecuting attorneys is an increase in funding and resources specifically targeted to the issues of digital evidence investigation. As lack of funding was described as the number one reason for the lack of attendance at digital forensic training courses and 48% of responding agencies noted a lack of funding for resources, it is incumbent upon the agencies, their associations, and State Legislatures to recognize this deficit and provide the resources necessary for Indiana law enforcement to effectively conduct digital crime investigations. A second recommendation is that the Indiana Law Enforcement Academy should include a training module in its Basic Training Course on collection and identification of digital evidence, and more advanced courses should be offered for officers wanting to increase their knowledge in this area. A top down approach on training may assist smaller and lower funded agencies in gaining some minimum level of knowledge and experience in this rapidly changing and demanding area.

A third recommendation is for a resource list to be created and distributed to both Indiana law enforcement and prosecuting attorneys that includes training opportunities, identification of local experts in the field, and the availability of academic resources in the State to assist with investigations. It is clear from the literature review that many free training opportunities are available, but 67% of the responding law enforcement agencies that did not have an officer on staff who had attended a digital forensics training reported

a lack of funding was the main reason. There seems to be a disconnect between the many free opportunities available and the knowledge of the agencies about these opportunities. A fourth recommendation is that each agency should establish Standard Operating Procedures (SOPs) for identifying, collecting, and preserving digital evidence. Guidelines for these SOPs should be created by the Indiana Law Enforcement Academy or the Indiana State Police and distributed to the agencies across the State to help ensure best practices are utilized. Finally, more research should be conducted in the State of Indiana that includes a greater number of agencies to further analyze the needs and capabilities in the area of digital investigations.

CHAPTER 6. CONCLUSION

Within the State of Indiana many law enforcement agencies are not participating in the training that is needed to effectively investigate crimes involving digital evidence. Over a decade has passed since the initial studies conducted by the Institute for Security and Technology Studies and the U.S. Department of Justice, and while the capabilities of Indiana law enforcement agencies has increased, participation in training and available resources seems to be still lacking in this state. Additionally, technology has improved, and more crimes involve digital evidence, which has put law enforcement at an even greater disadvantage. Federal agencies and academia have tried to assist by providing training, but it does not appear that local law enforcement agencies are taking full advantage of these opportunities. There is still much more work to be done to ensure that Indiana law enforcement is aware of the available resources, and has the tools, training, and resources necessary. It is hoped that this study will further the goal of meeting these demands.

Despite the concerns raised, this research is important to both the law enforcement community and academia in continuing the review of their capabilities. It is also available for use by legislatures and organizations in determining what is needed to further the advancement of abilities in investigating digital crime. Further, the

contribution of this research to this area continues to build on the knowledge from the previous studies conducted on both national and local levels.

Future research should be conducted that inquires into the reasons that law enforcement agencies have such a low perception of their abilities, but a high perception of judicial and jury capabilities of understanding, clarification of the number of employees with degrees versus certifications in digital evidence fields, a larger representative sample of the agencies in the state, and determines the specifics of the needs by agencies that are required to improve their self perceived abilities.

LIST OF REFERENCES

LIST OF REFERENCES

About (webpage) for National Computer Forensic Institute (2014). Retrieved from https://www.ncfi.usss.gov/ncfi/pages/about.jsf

Basic Training – Tier I (webpage) for Indiana Law Enforcement Academy (2014). Retrieved from http://www.in.gov/ilea/2380.htm

Bhaskur, R. (2006, February). *State and Local Law Enforcement is not Ready for a Cyber Katrina*. Communications from the ACM, 49(2), 81-83.

Bossler, A., & Holt, T. (2011). *Patrol officers' perceived role in responding to cybercrime*. Policing: An International Hournal of Police Strategies & Management, 35(1), p. 165-181.

Brenner, S., & Schwerha, J. (2002). *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*. The John Marshall Journal of Computer and Information Law, 20(347).

Bulbul, H. I., Yavuzcan, G. H., & Ozel, M. (2013). *Digital Forensics: An Analytical Crime Scene Procedure Model (ACSPM)*. Forensic Science International, 233, 244 - 256.

Casey, E., Katz, G., & Lewthwaite, J. (2013). *Honing digital forensic processes*. Digital Investigation, 10, 138-147.

Center for Strategic and International Studies, McAfee. (2014, June). *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara, CA.

Courses (webpage) for National Computer Forensic Institute (2014). Retrieved from https://www.ncfi.usss.gov/ncfi/pages/courses.jsf

Cyber Crime (webpage) for the Federal Bureau of Investigation (2015). Retrieved on October 17, 2015 from https://www.fbi.gov/about-us/investigate/cyber

Cybercrime and Investigative Technologies Section (webpage) for Indiana State Police (2015). Retrieved on October 17, 2015 from http://www.in.gov/isp/3234.htm.

Federal Buruea of Investigation (2014). *2014 Internet Crime Report*. Washington, DC: U.S. Govt Printing Office.

Gogolin, G., Jones, J. (2010). *Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business*. Information Security Journal: A Global Perspective, 19, 109-117.

Goodison, S., Davis, R., & Jackson, B. (2015). *Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Priority Criminal Justice Needs Initiative. Rand Corporation.

Henrry, P., Williams, J., & Wright, B. (2013, July). *The SANS Survey of Digital Forensics and Incident Response.* SANS Institute InfoSec Reading Room.

Hickman, M. J., & Peterson, J. L. (2004, September). *Census of Publicly Funded Forensic Crime Laboratories: 50 Largest Crime Labs, 2002*. Bureau of Justice Statistics Fact Sheet.

Inservice Training (webpage) for Indiana Law Enforcement Academy (2014). Retrieved from http://www.in.gov/ilea/2376.htm

Institute for Security Technology Studies (2002, June). *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment.*

Law Enforcement Training Courses (webpage) for Purdue University Cyberforensics Laboratory (2014). Retrieved from http://cyberforensics.purdue.edu/lawenforcement.php

National Institute of Justice. (2004). *Status and Needs of Forensic Science Service Providers: A Report to Congress.*

National White Collar Crime Center (webpage) (2015). Retrieved on October 17, 2015 from https://www.nw3c.org/

Pricewaterhouse Coopers, CSO Magazine, CERT Division of Carnegie Mellon University, & United States Secret Service. (2015). *U.S. cybersecurity: Progress stalled. Key Findings from the 2015 US State of Cybercrime survey*. Delaware.

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

Schedule (webpage) for National Computer Forensic Institute (2014). Retrieved from https://www.ncfi.usss.gov/ncfi/pages/schedule.jsf

Stampaugh, H., Beaupre, D., Icove, Dr. David J., Baker, R., Cassaday, W., Williams, W. (2000, August). *State and Local Law Enforcement Needs to Combat Electronic Crime.* U. S. Department of Justice, National Institute of Justice Research in Brief.

State, Local, & Tribal (webpage) for the Federal Law Enforcement Training Center (FLETC) (2014). Retreived from https://www.fletc.gov/state-local-tribal

Training Calendar (webpage) for the Federal Law Enforcement Training Center (FLETC) (2014). Retreived from https://www.fletc.gov/training-calendar

Training at FLETC (webpage) for the Federal Law Enforcement Training Center (FLETC) (2014). Retreived from https://www.fletc.gov/training-catalog

Technical Working Group for Electronic Crime Scene Investigation (TWGECSI) (2001). *Electronic Crime Scene Investigation: A Guide for First Reponders*. National Institute of Justice, U.S. Department of Justice, Office of Justice Programs.

Verizon (2015). 2015 Data Breach Investigations Report. *Verizon Enterprise.* Retrieved from http://www.verizonenterprise.com/DBIR/2015/

Weiner-Bronner, D., (2014, April 22). Report Shows Cyber Crime is on the Rise. *The Wir*e. Retrieved from http://www.thewire.com/technology/2014/04/report-shows-cyber-espionage-is-on-the-rise/361024/

West Virginia University College of Business & Economics (2008). *Survey of Forensic Service Providers.*

APPENDICES

Appendix A

Law Enforcement Agencies' Survey

1. How many sworn law enforcement officers does your agency employ?
    a. 0 – 5
    b. 6 – 10
    c. 11 – 20
    d. 21 – 50
    e. 51 – 75
    f. 76 – 100
    g. 101 – 150
    h. 151 – 250
    i. 251 – 500
    j. 500 +

2. Does your agency employ at least one person whom you would consider an expert in digital forensics?
    a. Yes
    b. No
    c. I do not know

    (If the Response to Question 2 is Yes, proceed to Question 2A. If the Response to Question 2 is No, proceed to Question 2B)

2A. Is this individual employed solely in the capacity of a digital forensics expert? (If the individual has other assigned job duties the proper answer is no.
    a. Yes
    b. No

2B. Please state the reason you do not have an individual employed as a digital forensics expert.
    a. Do not need an expert
    b. Do not have funding to employ an expert
    c. Unable to find a qualified expert
    d. Other _____

3. In the past five years, have you sought outside expert assistance with a digital crime investigation?
    a. Yes
    b. No

    (If the Response to Question 3 is Yes, proceed to Questions 3A and 3B.

3A. Did your office provide compensation to this outside expert?
    a. Yes
    b. No

3B. How did you locate the outside expert assistance? (please select all that apply)
    a. Referral from other law enforcement agency
    b. Indiana Prosecuting Attorneys Council
    c. Referral from local university or other academic source
    d. Referral from Training or Conference attended
    e. Telephone book
    f. Internet
    g. Other _____

4. In the past five years, have you or anyone in your agency attended digital forensics trainings?
    a. Yes
    b. No
    c. I do not know

    (If the Response to Question 4 is Yes, proceed to Questions 4A and 4B. If the Response to Question 4 is No, proceed to Question 4C.)

4A. How many different digital forensics training programs have you or your employees attended?
    a. 1
    b. 2-3
    c. 4-5
    d. 6 or greater
    e. I do not know

4B. Does at least one of your employees have a formal certification or degree related to digital forensics?
    a. Yes
    b. No
    c. I do not know

4C. Why have no officers/employees attended a digital forensics training program?
   a. Training in this subject matter area is not needed
   b. Officers do not have time to attend because of other job requirements
   c. No interest from officers/employees on staff
   d. No funding available for this type of training
   e. Other _____

5. Where do you rank your agency's ability to effectively investigate a case involving digital evidence?
   a. Very high
   b. High
   c. Medium
   d. Low
   e. Very low

6. Please rate your perception of the ability of your local Prosecuting Attorney's Office to present digital evidence at a hearing or a trial.
   a. Extremely effective
   b. Moderately effective
   c. Effective
   d. Somewhat effective
   e. Not effective
   f. Prefer not to answer

7. Please rate your perception of the ability of your local judges to understand digital evidence and its admissibility at trial.
   a. Very high
   b. High
   c. Medium
   d. Low
   e. Very low
   f. Prefer not to answer

8. Please rate your perception of the ability of your local juries to understand digital evidence when it is presented at trial.
   a. Very high
   b. High
   c. Medium
   d. Low
   e. Very low
   f. Prefer not to answer

9. Do you believe your office has adequate resources to effectively conduct an investigation of a crime involving digital evidence?
    a. Yes
    b. No
    c. Other _____

10. In the past five years, please rate your perception of the number of crimes your office has investigated that involved digital evidence.
    a. Significantly increased
    b. Increased
    c. Remained steady
    d. Decreased
    e. Significantly Decreased

11. Please rate your perception of the ability of your sworn law enforcement officers and evidence technicians to identify, preserve, and collect digital evidence.
    a. Very good
    b. Good
    c. Fair
    d. Poor
    e. Very poor

12. Does your agency/office have a defined standard operating procedure regarding the identification, preservation, and collection of digital evidence?
    a. Yes
    b. No
    c. Other _____

13. Are you concerned about your ability to collect digital evidence from the cloud or the Internet of things?
    a. Yes
    b. No
    c. I do not know what the cloud is
    d. I do not know what the Internet of things is
    e. Other _____

14. Please provide any other comments you have with regard to the ability of your office to investigate crimes involving digital evidence.

Appendix B

Prosecutors' Offices Survey

1. How many prosecuting attorneys does your office employ (including the Elected Prosecutor, Chief Deputy, and any Deputy Prosecuting Attorneys that work either full-time or part-time)?
    a. 1
    b. 2
    c. 3 - 4
    d. 5 - 10
    e. 11 – 15
    f. 16 – 20
    g. 21 – 25
    h. 26 or more

2. In the past five years, has your office received investigations from law enforcement agencies or investigators that include digital evidence?
    a. Yes
    b. No

    (If the Response to Question 2 is Yes, proceed to Questions 2A and 2B.)

2A. In considering the typical condition of digital evidence the attorneys in your office present at hearings or trials, in the past five years, how much additional effort has been necessary after receiving digital evidence from law enforcement before it was ready to be offered?
    a. Substantial amount of effort
    b. Moderate amount of effort
    c. Some effort
    d. Minimal effort
    e. No effort

2B. Considering the same digital evidence discussed in the previous question, please rate your confidence level in using the evidence in the form or condition in which it was initially received by your office when submitted by law enforcement, prior to any additional work that your office may perform.
    a. Highly confident
    b. Moderately confident
    c. Confident
    d. Minimally confident
    e. Not confident

3. In the past five years, have the attorneys in your office presented digital evidence in a hearing or at trial?
    a. Yes
    b. No

    (If the Response to Question 3 is Yes, proceed to Questions 3A, 3B, and 3C.)

3A. Please rate the ability of the attorneys in your office to effectively present digital evidence in a hearing or at trial.
    a. Very high
    b. High
    c. Medium
    d. Low
    e. Very low

3B. How did the attorneys in your office prepare to present this digital evidence? (select all that apply)
    a. Worked with officer/individual who submitted evidence
    b. Attended training
    c. Sought outside expert
    d. Did not conduct additional preparation beyond normal trial preparation
    e. Other _____

3C. Do you believe your office has been successful in presenting digital evidence at hearings or trial as measured by the outcome of those cases?
    a. Yes
    b. No
    c. Neutral
    d. I do not know

4. In the past five years, has your office hired an outside expert to assist you in presenting digital evidence in a hearing or trial?
    a. Yes
    b. No

    (If the Response to Question 4 is Yes, proceed to Questions 4A and 4B.)

4A. How did your office find this expert? (select all that apply)
    a. Referral from Law Enforcement
    b. Referral from the Indiana Prosecuting Attorneys Council
    c. Referral from local university or other academic source
    d. Referral from Training or Conference attended
    e. Telephone Book
    f. Internet
    g. Other _____

4B. Did your office compensate this expert for his/her assistance?
   a. Yes
   b. No

5. In the past five years, have any employees in your office attended training on the subject matter of digital investigations or cyber crime?
   a. Yes
   b. No
   c. I do not know

   (If the Response to Question 5 is Yes, proceed to Questions 5A, 5B, and 5C.)

5A. Does at lest one of your employees have a formal certification or degree related to digital evidence?
   f. Yes
   g. No
   h. I do not know

5B. In the past five years, how many employees have attended digital investigation or cyber crime training?
   a. 1
   b. 2
   c. 3
   d. 4 or greater
   e. I do not know

5C. What category of employee has attended this training? (select all that apply)
   a. Investigator
   b. Prosecuting Attorney
   c. Office Assistant
   d. Other _____

6. Please rate your perception of the ability of the effectiveness of your local law enforcement agencies at investigating crimes involving digital evidence. (excluding any involvement by Indiana State Police or Federal Agencies)
   a. Very high
   b. High
   c. Medium
   d. Low
   e. Very low
   f. Prefer not to answer

7. Please rate your perception of the ability of your local judges to understand digital evidence and its admissibility at trial.
    a. Very high
    b. High
    c. Medium
    d. Low
    e. Very low
    f. Prefer not to answer

8. Please rate your perception of the ability of juries to understand digital evidence when it is presented at trial.
    a. Very high
    b. High
    c. Medium
    d. Low
    e. Very low
    f. Prefer not to answer

9. Over the past five years, what is your perception of the rate of change of crimes that involve digital evidence?
    a. Significantly increased
    b. Increased
    c. Remained steady
    d. Decreased
    e. Significantly decreased

10. Please provide any other comments or concerns you or your office has with regard to your ability to prosecute crimes involving digital evidence.

Appendix C

Law Enforcement Comments

1. The ability to train LE Officers to manage/track/obtain digital evidence is extremely difficult. Technology is advancing at a rate that far exceeds LE to adequately investigate. We are way behind the curve. Purdue University has been a tremendous asset to our agency, but they need funding to help LE. Purdue should partner with LE agencies and train Computer Experts to work with LE Investigators.

2. Our agency has software for analyzing cell phones however this is the extent to our digital forensics. The program is very basic for obtaining the information off of the phone. We would love to hire someone with great knowledge in this area to help with with more forensic issues such as frauds etc. but we cannot find qualified candidates wanting to enter the field as a patrol officer to start.

3. We utilize the services of our state police lab for advanced digital forensics. We have a good understanding of evidence collection and storage but do have concerns about the advancement of computer science involving cloud storage and related.

4. partnering with Academia which we have done with Purdue for the past 12 years in a great resource.

5. We are a small department with a very small amount of these crimes. When the need arises, we utilize the Indiana state police resources available.

6. We've been using Cellebrite software to extract cell phone, iPad and other electronic data. We have an officer/investigator whose attended numerous schools in the private sector for electronic medium. Due to this being a rapidly changing environment we continually look to updated training and processes.

Appendix D

Prosecuting Attorneys' Comments

1. In cases where digital evidence is relevant, it is extremely time consuming to separate the relevant information from the multitude of irrelevant information.

2. Law Enforcement agencies need to realize the potential and send their own people to training instead of using other trained experts from other agencies.

3. We often do not possess the technology needed due to funding contraints [sic].

VITA

VITA

LICENSED ATTORNEY

- Indiana State Bar, October 2005
- District of Columbia Bar, November 2012

EDUCATION

Purdue University, West Lafayette, IN December 2015
Master's of Science, Information Assurance and Security

- Research Principle on "A Needs Analysis of Indiana Law Enforcement Agencies" study
- Cyber 9/12 Challenge team CERIAS member– National Cyber Policy competition
- Research Principle on "Coping Mechanisms in Password Selection" study in the INSuRE project

Valparaiso University School of Law, Valparaiso, IN May 2005
Juris Doctor

- Honors Program Award
- Study Abroad
- Member, Phi Alpha Delta

Purdue University, West Lafayette, IN December 2001
Bachelor of Science, Hospitality and Tourism Management

- Member, Alpha Chi Omega

EXPERIENCE

The Office of United States Senator Joe Donnelly

- *Intern with Defense Team*
- May 2015 – August 2015

Flory and Smith/Flory Law Firm, Sandy Law Firm

- *Private Practice, Owner/Partner/Sole Proprietor and Associate Partner*
- May 2012-August 2014, March 2008 – April 2010

Tippecanoe County Prosecutor's Office, Marion County Prosecutor's Office
- *Deputy Prosecuting Attorney*
- March 2007 – February 2008, December 2005 – November 2006

U.S. Courts, Southern District of Florida
- *U. S. Probation Officer*
- May 2010 – Oct. 2011

HONORS AND AWARDS
- Court Services performance award, U.S. Courts
- CyberCorps: Scholarship for Service, Purdue University
- Honors Program Scholarship, Valparaiso University

LEADERSHIP POSITIONS, PROFESSIONAL AFFILIATIONS, AND LICENSES
- Admitted to Practice Law in Northern and Southern District Courts of Indiana
  Oct. 2005 - Present
- Alpha Chi Omega Home Inc., Member, Board of Directors
  Oct 2012 - Present
- Alpha Tau Alpha, Alumni Group of Alpha Chi Omega
  June 2012 - Present
- American Bar Association
  Aug. 2012 - Present
- Indiana State Bar Association
  Oct. 2005 – Present
- Tippecanoe County Bar Association
  Jul. 2008 – Present
  - Chairperson of the Young Lawyers Section
    2009-2010
  - Member of Technology Committee
- Legal Aid Corporation, Member, Board of Directors
    Nov. 2012 – Apr. 2015
  - Fundraising Chairperson
    Apr. 2013 – Apr. 2015
- Federal Law Enforcement Officers' Association
  Oct. 2010 – Oct. 2011
- Federal Pretrial and Probation Officer's Association
  Jul. 2010 – Oct. 2011