



THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 11 | Number 1

Article 4

2016

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

Teri A. Cummins Flory
Purdue University

Follow this and additional works at: <https://commons.erau.edu/jdfsl>



Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Cummins Flory, Teri A. (2016) "Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies," *Journal of Digital Forensics, Security and Law*: Vol. 11 : No. 1 , Article 4.

DOI: <https://doi.org/10.15394/jdfsl.2016.1374>

Available at: <https://commons.erau.edu/jdfsl/vol11/iss1/4>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



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

Teri A. Cummins Flory
Purdue University
West Lafayette, Indiana
tf@ccdproject.org

ABSTRACT

Cyber-crime is a growing problem, but the ability of Indiana law enforcement agencies to investigate and successfully prosecute criminals for these crimes is unclear. While law enforcement agencies have been conducting these investigations for many years, the previously published needs assessments all indicated that state and local law enforcement did not have the training, tools, or staff to effectively conduct investigations with the volume or complexity included many of these cases. This study provided a current assessment of the training levels, needs, and perceptions of abilities of Indiana law enforcement agencies and prosecuting attorneys, and whether they are engaged in investigating crimes involving digital evidence. The results support the recommendation that a comprehensive resource guide, focused on Indiana, is needed, as standard operating procedures are lacking, and there is a lack of awareness of available training courses or educational materials.

Keywords: cyber forensics, computer forensics, digital evidence, cyber security, law enforcement, investigation, prosecution, training, ability

1. INTRODUCTION

Cyber-crime 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 survey¹, 79% stated they had a security incident within the past 12

months, the highest percentage ever in the annual survey (PWC et al., 2015). For effective criminal investigations of these incidents, it is necessary that law enforcement has the capability to thoroughly analyze any evidence retrieved.

The investigative capabilities of law enforcement have been reviewed previously in needs assessments and analyses conducted on issues involving digital forensics. (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, &

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

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).

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. The study found that only a small number of responding law enforcement personnel had even a basic understanding of computer forensics, and that individual organizations thought it difficult to respond to incidents because of the limited knowledge of computer forensics within law enforcement and legal personnel such as prosecuting attorneys (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).

A 2008 study conducted at West Virginia University 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 is concerning, as it appears that many digital evidence investigations are being

conducted by untrained or unqualified personnel.

The current paper discusses the past state of digital forensic 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 to analyze 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, prosecuting attorneys, judges, and juries. The surveys asked the agencies about topics including whether they 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 digital evidence related training, and the agencies' perception of their own effectiveness in investigating crimes with digital evidence. Additionally, a pilot study that was previously conducted assisted in preparing the current larger scale needs analysis. There was a low response rate to the survey, which is further analyzed in the Discussion section, but because the area of cybercrime is a growing problem that has increasingly affected the investigations and prosecutions in both large and small communities, it is important to restart this conversation with the hope that further needs assessments will follow.

The concept of digital evidence is described in many different terms throughout the previous research, including 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 discusses the results of the study. Section 5 is the Discussion section which analyzes the results, and Section 6 concludes the paper.

2. LITERATURE REVIEW

The focus of many of the original needs assessments on the investigation of crimes involving digital evidence was at a national level, and did not typically focus on one state or county. This is important to note, as funding, training, and resources, such as having personnel to apply for grants, can vary drastically across jurisdictions, leading to one state or county having a much greater ability to conduct certain types of investigations (Police Executive Research Forum [PERF], 2002). While there have been a few studies published on the abilities of agencies within states or specified jurisdictions, none of these specifically looked at Indiana law enforcement agencies. Additionally, most studies have reviewed only the law enforcement aspect of digital investigations, and very few have analyzed the issue from the perspective of prosecuting attorneys' ability to successfully prosecute crimes involving digital evidence, or reviewed the available training resources. The accessibility of training 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. A lack of understanding of the specifics of digital evidence could lead to issues with getting the evidence admitted in hearings or trials, and ultimately to the possibility of the alleged perpetrator being released from any liability for his actions.

2.1 Prevalence of Digital Crime 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 top three industries effected 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), 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' must have the ability to effectively investigate crimes involving digital evidence. 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.

Even if digital crime is impacting society, the next important question that needs answered is whether our law enforcement already has the capability to effectively investigate these cases. Stambaugh et al. (2000), who analyzed the data collected by the National Institute of Justice in a 1998 study, 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. They also noted a sense of urgency 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).

2.2 Analysis of Previous Studies

As will be further discussed in subsequent sections, there are many issues involved in the investigation of crimes involving digital evidence, including access to effective tools or software, up to date training, access to labs that may have greater resources, knowledge of how to find greater expertise if needed, or formal foundational education in this field (Hickman & Peterson, 2002; ISTS, 2002; NIJ 2004). The review of these previous studies assisted in the creation of the surveys used in the current research. Henry, Williams, and Wright (2013) at the Sans Institute conducted a survey of forensic examiners working in both private industry and government and found the following five challenging areas exist 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 recommendation of the white paper was for all forensic and legal professionals to stay current on the latest cases and practices in digital forensics (Henry et al., 2013) Most of these concerns noted are discussed herein.

2.2.1 Tools and Software

Many officers use tools or software to conduct investigations into digital evidence, and the National Institute of Justice provides access to some of these for free (NIJ, "Technology and Tools," 2016). Previous studies that have analyzed law enforcement abilities in the investigation of crimes involving digital evidence have found that tools and software available for examining networks or devices were lacking (ISTS, 2002). A study conducted

by the Institute for Security and Technology Studies (ISTS) at Dartmouth College during 2001 and 2002 found that 41% of their respondents were not satisfied with the available tools and software available to examine a compromised machine or network. 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).

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. 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.

2.2.2 Formal Education, Training, and Standards in the Field

This broad range of abilities and formal education level of digital evidence investigators may also effect the tools used and the understanding of any evidence retrieved. In the ISTS (2002) study, 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. This has led to the circumstance where some digital evidence investigators are only comfortable with utilizing point and click tools, while others regularly rely on command-line-based tools (ISTS, 2002).

Training on effective handling of digital evidence is important to ensure a timely, valid, and accurate presentation to a court (Bulbul, Yavuzcan, and Ozel, 2013). 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).

The National Institute of Justice (2004) report to Congress discussed 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).

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 conduct forensic

examinations. Officers conducting digital forensic investigations 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). 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 lack of nationally recognized education or training requirements has led to each department determining which officers are able to conduct digital evidence investigations, and determine those officers' training requirements.

2.2.3 Ability to Locate Experts

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).

2.2.4 Access to Labs, Funding, and Manpower

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 agency facilities (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, and as previously stated, do not have to meet formal certification requirements.

While it appears that most digital evidence investigations do not occur in formal labs, it is important to review the capabilities of the labs that are utilized and available. Certain investigations with a high level of technical difficulty are likely to be conducted in a more formal laboratory environment, such as those run by the State Police agencies or the Federal Bureau of Investigation. Many forensic labs have faced an increase in both the number of cases and the amount of data that needs to be analyzed (Casey et al., 2013). 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).

In addition to state and federal law enforcement labs, many universities have digital evidence labs with a greater variety of tools and investigative ability than local agencies. However, if these labs are inaccessible to those agencies because of lack of knowledge, backlogs for processing, or funding issues, the evidence in question may not be analyzed in a timely or accurate manner. In 2002, forensic laboratories that responded to a needs assessment conducted by the Department of Justice reported a backlog of 142 computer crimes related cases at that time (Hickman & Peterson, 2002). The volume of computer crimes each year has continued to grow, and this backlog in laboratories is much greater now (Casey, Katz, & Lewthwaite, 2013). The issue of the availability of funds for agencies is mixed, as the Rogers and Seigfried (2004) study found it as the least reported issue, but other studies specifically found lack of

resources to be a significant issue (ISTS, 2002; NIJ, 2004).

2.2.5 State Specific Analysis of Localized Needs

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). In this study, 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).

One important aspect that has not yet been discussed is the role 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 may 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 and the admissibility of that evidence in court.

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 funded 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 Federal or State Level Expertise

The State of Indiana established a cybercrime unit within the Indiana State Police (ISP) in 1998 (ISP, "Cybercrime & Investigative Technologies Section," para 3). This cybercrime unit assists with investigations where digital media is an "integral part of the crime" (ISP, "Cybercrime & Investigative Technologies Section," para 3). 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 (ISP, "Cybercrime & Investigative Technologies Section," para 3). The ISP also has a Crimes Against Children Unit that focuses solely on investigating crimes involving the possession and distribution of child pornography, which regularly involve digital evidence (ISP, "Cybercrime & Investigative Technologies Section," para 2).

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 (FBI, "Cyber Crime"). 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 (FBI, "Cyber Crime"). 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 (FBI, "Cyber Crime").

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, it provides technical assistance to local agencies upon request that are investigating white collar or high-tech crimes (NW3C, "What We Do," para 1).

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) (ILEA, "Basic Training," 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 (ILEA, "Basic Training," 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 (ILEA, "Basic Training"). 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 ("In-service Training," 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, one conducted by federal agencies, or by private companies. One University within the state that provides training in digital forensics is Purdue University, through their Cyber Forensics Laboratory (Purdue Polytechnic, "Cyber Forensics Lab," para 2). It is located on the West Lafayette, Indiana, campus, and provides training courses for law enforcement, the military, the private sector, and academia (Purdue Polytechnic, "Cyber Forensics Lab," para 2).

A federal training opportunity for all law enforcement, prosecuting attorneys, and judges, including those in Indiana, is at the National Computer Forensics Institute (NCFI). The NCFI, located in Hoover, Alabama, 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 (NCFI, "About," para 1 - 2). This training is provided at no cost for state and local law enforcement, judges, and prosecuting attorneys (NCFI, "About," para 7). Courses are offered on an almost weekly basis at a facility specifically designed, built, and dedicated to this training, ranging in topics from Basic Computer Evidence Recovery Training to Advanced Mobile Device Examination (NCFI, "Courses;" NCFI, "Schedule").

Training is also provided at no cost to State and local law enforcement agencies at the Federal Law Enforcement Training Center (FLETC) (FLETC, "State, Local, & Tribal," para 1). Some relevant courses offered include Computer Network Investigations Training and Digital Evidence Acquisition Specialist Training (FLETC, "Training at FLETC"). These training courses are provided throughout the year, with a master calendar posted on the agency's website (FLETC, "Training at FLETC;" FLETC, "Training Calendar"). It is not known if the training opportunities available at FLETC or the NCFI 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.

Additionally, many state and local agencies have access to the Regional Computer Forensics Laboratory (RFCL) program, which provides training and examination of digital

evidence in criminal investigations (RFCL, "About," para 1). These programs combine people from different agencies, including state, federal, and local, to seize and collect digital evidence, conduct an examination of the evidence, and testify regarding that evidence if needed (RFCL, "About," para 3). Unfortunately, Indiana is not one of the jurisdictions served by an RFCL program (RFCL, "Home").

Beyond facility based training, there have also been training materials developed on this subject that are available to law enforcement. 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 (FBI, "Cyber Crime"). 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 (FBI "Cyber Crime").

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, "What We Do," para 1). The NW3C also provides Whitepapers and publications at no cost on relevant areas of cyber-crime and digital investigations (NW3C, "What We Do," para 1).

In review, a comprehensive analysis of this literature suggests that many national studies were completed in the early part of the decade, but recently, most needs assessments 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. This 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.

3. METHODOLOGY

To ascertain the current training levels, needs, and perceptions of abilities of law enforcement and prosecutors, a total of three surveys were conducted in this study, 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. 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 were successfully collected out of the 30 agencies selected. An interesting note is that this process revealed that there are still a number of law enforcement agencies within Indiana that do not have a dedicated webpage or contact information available online. 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 was completed, for a total of five complete survey responses. The data from the pilot study is based upon those five responses.

3.2 Pilot Study Results

The five responding agencies varied in size from small, between 0 to 5 sworn officers, to large, between 101 to 150 sworn officers. The sizes of the responding agencies are noted in Table 3.1.

Table 3.1

Number of Sworn Officers per Responding Agency

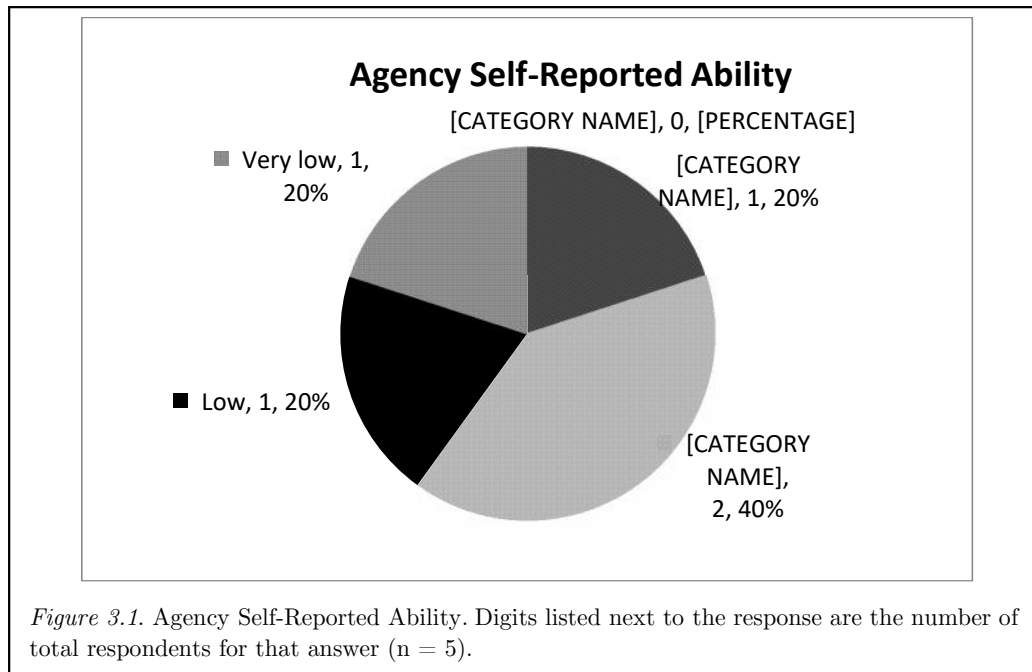
Number of Sworn Officers	Responses	Percent of Total Responses
0 – 5	1	20%
6 – 10	1	20%
11 - 20	2	40%
21 - 50	0	0%
51 – 75	0	0%
76 - 100	0	0%
101 – 150	1	20%
151 – 250	0	0%
251 +	0	0%

None of the responding agencies employed a full time digital forensics expert, and even though the response size was only 23%, this answer 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, and 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 based upon the lack of employed experts or trained employees in this subject matter.

The results of the question regarding agency perception of ability to investigate crimes with digital evidence are summarized in Figure 3.1. 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.



The results of the pilot study provided certain expectations for the full study. Indiana agencies were expected to an average level of competence in investigating with digital evidence. Further, it was obvious that certain questions were lacking, such as the number of training opportunities employees had attended, their competence in collecting and preserving digital evidence, the prevalence of prosecutions involving digital evidence, the perceptions of prosecuting attorneys, and whether it was 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 91 prosecuting attorneys' offices in Indiana. The law enforcement survey was also redesigned, to include questions on 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 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. 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), one² 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 92³ 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 were not successfully delivered; 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 was sent. Between these two messages, a total of 14 surveys were completed, for a response rate of 19%.

The same process was conducted for the prosecuting attorneys' offices, with one office not willing to provide an email address, and one office 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 were not successfully delivered, leaving the email 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 Association⁴. 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 rate⁵ for the law enforcement survey was only 9.9%.

The survey questions used in this study were based upon the information sought in

² 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.

³ The Indiana State Police were also added in to this group, so the total agencies directly contacted via email was 83.

⁴ The researcher 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.

⁵ 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.

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 deputy prosecuting attorneys. Finally, the 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.

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. The results of this question are displayed in Table 4.1.

Table 4.1
Number of Sworn Officers Employed

Number of Sworn Officers	Responses	Percent of Total Responses
0 – 5	1	4%
6 – 10	2	8%
11 - 20	6	23%
21 - 50	9	35%
51 – 75	2	8%
76 - 100	0	0%
101 – 150	4	15%
151 – 250	1	4%
251 +	1	4%

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

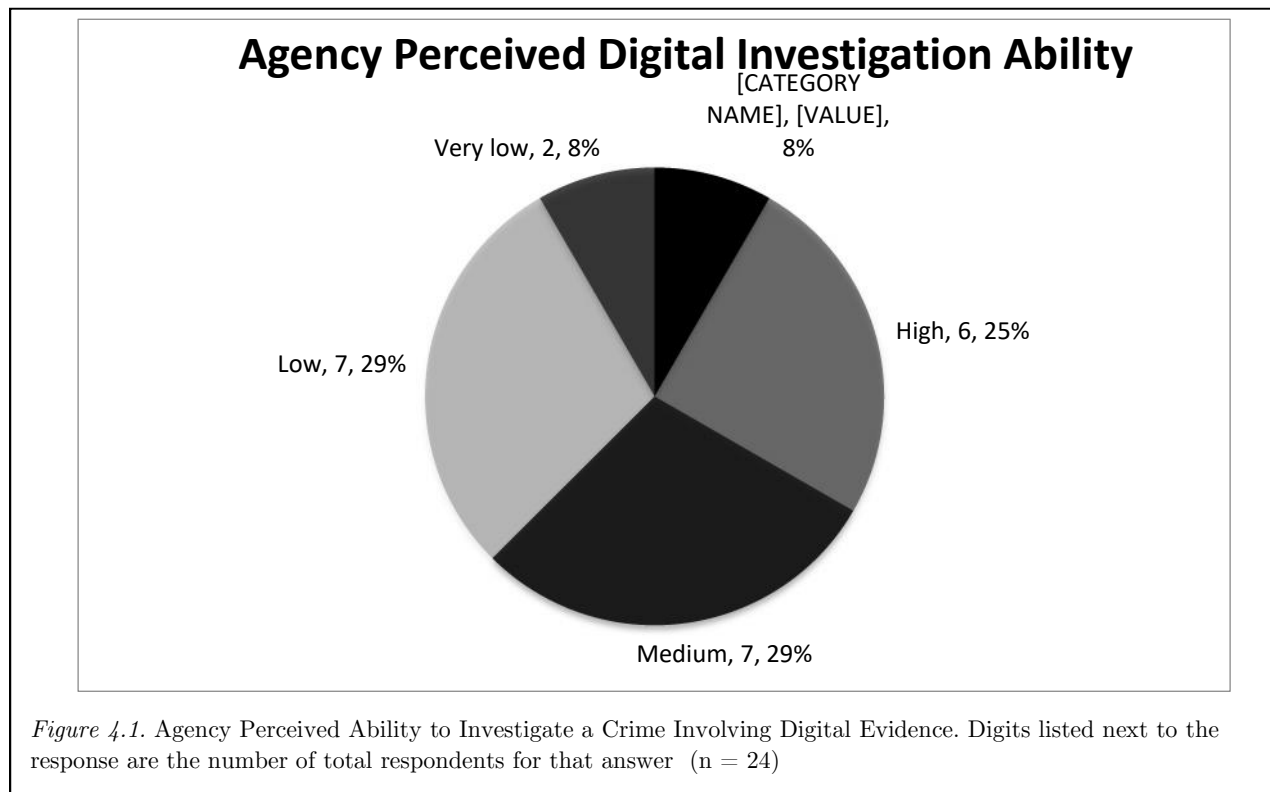
forensics expert employed, 80% responded that lack of funding was the reason. A total of 22 responding agencies have sought outside expert assistance with a digital forensics investigation over the past five years, but 20 of those 22

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.

When questioned about attendance at a 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. Additionally, in the full study, six of those 15 agencies, or 24% of the total respondents, have an employee on staff who has obtained 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 Figure 4.1, of the 24 respondents, 14 perceived their ability to be medium or low, with another two perceiving an ability of very low. In response to a question on available resources, 52% of respondents in the full study believed their office had adequate resources to effectively conduct an investigation into crimes 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.

Every one of the responding agencies in the full study 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. An additional question 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.

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.

4.1 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, as the size of an office or county may reflect the amount of resources available for training. 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. The results are displayed in Table 4.2, and should be recalled while reviewing the remaining survey responses.

Table 4.2
Sizes of Responding Prosecuting Attorney Offices

Number of Prosecuting Attorneys	Responses	Percent of Total Responses
1 - 2	2	11%
3 - 4	8	44%
5 - 10	5	28%
11 +	3	17%

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

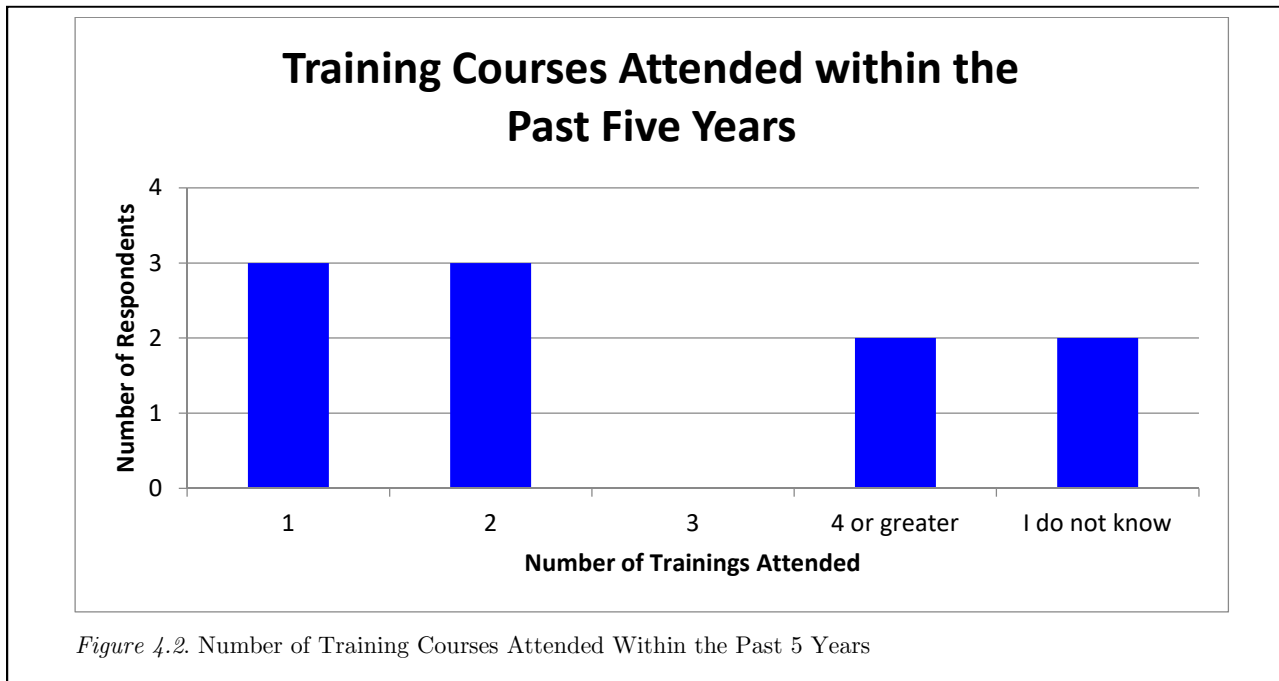
during trial in the past five years. To help prepare for that presentation of digital evidence, the attorneys typically worked with the submitting officer or investigator (73%), attended training (27%), or worked with an outside expert (27%). Certain agencies

reported no need for additional training (20%) and another 20% conducted self-research, utilized their IT department, or another attorney in the office.

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. Every one 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 Figure 4.2.



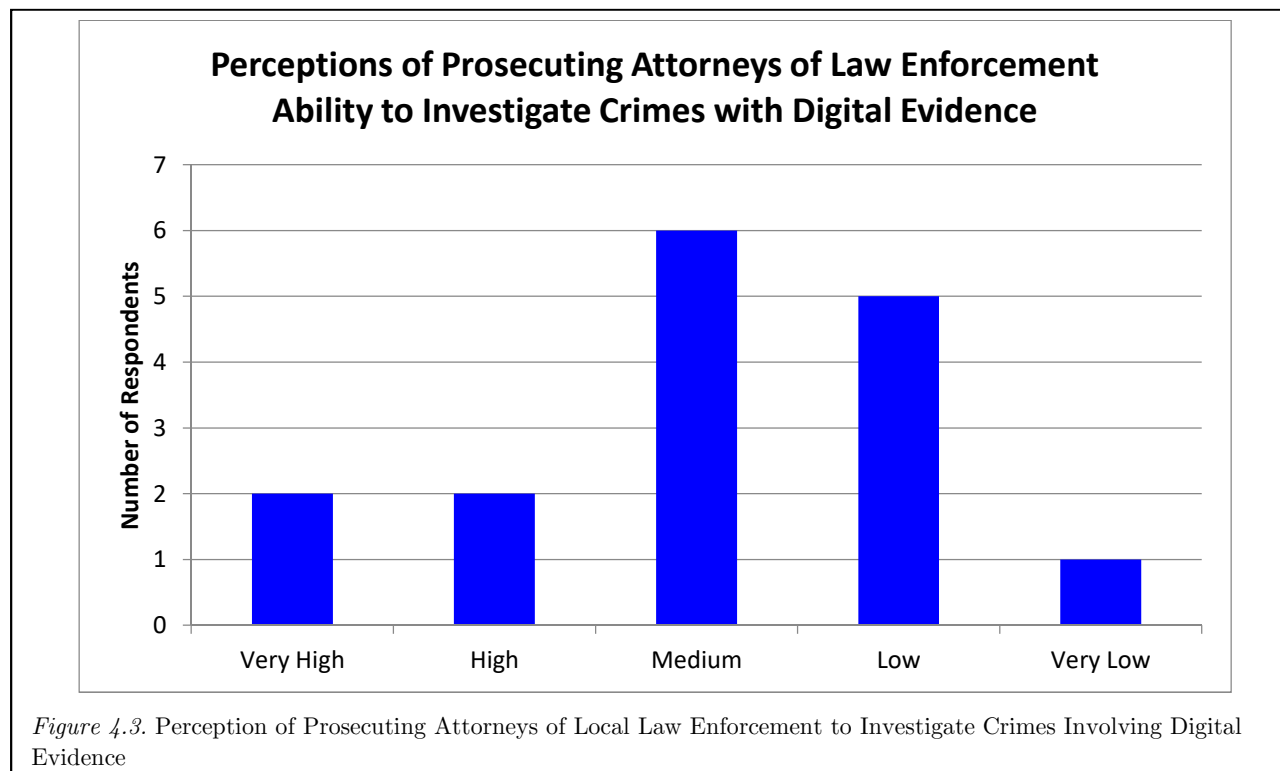
Only 20% of the offices reported having an employee with a formal degree or certification related to digital evidence, 60% responded that they do not have such an employee, and 20% responded that they do not know if such an employee is on staff. Additionally, 78% of the respondents with employees that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

courses. The respondents were asked to select "all that apply" for this question, so the total percentage reflects that some offices had both attorneys and investigators that have attended training.

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, in a separate question, 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 Figure 4.3. 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.



Interestingly, 75% of respondents believed that their judges' 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.

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 a majority of digital investigations in house. Without having a digital forensics investigator on staff, this is seemingly impossible. Responses from current digital forensics investigators in both government and private industry have 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).

To assist with analyzing the responses from the pilot study, full study, and prosecutors' office study, Table 5.1 aggregates some of the more revealing questions between all three. If the question was not asked, an N/A is placed instead in the column.

Table 5.1

Comparison of Percentage of Agencies with Digital Forensics Expert on Staff

Question	Pilot Law Enforcement	Study Law Enforcement	Prosecutor's Offices
Full time digital forensics expert on staff	0%	38%	N/A
Employee attend digital forensics training within the past 5 years (the pilot study did not have a time frame included)	40%	60%	56%
Employee on Staff with formal degree or certification	N/A	24%	20%
Perception of local law enforcement (self for LEO study) to investigate cases with digital evidence (Mean on scale of 1 – 5, with 1 being very high).	Medium-Low (3.4)	Medium (3.04)	Medium (3.06)
Perception of local judges to preside over cases involving digital evidence (Mean on scale of 1 – 5, with 1 being very high)	N/A	Medium (2.75)	Medium (3.06)
Have provided compensation to experts	N/A	9%	100%

The size of the responding agencies and offices assists in providing a better idea of the population of the responding jurisdiction. For example, the researcher previously worked in two different Indiana Prosecutors' Offices, one county with a population of approximately 45,000 and a total of four prosecuting attorneys employed, and one county with a population of approximately 185,000 and 27 prosecuting attorneys employed. Since 83% of the responding prosecuting attorneys' offices

had 10 attorneys or less, this indicates that the responding prosecuting attorneys' offices are from relatively low population counties. Further, it is important to note 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. Overall, 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 of greater capabilities is based upon the higher number of agencies with employees that have attended a digital evidence training course. Of note, only 40% of the responding agencies in the pilot study had an employee attend a digital forensic related training course, while 60% of the responding law enforcement agencies in the full study noted attendance. This again could be because of the larger average size of the responding agencies in the full study (23% employ between 11 and 20 officers) and pilot study (40% employ between 11 and 20 officers). While only 38% of the responding agencies in the full study 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 means that a total of 24% of the responding law enforcement agencies have an employee on staff with a degree or certification related to digital forensics. Therefore, a majority of the agencies have some minimal level of ability regarding investigations involving digital evidence, and almost one quarter 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, 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 40% of law enforcement agencies are 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.

Further of note is the contrast between law enforcement and prosecutors when asked about payment for hired experts. Only 9% of law enforcement agencies provided compensation to a hired expert in this field, compared to 100% of prosecutors' offices. This could be explained by law enforcement utilizing expertise from other law enforcement agencies, and prosecutors using experts for testimony from academia or industry. However, it is an interesting disparity between the two groups of respondents, and warrants further examination in future research.

Within the results from the prosecutors' offices, it is noteworthy that 56% of respondents had an employee attend digital forensics training within the past five years, but only 20% actually employ an individual with a formal degree or certification. This may lead to a more horizontal level of training in the office, with many people having a low level of knowledge or education in this field, but very few if any having a significant level of knowledge to be considered an expert.

Participating law enforcement agencies self-perceive a better than average level of capability, as 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 63% 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. The difference between the results in the 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. This is important to pursue further, as a lack of perceived ability may inhibit officers from pursuing investigations into these areas.

As to the ability of prosecuting attorneys, judges, and juries, the law enforcement agencies ranked them as follows; 54% of prosecuting attorneys' offices were deemed at least effective in introducing digital evidence, 81% of judges have at least a medium ability to understand digital evidence admissibility, and 80% of juries have 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 issues than they do of law enforcement to actually investigate them or prosecuting attorneys to present them.

While this analysis is interesting, it is not truly important unless it is actually necessary for law enforcement to have the ability to investigate crimes involving digital evidence. Both law enforcement and prosecutors 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. This large majority of agencies that noted an increase in digital evidence investigations and cases over the past five years indicates that it is important for law enforcement agencies in Indiana to have this knowledge and ability. 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.

5.1 Limitations

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 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 offices remain 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 have been present in the respondents' interest when reading the link in the email; if they are already interested in the area of digital evidence, they may have been 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 forensic 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 because of 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.

5.2 Recommendations

There are some recommendations to help meet some of the lingering concerns about agency capabilities that are secondary to the results of this study. One recommendation for both law enforcement and prosecuting attorneys is a review of whether an increase in funding and resources specifically targeted to the issues of digital evidence investigation is needed. In this study, a 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 the State Legislature to recognize this concern and ensure the necessary resources are provided 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 a 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 digital forensics training reported a lack of funding as the main reason. There seems to be a disconnect between the many

free opportunities available and the knowledge of agencies about these opportunities. An agency such as the Indiana Criminal Justice Institute, which is responsible for planning for statewide criminal justice and victim services, among other services, is perfectly aligned to be in communication with both Indiana agencies and national entities, and could create and regularly update this list (ICJI, "Home," para 1). 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, utilizing the national standards already in place in this subject matter to help ensure best practices, 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.

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. 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. It is important to understand why law enforcement has an average perception of their abilities in this

subject matter, while also analyzing why the perception of the abilities of judges and juries in this area is so high. Finally, it should be clarified how many employees have certifications, what certifications have been obtained, and how many have a formal education or degree. The answers to these questions should be determined by analyzing a much larger representative sample of the agencies within the state, with the added goal of better understanding the specific needs of the agencies that are required for them to improve their self-perceived abilities.

6. CONCLUSION

Within the State of Indiana approximately 40% of law enforcement agencies are not participating in the training that is needed to 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 have 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 both Indiana law enforcement and prosecuting attorneys are aware of the available resources, and have 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.

AUTHOR BIOGRAPHY

Teri A. Cummins Flory is an attorney, licensed to practice law in the State of Indiana and Washington D.C., having earned a Juris Doctor from the Valparaiso University School of Law. She has worked in the criminal law system as a deputy prosecuting attorney, criminal defense attorney, and a federal probation officer. Ms. Cummins Flory also earned a Master of Science from Purdue University in Information Assurance and Security, and conducted this research for her Master's Thesis. She is currently employed as an attorney in Washington D.C., and additionally works as a Research Analyst for the Cyber Conflict Documentation Project.

REFERENCES

- [1] Bhaskur, R. (2006, February). State and Local Law Enforcement is not Ready for a Cyber Katrina. *Communications from the ACM*, 49(2), 81-83.
- [2] Bossler, A., & Holt, T. (2011). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management*, 35(1), p. 165-181.
- [3] 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).
- [4] Bulbul, H. I., Yavuzcan, G. H., & Ozel, M. (2013). Digital Forensics: An Analytical Crime Scene Procedure Model (ACSPM). *Forensic Science International*, 233, 244 - 256.
- [5] Casey, E., Katz, G., & Lewthwaite, J. (2013). Honing digital forensic processes. *Digital Investigation*, 10, 138-147.
- [6] Center for Strategic and International Studies, McAfee. (2014, June). *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara, CA.
- [7] Federal Bureau of Investigation (2014). *2014 Internet Crime Report*. Washington, DC: U.S. Govt Printing Office.
- [8] FBI – Cybercrime. (2014). Retrieved on November 2, 2014 from <https://www.fbi.gov/aboutus/investigate/cyber>
- [9] FLETC – State, Local, & Tribal. (2014). Retrieved on November 2, 2014 from <https://www.fletc.gov/state-local-tribal>
- [10] FLETC – Training Calendar. (2014). Retrieved on November 2, 2014 from <https://www.fletc.gov/training-calendar>
- [11] FLETC – Training. (2014). Retrieved on November 2, 2014 from <https://www.fletc.gov/training-catalog>
- [12] 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.
- [13] 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.
- [14] Henry, P., Williams, J., & Wright, B. (2013, July). *The SANS Survey of Digital Forensics and Incident Response*. SANS Institute InfoSec Reading Room.
- [15] 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.
- [16] ICJI – Home. (2016). Retrieved on July 28, 2016 from <http://www.in.gov/cji/>
- [17] ILEA – Basic Training. (2014). Retrieved on November 2, 2014 from <https://www.in.gov/ilea/2380.htm>
- [18] ILEA - Inservice Training. (2014). Retrieved on November 2, 2014 from <http://www.in.gov/ilea/2376.htm>
- [19] Institute for Security Technology Studies (2002, June). *Law Enforcement Tools and*

- Technologies for Investigating Cyber Attacks: A National Needs Assessment.
- [20] ISP – Cybercrime & Investigative Technologies Section. (2014). Retrieved on November 2, 2014 from <http://www.in.gov/isp/3234.htm>
- [21] NCFI - About. (2014). Retrieved on November 19, 2014 from <https://www.ncfi.usss.gov/ncfi/pages/about.jsf>
- [22] NCFI – Courses. (2014). Retrieved on November 19, 2014 from <https://www.ncfi.usss.gov/ncfi/pages/courses.jsf>
- [23] NCFI – Schedule. (2014). Retrieved on November 19, 2014 from <https://www.ncfi.usss.gov/ncfi/pages/schedule.jsf>
- [24] National Institute of Justice. (2004). Status and Needs of Forensic Science Service Providers: A Report to Congress.
- [25] NIJ – Technology and Tools. (2016). Retrieved on July 28, 2016 from <http://www.nij.gov/topics/technology/pages/software-tools.aspx>
- [26] NW3C – What We Do. (2014). Retrieved on November 2, 2014 from <https://www.nw3c.org/>
- [27] Police Executive Research Forum. (2002). Police Department Budgeting: A Guide for Law Enforcement Chief Executives.
- [28] 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.
- [29] Purdue Polytechnic – Cyber Forensics Lab. (2016). Retrieved on July 27, 2016 from <https://polytechnic.purdue.edu/facilities/cyber-forensics-lab>
- [30] RCFL – About. (2016). Retrieved on July 27, 2016 from <https://www.rcfl.gov/about>
- [31] Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security*, 23, 12-16.
- [32] Stampagha, 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.
- [33] Technical Working Group for Electronic Crime Scene Investigation (TWGECSI) (2001). Electronic Crime Scene Investigation: A Guide for First Responders. National Institute of Justice, U.S. Department of Justice, Office of Justice Programs.
- [34] Verizon (2015). 2015 Data Breach Investigations Report. Verizon Enterprise. Retrieved from <http://www.verizonenterprise.com/DBIR/2015/>
- [35] Weiner-Bronner, D., (2014, April 22). Report Shows Cyber Crime is on the Rise. The Wire. Retrieved from <http://www.thewire.com/technology/2014/04/report-shows-cyber-espionage-is-on-the-rise/361024/>
- [36] West Virginia University College of Business & Economics (2008). Survey of Forensic Service Providers

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?
- Training in this subject matter area is not needed
 - Officers do not have time to attend because of other job requirements
 - No interest from officers/employees on staff
 - No funding available for this type of training
 - Other _____
5. Where do you rank your agency's ability to effectively investigate a case involving digital evidence?
- Very high
 - High
 - Medium
 - Low
 - 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.
- Extremely effective
 - Moderately effective
 - Effective
 - Somewhat effective
 - Not effective
 - 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.
- Very high
 - High
 - Medium
 - Low
 - Very low
 - 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.
- Very high
 - High
 - Medium
 - Low
 - Very low
 - Prefer not to answer
9. Do you believe your office has adequate resources to effectively conduct an investigation of a crime involving digital evidence?
- Yes
 - No
 - 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.

