Spring 2015

Digital forensics and community supervision: Making a case for field based digital forensics training

Christopher Michael 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 Christopher Michael Flory

Entitled

DIGITAL FORENSICS AND COMMUNITY SUPERVISION: MAKING A CASE FOR FIELD BASED DIGITAL FORENSICS TRAINING

For the degree of Master of Arts

Is approved by the final examining committee:

Eugene H. Spafford
Chair

Marcus K. Rogers
Co-chair

Baijian Yang
Co-chair

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 4/13/2015
Head of the Departmental Graduate Program Date

DIGITAL FORENSICS AND COMMUNITY SUPERVISION: MAKING A CASE FOR FIELD BASED DIGITAL FORENSICS TRAINING

A Thesis

Submitted to the Faculty

of

Purdue University

by

Christopher M. Flory

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Arts

May 2015

Purdue University

West Lafayette, Indiana

ACKNOWLEDGMENTS

I would like to extend gratitude to the members of my thesis committee: Dr. Eugene Spafford, Dr. Marcus Rogers, and Dr. Justin Yang for the time and effort that was given to assisting me in the completion of this work. I would also like to thank my wife for believing in me and always wanting what is best for me, no matter how much stress it causes in her life. Finally, to my loving brother, I know you would have been proud of me for this accomplishment, may you forever rest in peace.

TABLE OF CONTENTS

ABSTRACT

Flory, Christopher M. MA, Purdue University, May 2015. Digital Forensics and Community Supervision: Making a Case for Field Based Digital Forensics Training. Major Professor: Eugene Spafford.

In this paper I will review the literature concerning investigator digital forensics models and how they apply to field investigators. A brief history of community supervision and how offenders are supervised will be established. I will also cover the difference between community supervision standards and police standards concerning searches, evidence, standards of proof, and the difference between parole boards and courts. Currently, the burden for digital forensics for community supervision officers is placed on local or state law enforcement offices, with personnel trained in forensics, but may not place a high priority on outside cases. Forensic field training for community supervision officers could ease the caseloads of outside forensic specialists, and increase fiscal responsible by increasing efficiency and public safety in the field of community supervision.

CHAPTER 1: INTRODUCTION

Rationale for the Thesis

In this thesis, I intend to show the current system community supervision agencies utilize for digital forensics analysis is a risk to public safety and inefficient. Cyber-crime is on the rise and the field of digital forensics continues to expand and seep deeper and deeper into our legal and justice systems. According to the 2013 Internet Crime Report (ICR), there were over 262,800 complaints of computer related fraud in the United States totaling to over $781 million in possible damages in 2013. Digital forensic tool usage has increased in local, state, and federal law enforcement agencies as well as in the private sector digital forensic industry over the past two decades (Garfinkel, 2010).

Cyber-crimes range from malware introduction to child exploitation and offenders range in age from juveniles to geriatrics, each group with varying computer skills. A common trait amongst all cyber-offenders is they utilize digital devices, i.e. computers, smartphones, tablets, to assist in their criminal endeavors. Additionally, some cyber-offenders have another trait in common. Many may have been convicted of a crime, computer related or unrelated, sentenced to a prison term, and released onto

community supervision for a period of time, i.e. parole, probation, or community corrections (Britz, 2009). Unless a defendant is convicted of murder and sentenced to death, or life without parole, the defendant will return the community on some form of supervision.

There is a specific group of offenders whose crimes may not have involved the use of a digital device, but because of the nature of the offense and the perceived risk to the community, when released or sentenced to community supervision the use of the internet and digital devices is forbidden or severely limited as a term of community supervision. This group of offenders are those that have been convicted of sexual based offenses. Sexual offenses in Indiana include, but are not limited to, child molestation, child seduction, rape, sexual assault, possession of child pornography, and sexual misconduct with a minor. For this paper, the focus will be concentrated on convicted sex offenders, and the community supervision agents that supervise this population, in the state of Indiana who have been placed on community supervision. Community supervision agents include probation officers, parole agents, and community corrections officers.

The Indiana Department of Corrections (INDOC) releases a monthly report in which it provides statistical data on all of the inmates sentenced to INDOC including the primary and secondary charges of conviction. According to the latest available report, dated October 2014, there were 700 new offenders sentenced to INDOC for sexual related offenses in 2014. Most of these offenders will have the opportunity to be released to some form of community supervision when the mandatory part of their

sentence is completed and all of the offenders will have internet and digital device restrictions as a term of community supervision, whether that supervision is probation, parole, or community corrections.

Convicted sex offenders in the state of Indiana when released from incarceration into the community are either placed on probation, community corrections, or parole. An inmate is released to community supervision when 50% of the total *executed* sentence, the offender was sentenced to serve, is completed. The offender is released to a minimum term of one year of parole supervision and the supervision could last until the offenders total sentence time expires (Parole and Discharge of Criminal Offenders, 1979). Some violent offenders, including defendants that have been convicted of certain sex crimes in Indiana, can also be sentenced to lifetime parole. Lifetime parole is exactly as it sounds, the offender is monitored by parole services for the remainder of his/her natural born life. Offenders are also released to a term of probation supervision or community corrections as directed by the sentencing order. Probation and community corrections are used as an alternative sanction to incarceration and time spent on community supervision is in lieu of actual incarceration time (Parole and Discharge of Criminal Offenders, 1979).

As stated earlier, INDOC reported that approximately 700 offenders were admitted to INDOC facilities, convicted of sex offenses, between January 2014 and October 2014 (Offender Population Statistical Report, 2014). Most of these offenders will be released to some form of community supervision, and all that are released to supervision, will have special supervision terms that severely limit access to digital

devices and internet usage. Parole offices in Indiana currently supervise over 9400 parolees, with each agent supervising a case load of 80-100 offenders. Sex offender agents typically have smaller caseloads and supervise approximately 25-40 offenders (Parole Districts, 2015). If an offender has *ever* been convicted of a sexual offense, no matter how long ago it happened or what the current offense is, that offender will be subject to sex offender stipulations while on parole supervision (Indiana Parole Board Offender Stipulations, 2013). Probation and community corrections standards vary in this area, according to the sentencing judge's order.

As a former Indiana Parole Agent that has worked closely with many probation offices, community corrections offices, and parole districts around the state, I can accurately state that there is not a single parole agent, probation officer, or community corrections officer that is trained in digital forensics. All 10 parole districts, 96 county probation offices, and 88 participating community corrections offices rely on either state or local police agencies for their digital forensic needs. Quite simply, this means that if an agent needs to have an offenders computer, phone, or tablet inspected for improper use, the agent must confiscate the device and take to a police agency that has a forensics officer on staff. The issue with this policy is that police agencies have their own cases and they are not compensated for time spent inspecting supervised offenders devices. This practice can lead to weeks or months passing before the supervising agent obtains the search results from the police department.

This practice is a risk to public safety. If a parole agent, probation officer, or community corrections officer confiscates an offender's computer or phone for a

search, and the offender knows there is information, pictures, or evidence on the device that could potentially violate his/her terms of supervision, the offender could just decide to abscond from supervision. Additionally, parole, probation, and community corrections officers in the state of Indiana do not receive formal evidence training. Probation officers need only take a test to be certified as there is no Indiana probation officer academy (Probation Administration, 1979). Most of the rules, regulations, and procedures utilized by probation officers are learned through on the job training. Parole agents attend INDOC Parole Academy, but there is not an evidence section to the three week training session (Correctional Training Institute, 2015). There is no formal academy for community corrections and officers are trained on the job, by current officers. The lack of evidence training alone could lead to police agencies either refusing to process offender's equipment or tainted evidence if a new crime is discovered being perpetrated by the offender.

CHAPTER II: DISCUSSION

History of Computer and Cyber Crime

We must first begin any discussion involving cybercrime with a definition of what exactly is cybercrime. According to Britz (2009), *cybercrime* is a term that is used to describe any criminal activity that is perpetrated through or facilitated by the internet. This definition contains an extremely important point, to be a cybercrime, the crime must involve the internet in one way or another. But before we delve too deep into what exactly cybercrime involves, let us take a look at a few other important terms. First is the definition of *Crime.* Crime is any activity or conduct that has been deemed unacceptable by society because of the ability to disrupt order (Brenner, 2010). Second is *Computer related Crime.* Computer related crime, is any crime that involves the use of a computer peripherally, meaning that a computer was used but may not have been the main medium to carry out the criminal act (Britz, 2009). Lastly, is *computer crime.* Computer Crime is generally defined as any crime that is committed using a computer or digital device as the main medium to carry out the crime. Computer crime may or may not involve the use of the internet but does include theft, counterfeiting, and child pornography, just to name a few (Britz, 2009). These definitions are broad, but

breadth is needed in an area that can change technologically in weeks or months. Now that a few important definitions are defined, computer crime can be discussed in more detail.

The origins of computer crime may date back to the invention of the computer in the 1940's, but the true computer crime did not begin until the advent of the mainframe in the 1950's. There was no internet and no interconnecting of different mainframes at this early stage of development. The mainframes were large computers and had to be housed in large rooms with lots of air conditioning, as the mainframes would heat up quickly and heat could destroy the million dollar machines. These mainframes were owned by businesses and only a select number of people had access. The mainframes worked by using a set of punch cards. A customer would provide the owner of the mainframe with a set of data and an operator would then use a punch card machine to make the appropriate punch cards for the computer to read. After the punch cards were produced another operator would then feed the cards into the mainframe and spit out the results (Brenner, 2010). This complex system with limited amount of access meant that typically insiders were the only persons with the knowledge, ability, and access to commit computer crime. Most of the crimes committed during this time were fraud or embezzlement (Britz, 2009).

One such case happened in the 1960's. Val Smith, an accountant in a small town, owned a UNIVAC system and utilized the computing capabilities of the mainframe to provide customers with computing services. After many years of providing computing services to his customers, Smith began to feel like his time and efforts were not being

rewarded by his customers in an appropriate financial way. So Smith decided to use his mainframe to bilk his customers out of millions of dollars. This was an easy crime for Smith to commit, as it was believed at the time any numbers that came from a computer were infallible. After stealing the desired amount of money, Smith made an error that he knew would be caught believing that he would only be sentenced to 18 months in jail, however, the judge imposed a sentence of 10 years. Smith was paroled after 5 years and never had to work again, thanks to one million dollars. All of which was tax free (Brenner, 2010). There are too many of these cases to list in this paper, but I wanted to give an idea of what a fraud or embezzlement case involved.

As technology involving computers began to increase, at a breakneck pace, the availability of computing devices became more affordable. This meant that more and more businesses were able to purchase and use computers in their day to day operations, and more and more people had access to, and knowledge of, computing devices. By the 1980's, the advent of the micro-processor made computers smaller and individuals were able to own personal computers and use them in their homes. These computers were expensive and the opportunity for people to commit financial crimes increased (Britz, 2009). Literature did not provide reliable statistics on the different types of financial crimes or computer crimes before 1990 and the advent of the internet.

It was not until the advent of the internet that computer crime became cybercrime and problem that could affect anyone at any time. The internet was invented and used by the US Military as a way to link all of its radar stations together to

better defend against a Soviet nuclear attack. This work began in the 1950's and by the time that the internet was rolled out for use by the public in the 1990's, personal computers were becoming household staples (Ryan, 2010). Businesses were forming all around the internet and people began to use the internet for many of their daily needs. Individuals were using computers to keep track of finances, do their taxes, and play games. People began to keep personal data stored on computers, such as bank account numbers and social security numbers. When these personal computers were hooked up to the new medium called the internet, it did not take persons with computer knowledge long to figure out how to exploit fellow users information (Jewkes, 2009) and crimes like identity theft and bank fraud began to rise (Brenner, 2010).

Britz (2009) noted that Americans alone reported more than 200,000 complaints of online fraud. The most popular form of online fraud was online auction fraud. This type of fraud culminated in over 44% of the total fraud reported in 2009. The author also stated that Americans reported over $200 million in losses to online fraud. Other complaints that people reported being victims of were check fraud, credit/debit card fraud, computer fraud, and non-delivery of merchandise. For the duration of this paper, only crimes that involve the internet, specifically child pornography/exploitation or fraud will be examined, as these are the most likely types of offenders a parole agent is to receive on supervision who may have internet based offenses or internet usage restrictions.

By 2010, the personal computer had overtaken the large mainframe computers in sales (Ryan, 2010). A large part of this was because of the roll out and expansion of

the internet as a medium that could be accessed anywhere by anyone. It took the internet just three years to reach 50 million users. To put this in perspective, it took television 15 years to reach that milestone (Jewkes, 2009). By 2009, North America alone had 74.4 percent of its population plugged into the internet, according to Jewkes (2009). With the explosion of the internet medium, its global reach, and ease of use, computer users became perfect targets for cyber-criminals. Much of this was attributed to the newness of the technology and no real security implementations existed at this time. Unfortunately, the technological advancement of personal computers and the internet also opened up a new market to an old trade, child pornography and exploitation.

Child exploitation has been around for centuries. It is common knowledge in academia that Roman soldiers and leaders kept pubescent boys as slaves and often used the children as sexual partners to satisfy lustful desires while traveling across the empire (Lascaratos & Poulakou-Rebelakou, 2000). Up until the early 20th Century, in the United States, it was perfectly normal for a 13 or 14 year old girl to be married off to an older male, so they could birth children as a source of labor for farms. Child exploitation in these times were limited to particular situations and places. The abuse took place in the home, at religious institutions, school, or a community members home (Ferraro, 2005). However, with the advent of the camera in the mid-19th Century, it became possible for persons to obtain pornographic images and view them repeatedly in the privacy of their own homes. As decades passed, people who had desires or urges and found pleasure through the participation and/or viewing of child pornography, were literally set free

from the restraints of having to go out to find and groom victims to satisfy their illicit desires. Things relatively remained the same for the next 150 years or so. The internet changed all of that, linking people all over the world with the strokes of a few keys on a computer. People located in different parts of the world were able to communicate and share common beliefs and practices in seconds (Ferraro, 2005). This literally was a child pornography lover's dream and they made sure full advantage was taken of this opportunity.

According to a US Department of Justice website (2014), 1 in 25 youth internet users received an aggressive online solicitation, where the perpetrator attempted to set up a face to face meeting. Another statistic shows that up to 9% of all youth internet users are exposed to graphic sexual material online. In 27% of cases where solicitors contacted youths on line, the solicitors asked for sexual photographs of the youth. And in a study (Wolak, Finkelhor, & Mitchell, 2004 and Mitchell, 2004) titled "*Internet Initiated Sex Crimes Against Minors: Implications for Prevention Based on Findings from a National Study"*, of 129 child victims identified, 67% were between the ages of 12-15 and the first encounter was in an internet chat room for 76%. 74% of the victims ended up having face to face meetings with the solicitor, and 93% of those meetings ended up in a sexual encounter. The National Center for Missing and Exploited Children claim on their website to have scanned over 90 million images of possible child victims since 2000. Specific details about crimes involving child pornography or exploitation will not be examined because of the graphic content involved in many of these cases.

History of Digital Forensics

Digital forensics is the *science* of collecting, maintaining, and recording evidence from digital devices. These devices may include, but is not limited to, computers, mobile phones, cameras, and storage devices (ISFS, 2004). The science of digital forensics is built around the idea that any information obtained from the digital device must be preserved in a manner that protects the integrity and accuracy of the digital evidence collected so that it may be used in a legal proceedings. The process needs to follow recognized procedures, which have been upheld in court proceedings, to ensure admissibility in a court of law. However, it is important to remember that there are many different digital forensics organizations, and each one has its own set of standards and procedures (Leong, 2006), but each organizations procedures should contain some commonality to ensure that they are admissible in court proceedings. In this paper I will be using the Scientific Working Group on Digital Evidence Standards as a model for standards and procedures for collecting digital evidence, as this is a widely accepted model and has been used in court proceedings across the United States.

In 2004, the Scientific Working Group for Digital Evidence (SWGDE, 2004), consisting of experts from the field of digital forensics, published a procedural manual for the collection and maintenance of digital evidence from digital devices. The manual covers everything from first on scene triage to report writing and is quite long. For this reason, I will discuss some of the more important steps the committee laid out in its report.

Powered On Systems

1. The examiner should first check the system for any running processes. Do not turn the computer off as it could damage the system or data.
2. Try to capture any data that is easily and readily available.
3. Make sure to document any other machines that may be connected to the network.
4. The examiner should isolate the device from any network it may be connected to.
5. Power off the machine if necessary for transport.

Powered Off Systems

1. Do not turn the computer on.
2. Disconnect the device from any network activity.
3. Power on the computer and capture evidence to a trusted media.

Evidence Packaging

1. Every piece of equipment should be labeled and secured for proper chain of custody.
2. All equipment should be handled with care as damage may occur during transport.

Equipment Preparation

1. All examiner equipment should be examined for proper working condition and documented.
2. Hardware and software need to be configured properly to maintain integrity.
3. Digital forensic tools must be validated prior to use.

Forensics Process

1. All digital forensics examiners should be properly trained in the field of digital forensics.
2. All physical evidence should be inspected for proper working condition and documented.
3. Methods should be forensically sound and need to be verifiable.
4. All evidence should be maintained as to assure integrity.
5. All errors should be documented.
6. Hardware or software blockers should be employed to prevent examiner from writing to the original source.

Forensic Examination

1. Examiners should be trained in digital forensics.
2. Examiner needs to review requestor information to determine examination processes.
3. Examiner should review legal documents/warrants.
4. Examinations should be conducted on digital copies, not the originals, if possible.
5. Examination should always follow appropriate standards and departmental policies.

Documentation and Chain of Custody

1. All processes and steps should be documented properly.
2. Chain of evidence should always be ensured.

Report of Findings

1. Report should be written in a non-technical form and easily understandable for non-technical persons.
2. Examiner should be able to explain his processes and findings.
3. Report should include all relevant information and address the requestor's needs.
4. Report should be fact based and non-biased.

The processes outlined above are neither complete nor exhaustive and have been paraphrased. The goal here was to provide a representation of some of the standards and processes that digital forensic examiners take to ensure that court cases are not dismissed due to examiner error while conducting a digital forensic examination.

History of Community Supervision

History of Probation and Community Corrections

Probation and community corrections are just two of the many types of intermediate sanctions that make the field of community supervision. Both probation and community corrections are sentences that are imposed upon a defendant in a criminal case, and both sanctions are in lieu of physical incarceration. That is to say, the judge must include in the sentencing order that probation and/or community corrections are ordered upon the defendant and that all/or part of the incarceration sentence will be suspended and the defendant is to serve the suspended sentence on probation and/or community corrections. It is important to note that to be placed on either probation or community corrections, the defendant's sentencing order must contain some incarceration time, as these sanctions are an intermediate sanction and are in lieu of actual prison time. Probation offices are state or county run entities and the probation officers employed in the local office, report directly to the judges in their local courts on the compliance of offender their supervision.

Up to mid-19th century, the prison system in the United States focused on the idea that persons that commit offenses against the public should be imprisoned as a form of retribution, or punishment (Scott, 1998). Prisons were not places that were thought of to be nice, comfortable, and clean. Prisons were horrible, unsanitary, dark,

and damp places where inmates were mentally tortured and beaten regularly for minor infractions of the rules. Many prisons were run on the principal that solitary confinement and hard labor were the ways to cleanse the soul of evil and talking was rarely permitted between inmates (Scott, 1998).

According to Morris (1999), the age of enlightenment in the late 18th century to the early 19th century, was the beginning of a turning point in the prison reformatory movement. Philosophers and idealists, such as Beccaria and Bentham, began to question the penal system and its role in the criminal justice system and wrote continuously on the topic for many years. This idea of reformation of the prison system, gave birth to the idea of reformation of the inmate as well (Morris, 1999). In 1841, a cobbler in Massachusetts began a quest with just that goal in mind.

John Augustus, was a 57 year old Boston boot maker, who believed that the prison system in the United States was too harsh on certain types of offenders. Augustus believed that a just sentence for a convicted offender should take in to consideration the person behind the crime, not just the criminal act (Lindner, 2007). When a criminal defendant was found guilty of petty crimes and was sentenced to incarceration, Augustus would plead with the court to allow himself to “bail out” the offender from jail or prison and in return that offender would work for Augustus in his boot making shop. In return, Augustus promised the court that the offender would be on good behavior and not commit any more crimes. If the offender did not follow the conditions of his bail, he/she would be placed back in jail and Augustus would lose his bail money. It was this work that guided Augustus in the rehabilitation of criminal

offenders and earned him the nomenclature, “Father of Probation” (Champion, 2002; Lindner, 2007). Today, over 3.94 million individuals are being supervised by probation and community corrections departments in the United States (Maruschak & Parks, 2012).

History of Parole

Parole services is similar to probation supervision, in that convicted offenders are released into the community, but only after the offender has spent a part of the sentence imposed by the judge in prison. According to Maruschak & Parks (2012), the definition of parole is a period of supervised release into the community, under specific conditions and guidelines. The parolee’s sentence must be executed fully, served to the amount of time state statute requires, and released to custody of the parole department. The structure and conditions of probation, community corrections, and parole will be examined later in this paper.

Again, much like in the early stages of probation services, parole services also has a “father of parole”, and his name was Alexander Maconochie. Maconochie was an Englishman and a lieutenant in the Royal Navy. After a long and distinguished career in the military, Maconochie was offered a post as the Lieutenant Governor of Tasmania around 1845, a British penal island off the southeast coast of Australia. It was a custom of the British to transport convicted criminals, and those members of society deemed to

be unfit for civilized life, too far away colonies for prison sentences. Two of the most famous penal colony destinations were the United States and Australia (Ekirch, 1985).

After a short time on the island, Maconochie became appalled with the system of discipline being used to keep control of the prisoners on the island (Barry, 1956). Prisoners were often beaten, worked to the point of death, and barely given enough sustenance to survive the hard daily life of a British prisoner. Maconochie curbed the beatings of prisoners and started a program of rewards for good behavior by prisoners. The system of "marks" that was introduced by Maconochie recorded the infractions by inmates and also rewarded the inmates for good behavior and task completions. Marks could then be traded in for extra privileges and rations. This idea completely separated the punishment phase from the rehabilitation phase of an inmate's sentence (Moore, 2001). However, the most important reformation legacy that Maconochie would leave for the prison system was the use of "tickets of leave" (Barry, 1956; Moore, 2001).

Tickets of leave was a practice that had been around in theory in the English penal system for decades before Maconochie took control of Birmingham Prison around 1850. The practice was more commonly used with prisoners of a higher status and was rarely a privilege given to the common prisoner (White, 1976). Tickets of leave could be purchased, with marks earned by the inmate, and would allow the inmate a specific amount of time outside the prison walls to roam free and conduct business as a free man. When the specific time had elapsed, the inmate was expected to return to the prison. The ticket of leave was rewarded for good behavior and could be revoked for poor behavior and the inmate would be returned to the penal colony if personal

conduct became an issue (Moore, 2001). In present day, prisoners can be granted parole, or release from incarceration, for a period of time and if the parolee's conduct is not of a high standard, then the parole can be revoked and the parolee returned to the prison to finish his/her sentence. Parole is based on the idea of *tickets of leave* and Maconochie, while he did not invent the idea, is credited for its use with common prisoners (White, 1976). Now that a basic understanding of the history of the three main forms of community supervision has been laid out, let us discuss the inner workings and how they differ from law enforcement in the area of search and seizure.

How Community Supervision Works

According to Dressler (1959) & Champion (2005), probation, parole, and community corrections are sanctions that are imposed upon individuals convicted of misdemeanor and felony offenses by a court of law. Probation and community corrections are alterative sanctions to incarceration, that are imposed by the sentencing judge and the court retains authority over the offender while the sentence is being served by the offender. Parole is a form of supervised release once a portion (mandated by state or federal law) of the original sentence has been served (Champion, 2005). An important item to remember is that for a convicted individual to be released onto parole supervision, the sentencing judge must have imposed a sentence and fully executed the sentence (no time suspension). This is an important fact, because with

fully executed sentences, the sentencing judge relinquishes any supervision or control over the cases and the parole board becomes fully responsible for overseeing offenders after release from incarceration and during parole supervision.

When an offender is placed on community supervision, whether probation, parole, or community corrections, the offender is being supervised by an officer of the court or Department of Corrections. The offender is expected to maintain good behavior during his/her release and the officer is in place to make sure that the offender is abiding by the terms of supervision. Terms of supervision are mandated directives that the court or parole board order the offender to abide by during the supervision period. Typically there are between 12-20 standard terms that all imposed on all offenders, such as:

1. Obey all local, state, and federal laws.
2. You will be subject to random urinalysis testing for the duration of your supervision term.
3. You waive your right to 4th Amendment search and seizure protections.
4. You must report to your probation/parole officer when ordered.

The above list is in no way exhaustive, but are examples of supervision conditions found in probation, community corrections, and parole offender stipulations ("Indiana Parole Board Offender Stipulations," 2013 & "Noble Counry Order of Probation", 2015). While jurisdictions may differ slightly on the order of stipulations, many of the conditions are consistent throughout the state of Indiana. The stipulation that is most important for this paper is the stipulation *waiving the right of 4th amendment search and seizure*

protections for any person on community supervision and the special stipulations imposed on offenders convicted of certain crimes like sex offenses.

Special conditions are a list additional stipulations that are imposed upon offenders that are convicted of particular crimes, such as sex offenses and computer crimes. In Indiana, special conditions can be ordered by the judge, if the offender is placed on probation or community corrections, or the parole board, if the offender is released to parole services. A common judicially ordered special condition for offenders that have been convicted of crimes involving the use of a computer is having the offender's internet and computer usage monitored or restricted and limitations placed on the types of employment white collar offenders are able to seek (Friedrichs, 2010).

Special conditions are most imposed on one group of criminal offenders though, sex offenders. In Indiana, state statute dictates what special conditions are imposed on which probation and community corrections offenders based on the crime the offender was convicted of. For instance, In Indiana IC 35-38-2-2.1 (1989) outlines the special conditions for sex offenders sentenced to probation and community corrections based on the original sex offense conviction listed in IC 11-8-8-4. Special conditions for sex offenders released to parole supervision are set by the Indiana Parole Board, are not statutory, but mimic the special conditions set by statute for those offenders released to probation and community corrections. Special conditions for sex offenders may include limiting internet usage, registration with local law enforcement of any usernames and email addresses and social media prohibitions (Indiana Parole Board Offender Stipulations, 2013). Of all the stipulations placed on offenders being supervised in the

community, only the stipulation waving the right to 4th amendment search and seizure protections allow the supervising officer the ability to search and confiscate offender's possessions.

The 4th Amendment and Law Enforcement

According to the 4th Amendment of the United States Constitution, people have a right to be secure in their persons, papers and homes. No unreasonable searches may occur without a warrant and probable cause (United States Constitution, 2012). The state must prove to a court that probable cause exists before they may execute a search on a citizen's home or person. In other words, the state must prove that the defendant has or is involved in some sort of criminal activity. However, there is an exception to this rule, it is called exigent circumstances. Exigent circumstances state, that if police believe that the suspect is trying to destroy evidence or that evidence to a crime is in danger of being destroyed the police may conduct a search and seize the evidence to prevent the destruction of said evidence. Police and the state must follow this rule or the evidence could be determined to be obtained illegally and no longer admissible in court, and this could jeopardize the case against the suspect. In Mapp v. Ohio (1961) , the US Supreme Court guaranteed that this right applied to the states, as it was originally written into the Bill of Rights, the amendment only applied to the Federal Government, and in Katz v. United States (1967), the US Supreme Court held that the 4th Amendment also applies

to a person's body as well. While the 4th Amendment applies to police and the state, parole agents have a different standard when it come to the rules of search and seizure.

The 4th Amendment and Community Supervision

For the remainder of this paper, probation, parole and community corrections will be referred to as community supervision. How offenders are supervised, the conditions offenders are subject to, and how officers perform their duties are similar. The only difference is how a violation is handled. Judges are a little more cautious when dealing with cases involving supervised offender's rights, as courts can be over ruled by higher courts on appeal. Whereas, the parole board is its own final authority. Offenders may sue for rights violations while on parole, but unlike in a criminal court where an attorney will be appointed if the offender does not have the financial means to hire an attorney, no such protection exists for parolees. Parolees must hire their own attorneys if they wish to file a law suit against the parole board, or go *pro se* (defend themselves without legal representation).

When an offender is sentenced to community supervision, the offender is agreeing to abide by a particular and well defined set of rules and standards. The offender signs a supervision release form which outlines those standards and conditions of release. As mentioned earlier in this paper, community supervised offenders have constrained rights when it comes to their supervision and waive his/her 4th Amendment

rights. In the state of Indiana, the supervising agent has the right to search offenders under the concept of reasonable suspicion. Reasonable suspicion states that a reasonable person would be inclined to believe that a person, is involved in or about to be involved in illegal activities. This is the standard and accepted practice for community supervision involving searches concerning supervised offenders.

The first case to be brought before the Unites States Supreme Court (USSC) involving search and seizure rights of a community supervised offender was Griffin v. Wisconsin (1987). In Griffin, Joseph Griffin was convicted in a Wisconsin court of resisting arrest, obstructing an officer, and disorderly conduct. Griffin was placed on probation as an alternative to incarceration and waived his 4th amendment rights as directed by probation and the sentencing judge. During the course of the offender's supervision period, it came to the attention of the probation department that Griffin might be in possession of firearms. Felons in possession of firearms is illegal in Wisconsin and a probation violation as listed in the conditions of supervision. Probation officers conducted a search of Griffin's residence on the tip provided to them and found a handgun. Griffin was found guilty of the probation violation and sentenced to incarceration. Griffin appealed the conviction to the US Supreme Court and the court ruled the search was legal and justified. The Supreme Court made its decision based on three main points:

a.) The warrantless search of the probationer's residence was reasonable as the condition requiring the search was reasonable. The state has an active interest in the probationer's supervision.

b.) Supervision of probationers is a *special need* of the state and therefore the state is not held to the same standard for 4th amendment issues as in non-probation cases.

c.) Supervision by the state is necessary to maintain probationer compliance while on supervision, probation is for rehabilitation, and the state is held responsible for probationer's actions and protection of the public (Griffin v. Wisconsin", 1987).

This same matter was taken up by the United States Supreme Court in Samson v. California (2006) for final clarification. The Court ruled that community supervised offenders waived their right to the 4th Amendment upon agreeing to early release from prison or an alternative to incarceration. The Court also stated that as parole violations are presided over by parole boards and not judges, offender's violations are "administrative" in nature and not subject to the 4th Amendment guarantee. In Lehman's terms, this means while offenders are on community supervision, most of the rules that applied to them while/if incarcerated, still apply on supervision in the community. This ruling has provided community supervision officers a wide breadth when supervising offenders in the community ("Samson v. California," 2006).

Under these two rulings, community supervision officers reserve the right to search an offender, his/her house, possessions, and any common area and in cases where the offender resides with another individual, and any digital devices the offender may have access to as well. This is an important issue if the offender resides with his

parents and the offender has access to the computer that is stationed in the living room, which is an area the defendant uses regularly, then the supervision officer has a right to search that particular device for contraband. If a multi-user computer has different login credentials for different users, the officer may only search the device using the offender's personal login information. The supervision officer does not have the authority to impede on the rights of others in the residence, who are not on community supervision, or search their personal spaces.

CHAPTER III: MAKING THE CASE: A NEED FOR BASIC DIGITAL FORENSICS TRAINING FOR COMMUNITY SUPERVISION OFFICERS

Types of Offenders on Community Supervision

Community supervision officers supervise offenders convicted of many different types of crimes. However, this paper will be focusing on two specific types of offenders where a need for digital forensics could help monitor the offenders and increase public safety. They are sex offenders and offenders whose crimes involved the use of a digital device or computer in the commission of their specific offense.

First, let us examine offenders convicted of sex offenses. Sex offenses can consist of many different types of criminal acts. Among those charges are Child Pornography, Child Exploitation, Rape, Child Molestation, Child Solicitation, Solicitation of a Minor, Sexual Misconduct with a Minor, Trafficking in Child Pornography, Incest, and Indecent Exposure. All of the above offenses would be considered felony offenses, with a small exception in some cases involving Sexual Misconduct with a Minor and Indecent Exposure, in which the case could be a misdemeanor depending on the age of the victim. If an offender has been convicted of any of the afore mentioned charged and the offender's sentence is executed, meaning no time has been suspended from the

sentence; the offender will be released to parole when the offender has reached completion of 50% of his/her sentence under Indiana law.

Upon release from incarceration or the sentencing court, offenders have to sign a release agreement to abide by a set of stipulations during community supervision. There are many stipulations that every offender must agree to be placed on community supervision, including the waiver of 4th Amendment rights. Offenders do not have the option to not sign the stipulations and a refusal to sign the stipulations is viewed as a violation and the offender will be returned to prison. Sex offenders have an approximate additional 25 stipulations that are imposed as well. Among these stipulations is the prohibition or limitation concerning the use of computers, digital devices, and the internet. The two stipulations from the Indiana Parole Board read as follows:

> a.) You shall not use any computer or electronic communication device with an internet connection with access to any online computer service at any location, including place of employment, without the prior approval of your parole agent. This includes internet service providers, bulletin board systems, email services, or any other public or private computer networks ("Indiana Parole Board Offender Stipulations," 2013).
>
> b.) You shall allow your parole agent and/or computer service representative to conduct periodic unannounced examinations of your computer(s) equipment which may include retrieval and copying of all files from your computer and any internal or external peripherals to ensure compliance with your stipulations. This

> may require removal of such equipment for the purpose of conducting a more thorough inspection. Parole agent may have installed on your computer, at your own expense, any hardware or software systems to monitor your computer usage ("Indiana Parole Board Offender Stipulations," 2013).

Additional stipulations state that offenders are not to have any contact with any person under the age of 18, unless approved by the supervising officer. Possession of obscene material is not allowed under any circumstances along with any depictions of persons under the age of 18 in provocative or any other manner that the offender could use to satisfy prohibited desires. This includes magazines and catalogs with children's fashions and other paraphernalia. No contact with the victim is ever permissible. Lastly, sex offenders have the prohibition of using his/her employment for obtaining new victims ("Indiana Parole Board Offender Stipulations", 2013; IC 35-38-2-2.1, 1989).

In addition to convicted sex offenders, persons that have been convicted of certain white collar crimes have some of the above stipulations imposed as well. Those offenders that have been convicted of Computer Fraud, Extortion, Money Laundering, and Computer Hacking are subject to the stipulations regarding internet usage and restrictions, non-victim contact, and using employment to gain new victims. Due to the nature of the crimes listed above and the direct use of a computer or digital device in the commission of the crimes, the Indiana Parole Board or sentencing judge may find it necessary to impose these additional stipulations to better protect the public and reduce the chance that an offender is tempted to re-offend with a similar offense.

The Indiana Parole Board and legislature has found it in the best interests of the communities the offenders are released back into, to impose these stipulations upon community supervised offenders. Unsupervised or supervised offenders can pose a great risk to the community they reside in, surrounding communities, and states due to the heinous and predatory nature of their offenses. The harm visited upon the victim/victims in these cases has been deemed by the Indiana State Legislator as both extremely serious and severely damaging, thus the strict parole supervision guidelines. The above stipulations try to regulate the areas where a convicted sex offender could use a computer or digital device to gain new victims or harass past victims ("Indiana Parole Board Offender Stipulations," 2013). Next, we examine the current procedure that community supervision officer's use when digital forensics are needed on an offender's computer or digital device.

Community Supervision Officers and the Digital Forensics Process

First, an examination and some background on how parole boards and violations work is necessary. In cases where the supervising officer feels that there has been a violation or is about to be a violation by the offender, the supervising officer submits a formal violation report to the Indiana Parole Board or sentencing judge and requests formal action. The actions requested can range from imposing intermediate sanctions, such as GPS monitoring or increased reporting instructions to incarceration. If the

supervising officer becomes aware that the offender poses an immediate risk to the community or has violated the supervised release agreement by committing a new offense, the supervising officer can call the parole board or sentencing judge directly and request an emergency warrant. This process could take between 10 minutes to one hour and the supervising officer is told over the phone if the circumstances justify an emergency warrant. It is important to note that parole agents and law enforcement officers have the authority to make warrantless arrests if a new crime is uncovered. If the parole board or sentencing judge agrees to issue the warrant, the supervising officer takes the offender in to custody and the signed warrant is faxed to the local jail and the offender is transported to the facility by the supervising officer or local law enforcement. There is no waiting for the warrant and no chance the offender absconds as the offender is never out of the supervising officer's sight. The Indiana Parole Board has full authority to issue warrants for parolees and the parole agents and community corrections officers have full arrest powers over offenders in their care (IC 11-13-3-3, 1979). Probation officers have full arrest powers over probationers (IC 11-13-1-1, 1979), however, judges overseeing the cases rarely allow the probation officers in their jurisdiction the authority to make arrests and local law enforcement are called in for the actual arrest.

For the remainder of this paper the author will be relying on eight plus years of training and experience as a probation and parole agent, two of which was with the Indiana Department of Corrections, Parole Services Division. There are no written standards or procedures in place within the Indiana Department of Corrections or

Indiana State Judiciary, in regards to probation officers, relating to the inspection or seizure of computers for digital forensics examinations. Indiana Parole Services does not utilize any form of evidence bags or labels and the agents are not trained in collection of evidence techniques and standards. If an agent seizes any property from a defendant, the defendant is asked to sign a form that states what the property being seized is, the date and time and the officer's signature. The form that is given to the offender has nothing to do with the integrity of the potential evidence taken or the chain of custody of said evidence, it is simply a form provided to the offender in case the property is lost or damaged by the agent.

Confiscated or seized property is taken to the parole agent's office and is locked in a file cabinet until it is to be returned to the offender. This process has a large flaw. In many cases the parole agent lives and works several hours from his/her district office and may only travel to the district office once a week. Parole districts are large and may encompass ten or more counties. In the case of Indiana Parole District 4B, the district office is located in Terre Haute, IN which is located in the southern most county in the district. Three parole agents, including myself, lived and worked in the six northern most counties in that district. This placed the agents a three hour drive from the district office. It is not reasonable nor efficient to have those agents drive to the office every time there is a confiscation issue. This means that the agent is forced to either take the property home with him/her or lock it in the trunk of the vehicle until the next trip to the district office. Either one of these choices could result in potential damage to the

property or exclusion from a court of law, as a judge would not allow evidence into a court proceeding that was kept at the agent's home for a week.

If the agent needs to have digital forensics performed on the confiscated electronic equipment, the property must be taken to a local police department that has personnel trained in digital forensics. There are many issues with this procedure. First, the agent has taken no steps to preserve any evidence that may be found on the confiscated equipment that could potentially lead to new charges being filed. Second, as stated above, the agent is not provided with the proper training and equipment to maintain a legal chain of custody when the property is given to local law enforcement for forensics testing. This may cause the police agency to deny the agent of their services as they do not want to be liable for any damage to the offender's property. Lastly, if evidence of a new crime is uncovered by the forensic examiner, they may not be able to use the evidence in a court of law as proper chain of custody was not observed, or the evidence was stored in the agent's home for several days before being turned over for examination. Chain of custody involves the proper recording of evidence and records of who is control of the evidence at all times.

With all the issues discussed in the above paragraphs concerning the proper handling and storage of confiscated property and potential evidence, there is one more issue that arises from the method currently utilized by parole agents in Indiana. That is the issue of time. When a parole agent has deemed it necessary to confiscate an offenders electronic devices and turn the property over to qualified forensic specialists for examination, time is extremely important. Once the confiscated property is in the

possession of the forensics specialist, the examination process could take weeks or even months to complete. Chances are that the officer or specialist has other cases that need to be completed involving their department and the local prosecutor's office. These cases will always come first for the examiner. The examiners are not compensated in any way for the analysis that is performed on devices turned over by parole agents and while department heads may not mind their employees helping out another agency with the forensics process, they usually expect the department's cases to take priority. In many cases this leads to a long delay in getting the results to the parole agents.

The problem with the aforementioned process and time issue, is that while the process is being played out between the parole agent and the forensic examiner, the parolee remains in the community. The parole agent has no grounds for a violation or arrest warrant until it is proven that there has been a disregard by the offender concerning his/her stipulations. If the parolee is engaging in illegal activity or using a digital device in a manner that violates the stipulations of supervision, the parolee may decide to abscond, meaning he/she may leave the state or area and the agent may not be able to locate the offender. The offender cannot be supervised if the agent is unable to meet with the offender. Another issue that arises from the time stand point, is that the offender may be in the cycle of offense. In the case of a sexual predator, if the offender has been looking at child pornography, this behavior could lead the offender to re-offend with another victim, as the behavior may trigger a desire to act on urges that they have been trying to avoid through supervision and treatment. The fear of being caught may lead the offender to re-offend as they will likely be going back to prison if

any violations are found by the examiner. The above scenarios place the greater public at risk for further victimization by violent predators.

As mentioned in a previous section, the Indiana Parole Board has complete authority over offenders released to parole supervision. If the offender has violated the stipulations of supervision, the parole board can issue a warrant, conduct a violation hearing, and return the offender to prison or continue them on parole supervision. A basic digital forensics training program for parole agents would allow the agents to conduct a preliminary examination of the offender's digital devices and take the appropriate actions based on those findings. This could greatly reduce the wait time between contact with the offender, confiscation of property, examination of the devices, returned results to the parole agent, and warrant request/apprehension. This process currently employed by parole services could take days, weeks, or even months. This delay could place the community at greater risk of being victimized and does not hold the offender accountable for prohibited behavior and violations in a timely manner. None of which is a good supervision strategy and a change needs to be made.

CHAPTER IV: RECOMMENDATIONS

While the current system for confiscation and forensic analysis in community supervision is ineffective and time consuming, there is hope that the system can be changed and improved upon. There are several programs that are utilized by prosecutors and law enforcement to assist agencies with training needs in the area of digital forensics. However, the nature of the violation process and waiver of 4th amendment rights by community supervised offenders dictates that a comprehensive program to train agents as digital forensic experts is not necessary. Supervision agents need a basic digital forensics training program that can assist them while conducting home visits in the field to locate contraband.

The biggest hurdle that will be faced in implementing any program that involves training and equipment, is always going to be funding. Indiana Parole Services is a faction of the Indiana Department of Corrections and typically has a small budget. Most of the Department of Correction's budget is allocated to the costs associated with incarcerating inmates. The Indiana FY Budget for 2013-2015 allocates approximately $9 million to parole services out of a $732 million Indiana Department of Corrections budget, or roughly 1% of the total budget. Parole Services in Indiana has approximately 100 agents with an average salary of around $33,000 per year with equals $3.3 million

per year in salary costs and agents supervise over 10,000 parolees. This means that roughly $3.3 million out of a $4.5 million yearly budget is allocated for salary considerations and that leaves $1.2 million per year for all other expenses which includes fuel costs for fleet vehicles and office supplies for 10 district offices (Indiana, 2014). There is little room in the budget for new trainings and equipment. It is also important to note that under Indiana Statute, parolees may not be charged a fee of any type for services rendered by the Department of Corrections involving investigations or violation, nor can a fee be imposed to help pay for training costs and equipment needs (IC 11-13-3, 1979). Parole services are completely funded by tax payer monies. An outside source of revenue, such as grants, would almost certainly have to be utilized to assist in the funding of such a program. Local community corrections departments receive a sizeable portion of their budget from the Indiana Department of Corrections and could simply piggy-back on the training provided by INDOC.

In the case of county probation departments, the funding issue looms a bit larger. County probation departments are generally funded at the county level. This means that requests for funding, whether it be for new officer hires or training needs, goes through the local county counsel. According to the Tippecanoe County Budget for FYI 2015, the probation department's annual budget is $1.475 million. This number includes juvenile and adult probation services and all the staff and operating costs associated with the department. Each county is responsible for the budgetary needs of the probation department within its county borders and receives little assistance from outside sources to fulfill budgetary those needs. While some counties may have a larger

tax base, such as Hamilton County, IN (pop. 275,000 according to US Census information 2010), and others may have a smaller tax base, such as Warren County, IN (pop. 8, 508 according to US Census information 2010), the amount of funds that can be drawn from its citizenry for extra training can be limited and become a political hot button issue.

While this paper will not address the political meanderings of local counties, I will say that the best way to secure the funding necessary for any additional programs at the county level, would be to apply for grant monies from the state and or local government. It is easier to sell the idea of "we have this program and it will cost you nothing extra to increase public safety" than to have to ask for additional funds from already beleaguered county coffers. Additionally, I have listed several digital forensics training options below that are either free or incur a minimal cost to the community supervision jurisdiction.

The National Institute of Justice released a Digital Forensics Training Program for First responders in 2001 (NIJ, 2007), which could be adapted for use by community supervision officers. Although, not currently being utilized at the Federal level, the details of the program are available for public information and could be adapted to meet the needs of community supervision officers. The program outlines the basic elements of digital forensics, including what to look for in a potential crime scene, how to handle computers and digital devices when encountered, procedures on how to handle evidence and confiscation of electronic devices, and proper chain of evidence. This program could be used as a training for specific parole agents who supervise sex offenders and offenders convicted of electronic device crimes and training could take

place during the academy training period for all new parole agents and at yearly seminars for other supervision agents already in the field with caseloads. The NIJ training can be taught over the period of one day and could be provided to training departments at a marginal cost. However, this training is not enough. Agents will need to be trained in basic computer functionality, terminology, as well as, internet functionality and blacklist sites. State or local law enforcement agencies could provide training utilizing the NIJ, or similar format, at a low cost to departments with community supervision officers.

The Department of Computer and Information and Technology at Purdue University conducts classes entitled, Law Enforcement Training Series for Digital Evidence Triage. This program is three days in length and can be technical at times, however, there are several sections of the program that could be utilized and transformed into a program that would be appropriate for community supervision officers in Indiana. There is a section that outlines the various components of a computer with real life pictures and graphics. The Purdue University training module also includes a section on web browsing and related activities. Training the agents in how to read a URL and what to look for when trying to locate graphic images on a digital device would also be an imperative. But the most important information that could be taught to supervision officers working in the field is when to *STOP*. Supervision officers must be trained to realize they are in over their heads and knowing when to stop before any evidence that could possibly lead to a new conviction or new law violation is tampered with or altered, endangering chances of criminal conviction in a court of law.

Supervision officers must know when to call in local law enforcement and treat the area as a new crime scene and proper training can provide for this requirement.

Another training opportunity is sponsored by the federal government. The United States Secret Service operates the National Computer Forensics Institute (NCFI). NCFI is a technical teaching institute for law enforcement, prosecutors, judges, and other agency employees that provides training in the area of computer forensics. The courses taught at NCFI range from basic forensics for law enforcement to a network intrusion response program. The institute was founded in 2008, by the US Secret Service and the Alabama Office of Prosecution Services, to provide cyber training to local, state, and federal offices, which at that time was difficult training to attain. NCFI utilizes the Secret Service model of cyber investigations, which relies on the sharing of information between private industry, academia, and the law enforcement legal communities (https://www.ncfi.usss.gov/ncfi/ pages/about.jsf). With the partnership from so many different sources, the curriculum reflects the latest trends in cybercrime and more importantly the issues that plague cyber investigations (NCFI, 2014). Trainings are free of charge and NCFI even provides housing while trainees are at the facility. NCFI was recognized by the US House of Representatives, Department of Homeland Security, International Associations of Police Chiefs, and the Major County Sheriff's Association as a mission oriented training facility.

The Federal Law Enforcement Training Center (FLETC) also provides training to local, state, and federal law enforcement agencies in the areas of cybercrime and digital forensics (https://www.fletc.gov/state-local-tribal) in Glynco, GA. Courses that are

offered at FLETC range from Computer Network Investigations Training to Digital Evidence Acquisition Specialist Training to Crime Scene Evidence Training. Trainings are offered at specified times and typically are posted 6 months to a year in advance. Trainings are typically free and open to any law enforcement officer at the local, state, and federal levels. Once again housing is provided for attendees and departments should only have to incur the costs of travel for attendees. A detailed description of trainings and requirements can be found on the FLETC website (https://www.fletc.gov).

Agencies can also look to neighboring states for training oportunities in the areas of digital forensics. Many times border states work closely together on cases as nefariuos individuals in one state cross state lines into neighboring states to commit criminal acts. This seems to be more prevelant in areas where a larger city, such as Chicago shares a border with neighbor Indiana, and the metro areas run together. States that share borders may be able to offset training costs by conducting joint training exercises. Federal grants are also available to most local, state, and tribal law enforcement offices, including probation, parole, and community corrections offices, to assist financial needs for officer training. Grants can range from hundreds of dollars to thousands of dollars. Grant information can be found on the US Department of Homeland Security's webpage (http://www.dhs.gov/law-enforcement-resources).

Conclusion

With the ever increasing numbers of computer and digital device crimes on the rise around the world, the need for digital forensics experts has increased over the past several decades. Computer crime and cyber-crime is growing faster than any other form of illegal activity and will soon outpace the global drug trafficking market in total costs. With this drastic increase in cyber and computer crime comes more criminal cases and convictions. The reality is that 85% of all convicted individuals will be released back into society at some time in their lives and many of these offenders will be released to parole supervision. Currently Indiana does not have any parole agents trained in the area of digital forensics and must rely on outside agencies to conduct forensic examinations of digital devices owned and operated by offenders under supervision. Many of the offenders on parole in the State of Indiana have been convicted of crimes involving the use of computers or other digital devices or have limitations placed on the use of such devices as a term of parole, such as sex offenders and violent sexual predators.

The current system used by parole services in the State of Indiana is inefficient and time consuming. Parole agents must rely on outside sources to conduct any type of digital forensic analysis and must do so at the leisure of these sources. Parole agents in Indiana need to be trained in a basic digital forensic course to decrease the time it takes to request and get a warrant if a suspect is in violation of the terms of supervision. The training should be steered towards parole services to better assist agents in carrying out

their duties, but keep in mind the intricacies of the court system if new charges need to be filed based on evidence uncovered during routine examination of offenders electronic equipment. Funding will most certainly be needed to help offset the costs of any training and equipment needs as well. More research is needed in this area, including studies to the nature of community supervision, types, and numbers of supervised releases in each locality and the needs based qualitative study of supervision agents and resources available to each agency. Financial feasibility studies should also be completed to better ascertain the types and amounts of funding available for each of the supervising agencies.

BIBLIOGRAPHY

BIBLIOGRAPHY

Barry, J. (1956). Pioneers in Criminology: Alexander Maconochie (1787-1860). *Journal of Criminology*, L.C &P.S. 145.

Brenner, S. W. (2010). *Cybercrime criminal threats from cyberspace*. Santa Barbara, CA: Praeger.

Britz, M. (2009). *Computer forensics and cyber crime : an introduction* (2nd ed.. ed.). Upper Saddle River, N.J.: Upper Saddle River, N.J. : Pearson Prentice Hall.

Champion, D. J. (2005). Probation, Parole, and Community Corrections, 5th ed. Upper Saddle River, NJ: *Pearson Prentice Hall*.

Conditions of Probation, IN Stat. § 35-38-2-2.1 (1989).

Correctional Training Institute (2015). *Indiana Department of Corrections*. Retrieved January 23, 2015, from http://www.in.gov/idoc/3283.htm.

Dressler, David. (1959). *Practice and theory of probation and parole*. New York: Columbia University Press.

Ekirch, A. R. (1985). Bound for America: A Profile of British Convicts Transported to the Colonies, 1718-1775. *The William and Mary Quarterly: A Magazine of Early American History*, 184-200.

Federal Bureau of Investigation. (2013). *2013 Internet Crime Report*. Washington DC.

Fredrichs, D. (2010). Trusted Criminals: White Collar Crime in Contemporary Society. Wadsworth, Belmont, CA: 4th ed.

Ferraro, M. M. (2005). *Investigating child exploitation and pornography: the Internet, the law and forensic science*. Amsterdam, Boston: Elsevier Academic Press.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, S64-S73. doi: 10.1016/j.diin.2010.05.009

Indiana (2014). *2013-2015 As-Passed Budget*. Indianapolis, IN.

Indiana Parole Board Offender Stipulations. (2013). Retrieved April 20, 2014, from http://www.in.gov/idoc/2324.htm.

ISFS. (2004). Computer Forensics *Part 1: An Introduction to Computer Forensics*: ISFS.

Katz v. United States, No. 389 U.S. 347, Lexus Nexus Academic Database (United States Supreme Court 1967).

Lascaratos, J., & Poulakou-rebelakou, E. (2000). Child sexual abuse: Historical cases in the Byzantine empire (324-1453 AD). *Child Abuse Negl., 24*(8), 1085-1090.

Leong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation, 3*, 29-36. doi: 10.1016/j.diin.2006.06.004

Lindner, C. (2007). Thacher, Augustus, and Hill: The Path to Statutory Probation in the United States and England. *Federal Probation*, 71 (3), pp. 36-41.

Mapp v. Ohio, No. 367 U.S. 643, Lexus Nexus Academic Database (United States Supreme Court 1961).

Maruschak, L. M., & Parks, E. (2012). Probation and parole in the United States, 2011. Washington, DC: *US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics*.

Moore, J. (2001). Alexander Maconochie's Mark System. *Prison Service Journal*, vol. 198.

Morris, T. (1999). What's all this about punishment? *Howard League Magazine*, 17 (1), pp. 6-8.

NIJ. (2007). *Investigations Involving the Internet and Computer Networks*. (NCJ 210798). Washington, DC: Department of Justice.

Noble County, IN Order of Probation. (2015). Retrieved February 17, 2015, from www.noblecountycourts.org/ncc/OrderProbation.pdf.

Offender Population Statistical Report (2014). *IDOC Division of Research Technology October 2014*.

Parole and Discharge of Criminal Offenders, IN Stat. § 11-13-3 (1979).

Probation Administration, IN Stat. § 11-13-1 (1979).

Parole Districts. (2014). Retrieved April 20, 2014, from http://www.in.gov/idoc/2330.htm.

Ryan, J. (2010). *A history of the Internet and the digital future*. London: Reaktion Books.

Samson v. California, No. 547 U.S. 843, Lexus Nexus Academic Database (United States Supreme Court 2006).

Scott, C. (1998). *With Liberty for Some: 500 Years of Imprisonment in America*. Boston: Northeastern University Press.

SWGDE. (2004). SWGDE Best Practices for Digital Forensics.

Tippecanoe County. (2015). *2015 As Passed Budget*. Tippecanoe County, Indiana.

United States Census Bureau. (2010). US Census 2010. Retrieved February 25, 2015, from http://quickfacts.census.gov/qfd/index.html.

United States Constitution. (2012). *The Constitution of the United States: with index and the Declaration of Independence* (25th ed.). Washington, DC : U.S. G.P.O.

White, S. (1976). Criminology: Alexander Maconochie and the Development of Parole. *The Journal of Criminal Law and Criminology*, 67 (1).

Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet- initiated sex crimes against minors: implications for prevention based on findings from a national study. *The Journal of Adolescent Health: official publication of the Society for Adolescent Medicine, 35*(5).