The Bill Blackwood
Law Enforcement Management Institute of Texas

Establishing a Computer Forensic Program

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Robert A. Rosenbusch

Round Rock Police Department
Round Rock, TX
July 2015

ABSTRACT

This research project will address the ever-increasing needs for establishing a computer forensic unit within a police department and provide executives with reasonable and affordable steps to take to accomplish this goal. Many smaller law enforcement agencies avoid technology related investigations because they do not understand, or believe they do not have the resources available to train personnel and buy equipment needed to establish a computer forensics solution.

Computer related crime has no boundaries. With the advent of the Internet, every department in this country has some degree of technology crime occurring within its jurisdiction. Police departments across the nation are facing similar challenges when it comes to handling computer related data. It is incumbent upon police mangers to find ways to handle an increasing amount of technology related devices and the mass amounts of data they contain. In addition, they need to find ways to achieve this in a timely, forensically sound method using limited resources.

The complexity of technology crime and the growing problem that is associated with these types of investigations makes it a necessity for police departments to establish a computer forensic program within their organization. This will assist in obtaining evidence that is admissible in a court of law and provide a guideline for training and possible funding options from a small scalable program, which can grow with the department and demand.

TABLE OF CONTENTS

INTRODUCTION

Technology has become a growing problem for law enforcement over the past few decades. The nature of computer forensics and electronic evidence is such that it poses a significant challenge to a nontechnical police force (Tomar, Rai, & Kharb, 2014, para. 30). This is predicated on the need for digital evidence to be admissible in court. Admissibility is tied to four functions in forensic analysis which include the collection of the digital evidence, the examination of the evidence in a sterile environment, the analysis of the findings, and the reporting of the findings. The techniques used for handling digital investigations are still fairly new (only being utilized for the past 12 years), and the tools are constantly being updated and improved as technology continues to evolve. Great care has to be used when working with digital evidence: "proper forensic procedures and techniques go hand in hand with good forensic tools, the evidence may be compromised or destroyed" (Tomar, Rai, & Kharb, 2014, para. 30). In order to ensure the admissibility of digital evidence, officers must be properly trained and become more literate about cyber-crime and the techniques and tools used to address the specialty area of evidence handling and analysis.

The public is using the Internet and computers more now than ever before. In the most recent report by the National White Collar Crime Center (Huff, Desilets, & Kane, 2010), it shows that 14% of households and17% of individuals reported at least one form of victimization online. In spite of the increasing amount of information that has been collected over the past 20 years, the actual financial impact of cybercrime is still greatly unknown. One of the main contributing factors to this lack of information due to the fact there is no standardized way of reporting these types of crimes. Communities

across the nation have consistently voiced their concerns about cybercrime and the lack of enforcement that is associated with it. The future of cybercrime fighting is here and needs to be addressed. Departments spend lots of money purchasing drones, robots, tactical gear, in-car cameras, and body cameras, but most fall short of establishing a functional computer forensics program that is capable of handling these advanced cybercrimes.

Criminals have always found new ways to commit crimes and elude law enforcement. One of the trends that are seen in law enforcement today is the rapidly growing use of technology crime. Organizations around the world are struggling with finding new ways to combat this type of crime and provide a solution that will enable them to address cyber criminals. While there are many different ways to deal with this issue, none has proven to be more efficient than creating a computer forensic solution within your department. Larger agencies have established some level of computer forensics within their organizations. The vast majority of smaller agencies rely on larger departments to assist and supplement their investigations when it comes to computer forensics. With the constant demand for computer forensic analysis placed on larger agencies, it is time that every department should establish their computer forensic program. With the significant increase of technology crime, especially those offences committed against children and the elderly, law enforcement has to adopt a position of protecting those that cannot protect themselves.

The BTK Killer (blind, torture, kill) case propelled computer forensics into law enforcement in 2004 (Rosen, 2014). Dennis Rader was responsible for murdering ten people. During the course of his crime, he wrote letters to police and local news

organizations outlining the details of the crime. The electronic word document that he sent also contained “Meta Data” which identified the registered owner of Microsoft Word program used to create the document. This led police to the church where Dennis Rader was a deacon and to the computer he used to create the letters sent to the media and police (Rosen, 2014, para. 12). After years of working on the BTK investigation, investigators were finally able to solve the case when the killer converted from paper letter to an electronic document on a floppy diskette. This is a small example of how computer forensics can have a significant impact in an investigation, even a homicide.

POSITION

There are several reasons for establishing a computer forensic program within a department. Technology crime has no boundaries. Regardless of the crime in today’s world, there is usually some form of technology either associated with or present during the commission of the crime. According to the National Institute of Justice (NIJ) digital evidence is now used to prosecute all types of crime, not just e-crime (“Digital Evidence,” 2010, para. 2). This spans from simple theft to fraud, child pornography, bullying, hacking, identity theft, and even homicide. These are only a few of the more common types of crimes where technology plays a role; there are many more that can be listed, and is only limited by the imagination.

Technology will continue to grow, and criminals will find new ways to exploit these technologies to commit crimes. McQuade (2001) stated it best when he said, “crimes are more likely to be committed by motivated offenders who have suitable targets in the absence of capable guardians” (para. 3). In 2011, two youths were arrested and convicted of murdering Kimberly Proctor, who was 18 at the time. The

police followed a trail of digital evidence which uncovered “Wikipedia searches, instant messages, a confession in a World of Warcraft chat, Global Positioning Satellite (GPS) data, an alibi text message sent from the scene of the murder, and Google map searches for a place to dump the body” (Hill, 2011, para. 1). All investigators should have a basic enough understanding of computer evidence to know they should look in these areas for evidence. Investigators should also know what they are looking at once they have found it. A murder weapon is useless if the investigator does not know that it was used to commit a crime.

The technology crime rate has grown out of control. According to the Federal Bureau of Investigations, (FBI) the cyber crime rate has increased from 16,838 complaints in 2000 to 262,813 complaints in 2013 (2013 Internet Crime Report, 2014, p.3). This report also identifies the United States as being the leading country of cyber crimes reported, with Texas being third in the total number of complaints filed in the United States (“2013 Internet Crime Report,” 2014, p. 3). These figures are staggering and seem to be growing each year. This report showed that in 2013, the reported loss exceeds $781,841,611 in adjusted losses (“2013 Internet Crime Report,” 2014, p.3). One of the more disturbing facts about these figures is that it only encompasses the crimes that were reported. Just as with any theft or fraud case, the majority of cases never get reported due to the small amount of loss, or the lack of cooperation with businesses that do not want to identify as being victims.

While cybercrime can be seen in every aspect of the criminal element today, none is more prevalent than identity theft. Identity theft has become the leading form of fraud. According to The Daily Finance, identity theft victims in 2013 suffered more than

$24.7 billion in direct and indirect losses (DiGangi, 2013, para. 1). In comparison to other types of theft, that is $14 billion dollars more in loss than any other reported crime combined in the same reporting period. According to the most recent report available from the Federal Trade Commission (FTC), they state that more than 9.9 million people were victims of identity theft in the United States in 2003 (“Survey of Identity Theft,” 2003, para. 1). Without the establishment of a computer forensic program, it becomes very difficult to find the resources to investigate these types of crime.

Society is evolving every day, and technology is no different. With the constant evolution of technology, the latest technology is replaced by new technology approximately every 18 months (Moore, 2011, p. 83). There is a constant change in technology as the new iPhone is released every ten months. This does not mean that it is outdated, it only means there is something better and faster, with more features added. However, as these new features are added, faster processors are created, and larger storage devices are increased, the technology behind them changes. When these technologies change, law enforcement has to be able to identify these changes and find ways to retrieve the evidence needed from them for their cases.

Law enforcement has customarily lagged behind the technology curve. This has given the criminal a window of opportunity to victimize people while the criminal justice system tries to figure out ways to address the problems. With competent, trained and educated law enforcement officer, trained in computer forensics, departments can adequately reduce this learning curve and apprehend criminals in a more timely fashion. It is incumbent upon law enforcement agencies to establish these forensic programs to combat this growing problem, and set its goals at getting ahead of the technology curve.

COUNTER POSITION

There are many things to take into account when trying to establish a computer forensic program for law enforcement. Some administrators believe that the cost of funding a computer forensic program with the proper equipment and training for the investigators is cost prohibitive for smaller departments with limited budgets. With the economic downturn and the constant reduction in budgets in departments across the nation, it is impractical to reallocate funding from other programs that are focused on officer safety to buy equipment and training for a computer forensic program ("The Impact," 2014, para.4). Officer safety must always be a priority in any law enforcement organization.

While it is true that there are a lot of organizations that are dramatically affected by the economic downturn, it is possible to implement a functional computer forensics program with a small organization. There are opportunities available to agencies that work with federal law enforcement agencies on criminal cases to receive funds from asset forfeiture. These funds are distributed in accordance with the DOJ "Equitable Sharing Guide", which also regulates the acceptable uses of the funds received through this program. The DOJ restricts the use of these types of fund for law enforcement use only. While this falls under a broad banner, the DOJ has outlined very specific uses. These uses include investigations, training, detention facilities, equipment, travel and transportation, awards, awareness programs, and several other areas ("Guide To Equitable Sharing," 2014, p.17).

This opens a door of opportunity for agencies to receive much-needed funding for specialized programs, such as computer forensics. The primary limitation of this

program is that the funding cannot be used for salaries, and it cannot be used for non-law enforcement programs (“Guide To Equitable Sharing,” 2014, p.20). In smaller organizations, it is not necessary to employ a full-time person to do computer forensics. Smaller agencies can partner with other small agencies to set up a forensics lab, or even participate in a federal high tech task force. This will enable these smaller departments to utilize their manpower to its fullest, and address the issues of technology crime at the same time. The FBI has established several regional computer forensics labs (RCFL) in every state. These labs utilize officers from many agencies “RCFL Examiners combine the talents and experience of federal, state, and local law enforcement agencies. Normally, an RCFL consists of 15 people: 12 of the staff members are Examiners and three staff members support the RCFL” (“About RCFL,” 2014, para. 3). At the very least, a small organization can utilize an existing officer or investigator to perform forensic analysis on a part-time basis if necessary. This will allow the department to address the issue and have the resources available when it is critical to an investigation.

Technology can be intimidating to a lot of people. This is no less true in the realm of law enforcement. Some officers do not feel comfortable dealing with technology, especially when it comes to doing something as advanced as computer forensics (Bush, 2013, para. 9). Most departments lack the skills and expertise to handle technology crime and typically do not have people in their employment with computer science degrees (Goodman, 1997, p. 466). It is almost impossible to keep up with technology changes in today’s world.

While it is true that most officers are intimidated by technology, that paradigm is shifting with the advent of younger more tech-savvy applicants entering the workforce. This does not mean older, more seasoned officers cannot learn how to do computer forensics. There are many programs currently available to train officers in the field of computer forensics. One of the most affordable and basic programs was started by the DOJ back in 1992, which is known as the National White Collar Crime Center (NW3C). This organization “has worked to support the efforts of state and local law enforcement to prevent, investigate and prosecute economic and high-tech crime” (“The National,” 2014, para.15). The NW3C offers training programs that will train officers with little to no computer forensic skills, into advanced computer forensic specialist through a series of courses that build on their knowledge. The courses that the NW3C offers start with the basics of teaching the officer the components of a computer, to establishing basic terminology and practices, and establishing good forensic technology and processes to investigate computer crime (“The National,” 2014, para. 15).

The NW3C is not the only organization that teaches this type of material. Other businesses such as EnCase, Forensic Tool Kit (FTK), Paraben, and Cellbrite offer products and training for police officers with varying skill levels, from investigators with no skills to experts. These programs are consistent with those of the NW3C and the International Association of Computer Forensic Specialist (IACIS) in the methodology and court approved practices for computer forensic examinations.

Large companies have grown weary of law enforcement capabilities to investigate technology crime and have implemented programs on their own to address the needs of the business. These companies have found ways to curb technology crime

within their organization and filled the gap left by the lack of expertise and skills of law enforcement agencies. This has led to companies handling these technology crimes on their own and rarely involving law enforcement (Tomar, Rai, & Kharb, 2006, para.15).

Large companies have found ways to address technology crime internally, and they have the personnel with the skill and the ability to address these issues. However, law enforcement has a great opportunity to build some quality, long lasting relationships with these companies and regain their trust in law enforcement abilities to address their criminal issues. The High Tech Crimes Investigators Association (HTCIA) has established itself to help bridge the gap between businesses and law enforcement. The HTCIA mission is to “provide education and collaboration to our global members for the prevention and investigation of high-tech crimes” (HTCIA, 2014, para. 6). These global members include investigators from the private sector as well as law enforcement officers at the local, state, and federal levels. Through this collaboration and others like it, the gap has narrowed, and new and better alliances have been forged with companies that do hold the expertise and can assist law enforcement with their knowledge.

Programs like the HTCIA and IACIS help law enforcement build trust between each other. This alliance shows the organizations willingness to learn and their commitment to the community. With an ever growing emphasis on community policing and establishing valuable, lasting relationships in the community, it is imperative that the business community not be left out in that mission. Organizations will find that businesses are just as dedicated to addressing these issues as law enforcement and will prove to be a reliable resource for the organization and the community as a whole.

This is being seen in today's news such as "Zetron, a leading provider of mission-critical communications solutions worldwide, announced that it is partnering with Government Capital Corporation, to offer tax-exempt financing to help public safety agencies purchase new equipment" ("Zetron's," 2014, para.5).

RECOMMENDATION

Establishing a computer forensic program is essential for any size organization. The future of computer forensics will only grow more complicated as technology continues to change and evolve. A group of technology experts were polled and stated they were "worried that privacy would become a luxury good, and people and organizations might not adapt fast enough" (Arit, 2014, para.3). This is presented as a challenge not only to the general public but also to law enforcement. Some law enforcement organizations have been slow to adapt to the technology age and are currently behind the curve when it comes to technology. The longer an organization waits, the further behind they will get. Eventually, it will be difficult to catch up with technology. The sooner an organization can implement a computer forensic program, the better they will be able to respond to these issues.

Every law enforcement department is tasked with protecting and serving the public. Each of these communities has entrusted the organization to be able to address all issues of crime adequately. Technology crime is one of those areas that the public expects law enforcement to be able to investigate and prosecute criminals. Organizations can no longer ignore the need to train their officers to handle these crimes and provide the resources and equipment necessary for them to be successful.

Cost is one of the primary contributing factors behind organizations refusing to establish a computer forensics program. This obstacle has not gone unnoticed. There are many programs available through the federal government grant programs that can assist the organization in dealing with the cost of training and purchasing equipment. In addition to the grant programs, there are other avenues to addressing funding. Organizations can utilize asset forfeiture funds to purchase equipment and training as well as reaching out to local technology businesses for assistance as well. There is an additional option if the organizations are unable to establish funding through their regular budgeting process. Contrary to popular belief, the average desktop computer system has sufficient power and resources needed to complete a forensic analysis. While a faster more robust system can speed up the process, it is not required. Other options are available for software that can be obtained for free, such as the ILook computer forensic software that is freely distributed by the Internal Revenue Service (IRS) (Koukoushkina, 2014, para.1). There are many software options available that range from free to very expensive. There are options available for every budget.

Computer forensic training is available from a variety of sources, and at a variety of costs. The NW3C offers forensic training programs at a low cost to law enforcement agencies (“The National,” 2014, para. 15). There are also many commercial software vendors that offer training a various cost and degrees of difficulty. Each of these programs will provide the investigator a solid foundation for dealing with digital evidence on an abundance of electronic devices and the ability to adequately investigate technology crimes. These types of devices can range from cell phones to servers. Establishing the investigator's skills are essential to prosecuting these types of cases.

Investigators will often have to testify to their processes and findings in court, and will have their work subjected to peer review. The evidence collected in these types of cases has to follow a strict process for admission in court, and the investigator needs to be trained on these processes.

Manpower can often become a stumbling block for many organizations. This should not be the case. Regardless of the size of a department, there is a good chance that there is at least one person in the organization that can be identified to establish these skill sets. This individual can work either part time or full time on computer crime cases, depending on staffing needs. The biggest challenge is establishing the training and skills the investigator will need to do the job. Establishing and maintaining competency in forensic analysis is a necessity for the investigator, and they should maintain their licensing and certification to prove their proficiency in the science. These skills are perishable, and the investigator needs to work regularly on technology utilizing their skills to improve their abilities and continue learning new processes.

Business communities have found much value in computer forensics. They have established some of their forensic programs within their companies. Most of these businesses are eager to work with law enforcement agencies and provide them with equipment, resources, and training, to ensure that these cyber criminals are prosecuted for the crimes they commit. In the digital age, businesses and law enforcement agencies need to send a strong message to criminals that they can no longer hide behind the screen of their computer anonymously. Through continued partnerships and strengthened relationships with the business community, community oriented policing

initiatives can be bolstered, and police departments can provide a much needed service to the business community, who is often left to fend for themselves in this area.

Protection is essential to a law enforcement agencies, and regardless of how difficult it may be, each organization needs to establish a computer forensic program. Training and resources are widely available from grants to partnerships with businesses in the community. Each of these will enable the department to obtain the skills and expertise it needs to investigate these highly technical cases. These types of crimes cover a large nexus, and this will only grow larger with time. Law enforcement agencies need to close the gap and fulfill the commitment to protect and serve, to include appropriately investigating and prosecuting technology crime. Cost for the establishment of the program can be minimal. Most organizations can utilize computers that they already have in their office. Training is essential and affordable with a vast array of opportunities at varying levels of cost and difficulty. Manpower is adjustable and can be addressed on a part time basis until the department can secure funding for a full-time position. Law enforcement agencies no longer have the luxury of looking the other way when it comes to technology crimes and crimes where technology is present. Each organization should work at tackling these small obstacles and provide a much-needed service.

Creating a plan of action is critical to the success of this type of program. The key to starting is identifying the person or persons who will be tasked with learning the skills and performing the work. Once these individuals have been identified, the department should determine which training they want to send them to, based on the budgetary constraints they have in place. Once the officers are trained, they will be able to assist

the department in identifying current equipment that can be used for establish the forensic program, or intelligently articulating the need for additional equipment and programs that are needed. Once this has been established, and the equipment and programs have been purchased, the final step is setting up a lab environment and testing the hardware and software for usability and accuracy. The officers who have received the forensic training will have detailed instructions on how to validate their tools and equipment to ensure that it is admissible in a court of law. At the end of each year, this program should be evaluated to identify future needs and feasibility for the department.

It is important to remember that law enforcement agencies can and should address technology related crimes. When the need arises, it is important that the department has the resources available to get the job done. With the constant backlog at centralized RCFL's, it has and may become completely unacceptable to have to wait a long period of time to get results back on an investigation. The process is by no means easy, but it is achievable.

REFERENCES

2013 Internet Crime Report. (2014). Retrieved from http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

About RCFL. (2014). Retrieved from http://www.rcfl.gov/DSP_P_abaout.cfm

Arit, J. (2014, March 3). Experts predict the future of technology. *The Wire*. Retrieved from http://www.thewire.com/polotics/2014/03

Bush, A. M. (2013, July 4). Technology continues to evolve in law enforcement. *CJOnline*. Retrieved from http://cjonline.com/news/2013-07-04/technology-continues-evolve-law-enforcement

DiGangi, C. (2013, December 31). These identity theft statistics are even scarier than you'd expect. *The Daily Finance.* Retrieved from http://www.dailyfinance.com/2013/12/31/scariest-identity-theft-statistics/

Digital Evidence And Forensics. (2010, November 5). Retrieved from http://nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx

Goodman, M. D. (1997). Why the police don't care about computer crime. *Harvard Journal of Law and Technology.* Retrieved from http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf

Guide To Equitable Sharing. (2014). Retrieved from http://www.justice.gov/usao/ri/projects/permuses_es.pdf

Hill, K. (2011, November 3). Solving a teen murder by following a trail of digital evidence. *Forbes*. Retrieved from http://www.forbes.com/sites/kashmirhill/2011/11/03/solving-a-teen-murder-by-following-a-trail-of-digital-evidence/

HTCIA. (2014). Code of ethics & bylaws . Retrieved from http://www.htcia.org/code-of-ethics-bylaws/

Huff, R., Desilets, C., & Kane, J. (2010). National public survey on white collar crime. Retrieved from http://www.nw3c.org/docs/research/2010-national-public-survey-on-white-collar-crime.pdf?sfvrsn=8

Koukoushkina, N. (2008). New technology will provide unprecedented access to electronic data and will dramatically increase the speed of digital discovery. Retrieved from http://www.perlustro.com/press-releases/groundbreaking-forensics-technology

McQuade, S. (2001). Technology-enabled crime, policing and security. Retrieved from http://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/mcquade.html

Moore, G. E. (2011). Cramming more components ont integrated circuits. Retrieved from http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf

Rosen, R.J. (2014, January 16). The floppy did me in.*The Atlantic.* Retreived from www.theatlantic.com/technology/archive/2014/01/the-floppy-did-me-in/283132

Survey Of Identity Theft In 2003. (2003, September 3). Retrieved from http://www.ftc.gov/news-events/press-releases/2003/09/ftc-releases-survey-identity-theft-us-273-million-victims-past-5

The Impact Of The Economic Down Turn On American Policing Agencies. (2014). Retrieved from http://www.cops.usdoj.gov/Default.asp?Item=2602

The National White Collar Crime Center. (2014, March 26). Retrieved from http://nw3c.com/docs/presskit/value-of-nw3c.pdf?sfvrsn=10

Tomar, P., Rai, B., & Kharb, L. (2006). New vision of computer forensic science: Need of cyber crime law. Retrieved from https://ispub.com/IJLHE/4/2/9300

Zetron's New Program Helps Public Safety. (2014, October 31). Retrieved from http://www.officer.com/press_release/12015447/zetrons-new-program-helps-public-safety-agencies-finance-equipment