INTEGRATING CIVILIAN COMPUTER FORENSICS EXAMINERS IN LAW ENFORCEMENT CRIMINAL INVESTIGATIONS

by

Steven Cvengros

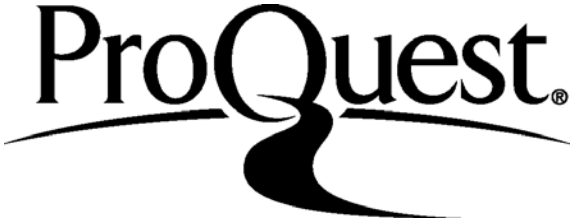
A Capstone Project Submitted to the Faculty of

Utica College

August 2016

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity



Abstract

Digital evidence is a staple in modern court cases. It is nearly impossible to find a case that does not present digital evidence during courtroom proceedings. The manner in which this evidence is gathered and presented varies widely between geographic regions and presents unique problems for the judicial system. Law Enforcement is facing an ever-increasing caseload and a lack of qualified individuals that can competently process digital evidence. Most agencies experience high turnover within the ranks of sworn staff that further compounds the caseload. Using civilian examiners, law enforcement agencies may be able to ease case backlogs and avoid the problems associated with high turnover rates. The use of civilian examiners presents different challenges to some organizations; civilian examiners generally are not accepted among sworn staff. Several law enforcement agencies have found success in blending a team of sworn investigators with civilian computer experts to pool the unique skills that each can bring to the investigative process. Keywords: Cybersecurity, Cynthia Gonnella, computer forensics.

Acknowledgements

This is dedicated to the unsung heroes that help the silenced victims of child abuse. I would like to thank my family for sacrificing with me, Christy Asbra for her help and support, Lieutenant Mike Browne, Sergeant Scott Landen, and the entire San Bernardino County Sheriff's Department for their help and encouragement in making this happen. I would also like to thank the Mercedes AMG Petronas F1 team for the inspiration to strive for excellence.

Table of Contents

Integrating Civilian Computer Forensics Examiners in

Law Enforcement Criminal Investigations

Digital and electronic devices have not only become a normal part of modern society, but these devices have also formed an integral part of criminal activity. Digital devices such as smartphones and computers record tremendous amounts of data about the day-to-day activities of their users. Many users are unaware that their digital devices are recording and tracking vast and varying bits of information, regardless if the device is actively being used or not. As pointed out by Sean E. Goodison Ph.D., former Washington D.C. Metropolitan Police analyst, Robert C. Davis, Police Foundation's Chief Social Scientist, and Brian A. Jackson, researcher for the RAND corporation, in their report *Digital Evidence and the U.S. Criminal Justice System*, the wide range and use of digital devices give tremendous potential for the acquisition of digital evidence in civil as well as criminal court cases (2015, p. 3).

The widespread use of digital devices, coupled with the amount of information contained within, has led to severe delays in processing digital evidence for most law enforcement agencies. Many law enforcement agencies suffer from inadequate staffing, budgetary, and equipment constraints, as well as turnover of examiners, all of which contribute to delays in processing digital evidence (Goodison, Davis, & Jackson, 2015, p. 5). Consider that the United States has over 336 million wireless subscriptions for various digital devices; each of these devices contains a vast amount of data that can be potential evidence (Goodison et al., 2015, p. 4). Digital evidence is not limited to the electronic device; social media websites as well as the networks that connect with digital devices also contain potential evidence (Goodison et al., 2015, p. 3).

The purpose of this research was to assess the integration of civilian computer forensic examiners in law enforcement criminal investigations. How are sworn officers trained to handle complex digital evidence in local agencies? What challenges are present for agencies when integrating civilian staff? What obstacles prevent local agencies from pursuing accreditation for computer forensic laboratories?

Justin P. Murphy and Adrian Fontecilla, attorneys at Crowell & Moring's Washington D.C. office specializing in white-collar crime, noted in their article "Social Media Evidence in Criminal Proceedings: An Uncertain Frontier," the online use of social media has increased by over 350% between 2006 and 2013, as over 90% of adults use applications such as Facebook on a daily basis (2013). Every day, vast amounts of data are created by users; Facebook receives over 500,000 pieces of new content every minute (Murphy & Fontecilla, 2013). The information provided from social media organizations is a veritable treasure of potential evidence. Connections inferred from a user's activity on social media could provide location data as well as potential accomplices (Murphy & Fontecilla, 2013).

Warrants and subpoenas are not always required with public information from social media (Murphy & Fontecilla, 2013). Google has relayed that the number of user information requests received has increased more than 40% from 2009 to 2011 (Murphy & Fontecilla, 2013). According to a survey of law enforcement professionals, most have not received training on using social media for investigative purposes. Of those surveyed, most intend to start using social media, if they have not done so already (Murphy & Fontecilla, 2013).

The amount of potential digital evidence that people create on a daily basis is enormous. Without following the proper investigative techniques, an examiner can overlook or change potential evidence. Mishandling of digital evidence can have serious consequences in criminal

cases. The murder trial of Casey Anthony had several mistakes with the digital evidence presented (Goodison et al., 2015). The software used in the Anthony case produced inaccurate results; additionally, there was a failure by investigators to search all internet browsing history (Goodison et al., 2015). Goodison, Davis, and Jackson, further explained that corrections made to evidence reports during the trial very likely influenced the reasonable doubt that jurors felt when acquitting Anthony of the murder charges (2015). Courts use digital evidence much the same as any other evidence, as detailed by Goodison, Davis, and Jackson, yet there are attributes that make it different to deal with than traditional physical evidence (2015). Digital evidence requires different training and tools to be effective and accurate in the judicial system (Goodison et al., 2015).

Most local agencies are ill prepared to handle digital evidence due to the challenges of budgetary constraints, lack of training, and difficulty retaining staff (Goodison et al., 2015). As explained by Arron Alva and Barbara Endicott-Popovsky faculty of the Center for Information Assurance and Cyber Security at University of Washington, in their report Digital Evidence Education in Schools of Law, there are gaps in the levels of understanding of digital evidence between the legal and judicial communities (2012). Lack of knowledge of digital evidence can have serious consequences on defendants in the courtroom, as was the issue in the Julie Amero case (Alva & Endicott-Popovsky, 2012).

Julie Amero was a substitute teacher that was the unfortunate victim of computer malware that displayed pornographic images on the classroom computer (Alva & Endicott-Popovsky, 2012). While reviewing the case, Alva and Endicott-Popovsky uncovered the forensics investigation did not use industry standard tools and the investigator had not received specialized training (2012). Alva and Endicott-Popovsky further determined the judge lacked

sufficient knowledge to allow questioning that detailed how the evidence was gathered (2012). The prosecuting, as well as the defense attorneys, in the Amero case did not understand the information being presented and failed to accurately direct the questioning of witnesses (Alva & Endicott-Popovsky, 2012). Alva, along with Endicott-Popovsky determined that questioning during the cross-examination in the case used phrases such as "parasites," displaying an extreme lack of knowledge in computer and Internet functionality (2012). To further compound matters, the prosecution showed full sized images to the jury where only thumbnail sized images displayed on the computer screen (Alva & Endicott-Popovsky, 2012).

Alva and Endicott-Popovsky discovered mishandling of the evidence in the Amero case was not limited to the attorneys but also included the detective assigned from the local police agency (2012). Based on court testimony, the detective may have examined the original hard drive of the computer instead of a forensic copy (Alva & Endicott-Popovsky, 2012). Competent forensic examiners would know that direct access to data on the hard drive can alter the evidence and can change timestamps on files (Alva & Endicott-Popovsky, 2012). Reviewing court transcripts, Alva and Endicott-Popovsky determined the detective plainly admitted to not examining the hard drive for viruses and other malware (2012). The failure of the detective to examine the hard drive for evidence of malware is a prime example of the need for specialized training and the need to establish an industry set of standards for dealing with electronic evidence.

The computer forensics training received by detectives in local law enforcement agencies varies greatly between jurisdictions. As noted in *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors,* authored by Anthony Reyes retired New York City detective, there are times when digital evidence and the methods for

gathering it seldom receive questions in court because many defense attorneys do not understand the technical details of the evidence (2007). Many in law enforcement feel that the computer investigator does not need to understand complex technical details, but rather just explain what they found while examining the digital evidence (Reyes, 2007). There are varying opinions on the level of expertise necessary for a computer forensic examiner. As a detective is not required to be an expert in binoculars to testify what they saw with them, some law enforcement agencies argue that an investigator does not need to be a computer expert to explain findings on a suspect's machine (Reyes, 2007).

Detailed in *Identifying a Computer Forensics Expert: A Study to Measure the Characteristics of Forensic Computer Examiners* by Gregory H. Carlton, California State Polytechnic University and Reginald Worthley, University of Hawaii, with the rapid expansion of digital evidence in the legal arena, the need for computer examiners is also growing (2010). The growing demand for examiners complicates the ability to find qualified resources able to perform this work (Carlton & Worthley, 2010). Courts have systems in place to qualify witnesses to provide expert testimony (Carlton & Worthley, 2010). There is currently a lack of understanding of computer forensics in various government organizations, which can allow an individual to be an expert in one geographic area and not in another (Carlton & Worthley, 2010).

The lack of understanding, coupled with the rapid growth and backlog of digital evidence, has led some law enforcement agencies to try new methods to deal with an ever-increasing caseload. As discussed in "High-Tech Forensics" by Warren Harrision, Computer Science Professor, Portland State University, George Heuston, retired FBI, Sarah Mocas, Assistant Professor, Portland State University, Mark Morrisey, Portland State University, John Richardson, Intel, with the continued use of electronic evidence in cases, there is a need for law

enforcement to explore different methods for processing it (2004). One agency has enlisted the help of volunteer civilians to assist with the processing of digital evidence (Harrison et al., 2004). The Hillsboro Police Department in Oregon has discovered that there is a pool of experts in areas that police typically fall behind the criminals, specifically where computers and sophisticated technology are factors in the commission of a crime (Harrison et al., 2004). Without an understanding of technology, emails, text messaging, and the related artifacts included with digital evidence, criminal cases may fail to reach trial or worse yet, the presentation of inaccurate evidence (Harrison et al, 2004). Some industry experts have placed the losses of cyber-crime as high as one hundred billion dollars, and most of the cases, over 90%, are not reported (Harrison et al, 2004).

The primary function of the police volunteers is to increase the effectiveness of the department in its mission to protect the public (Harrison et al., 2004). The volunteers help with the entire investigation, from beginning to end, including search warrants and analyzing digital evidence (Harrison et al., 2004). While the volunteers are not experts in every aspect of computer and digital evidence, their knowledge has shown to be far greater than that of the average detective assigned to a computer crimes division (Harrison et al., 2004). The volunteers in Hillsboro can expect to serve for at least two years and serve in various capacities, from working in the lab to being available for consultations in emergencies (Harrison et al., 2004). Traditionally, law enforcement has been lukewarm, at best, to the idea of integration with civilians to assist with investigations (Harrison et al., 2004); with the ever-increasing backlog of digital evidence, this attitude is changing in some jurisdictions.

Despite the successes that various agencies have had with the integration of civilian investigators, some organizations are against the idea. In an article by Ryan Flynn, staff writer

for the New Haven Register, “Civilians seen as option for forensic units; union disagrees”, Assistant Police Chief Achilles Generoso explained, the police department in New Haven Connecticut would like to integrate civilian personnel into the forensics unit; however, the police union is against the idea (2015). The department has trouble with staff turnover in the forensics unit, and the department feels that civilians with specific areas of expertise might be a better fit for these technical positions (Flynn, 2015). The local police union feels that sworn personnel should do this work, and they should hire more detectives if more staff is required (Flynn, 2015). The union also suggests that a possible solution to staff turnover would be an increase in pay, but with the budget shortfalls so many agencies are facing, this does not seem like a viable option (Flynn, 2015). Local law enforcement agencies must be open to new ways of handling cases that contain digital evidence. Resistance to new methodologies, use of additional civilian staff and new processing techniques will continue to burden the departments, as well as the criminal justice system.

Literature Review

Training Sworn Officers to Handle Complex Digital Evidence in Local Agencies

Digital Evidence

Digital evidence is information that is pertinent to an investigation that is stored, collected, or transmitted by an electronic device (Goodison et al., 2015). This information is not new and has existed for decades in various forms. The criminal justice system has faced challenges with processing digital evidence from the prolific increases in the use of personal electronic devices. The courts have recognized smartphones as not just communication devices but also calendars, diaries, and emails systems (Goodison et al., 2015). The type of information

normally contained in a smartphone goes beyond typical evidence that law enforcement would generally collect (Goodison et al., 2015).

Common Types of Digital Evidence. There are four common types of digital evidence. There is Internet evidence pertaining to activity a user or computer would have done while connected to the Internet. File sharing evidence is associated with peer-to-peer networks. Computer and smartphone evidence pertains information found within and associated with the respective device.

Internet. Internet evidence includes information from communication websites and social media (2015). According to Goodison, Davis, and Jackson, Internet evidence was some of the first types of digital evidence used in law enforcement investigations (2015). Sites such as Facebook and Twitter are examples of Internet digital evidence that are still widely used in investigations today (Goodison et al., 2015). One of the many challenges faced by law enforcement in gathering Internet evidence, as explained by Goodison, Davis, and Jackson, is the secrecy in the location of many of these services (2015). The use of encryption on some communication sites poses a significant challenge for law enforcement to extract potential evidence from a suspect's correspondence (Goodison et al., 2015). Goodison, Davis, and Jackson stress that encrypted communications linking two or more suspects together is still valuable potential digital evidence despite law enforcement's inability to read the communications (2015).

File sharing networks. File sharing networks connect users to share data such as pictures, videos, and other digital files (Goodison et al., 2015). Goodison, Davis, and Jackson explain the tracking of peer-to-peer network users is by IP address, making the investigation of these networks a substantial source of digital evidence (2015). With the ability of network-

administrators and Internet service providers to log user activity, some users have taken steps to anonymize their actions online (Goodison et al., 2015). Developed with citizenry of oppressive governments in mind, as explained by Goodison, Davis, and Jackson, the TOR system hides illegal activity on the Internet (2015).

TOR is in use all over the world to encrypt both the legal and illegal activities of its users (Goodison et al., 2015). The notorious Silk Road website utilized TOR for the trade of illegal drugs, child pornography, and other contraband items (Goodison et al., 2015). According to Goodison et al., to access sites like Silk Road, users are required to use applications such as TOR, which can anonymize a website just as it can mask the activity of a person (2015). Websites that rely on TOR for access are part of the dark web and present a significant challenge to law enforcement (Goodison et al., 2015).

Computers. Personal computers contain information that is also on the Internet, but computers also store unique information specific for each user (Goodison et al., 2015). According to Goodison, Davis, and Jackson, temporary Internet files, cookies, and browsing history are all examples of potential digital evidence that is available from computers (2015). Emails and messages are other sources of information that could be relevant to an investigation that can yield significant clues of a user's activities (Goodison et al., 2015).

Smartphones. As explained by Goodison, Davis, and Jackson, smartphones are arguably the largest area of concern in digital forensics today (2015). Smartphones are a staple of modern society and have exploded with new features and capabilities recently (Goodison et al., 2015). In most cases, courts have ruled a warrant is necessary to search a phone in the field (Goodison et al., 2015). According to Goodison, Davis, and Jackson, smartphones can contain a wide and

varied amount of data about their users, information such as GPS coordinates, pictures, text messages, and other personal attributes are available to examiners (2015).

Varied Skillsets

There is a massive amount of variety in electronic devices, local law enforcement agencies need staff with varied skillsets to efficiently and accurately process digital evidence. With the varying methods that devices require to extract digital evidence, agencies face complex challenges to build and maintain staff capable of performing competent forensic analysis (Goodison et al., 2015). With the rapid advancements in technology, many jurisdictions are struggling to cope with the tremendous amount of digital evidence (Goodison et al., 2015). Already suffering from an influx of digital devices, Goodison, Davis, and Jackson explain many departments are suffering from budgetary and training shortages as well (2015). In most cases both the victim and suspect will have devices that will need examination leading to an ever-increasing amount of devices that will need specialized skills for each type of device (Goodison et al., 2015).

In 2016, there is a lack of accepted standards in regards to processing electronic evidence (Goodison et al., 2015). According to Goodison, Davis, and Jackson, it is nearly impossible for departments to keep up without accepted standards and methodologies for information (2015). The varying and expansive list of devices poses a significant challenge for law enforcement as there is no agreed upon process to obtain information for makes and models, let alone different devices (Goodison et al., 2015).

Proper examination of a smartphone can produce evidence showing what each party was doing before and possibly during the crime (Goodison et al., 2015). Evidence that points toward guilt as well as exculpatory evidence found mixed on a suspect's smartphone can be a challenge

for prosecution as well as the defense, without standard methodologies, the risk of missing some evidence increases (Goodison et al., 2015). As detailed by Goodison, Davis, and Jackson, the issue of multiple jurisdictions, each with their own unique methods further complicates information sharing between agencies (2015). Electronic devices have the ability to connect to multiple networks often times across counties, states, and even countries away (Goodison et al., 2015).

Training Available

Based on the numerous types of electronic devices and the various types of information each device contains, examiners need specialized skills, training, and tools to perform forensic analysis (Goodison et al., 2015). As explained by Goodison, Davis, and Jackson, law enforcement agencies should not expect that a small staff could adequately process any type of electronic device that may come their way (2015). Many agencies report that processing digital evidence comes with a high cost; equipment and training can be in the tens of thousands of dollars (Goodison et al., 2015).

As outlined in "The National Computer Forensics Institute provides sorely needed training for cops" by Linda Musthaler, Principal Analyst with the Essential Solutions Corporation, federal agencies have been providing training and equipment to state and local law enforcement in an attempt to offset the high costs associated with processing digital information (2014). According to Musthaler, as late as 2006, many smaller agencies were unable to process digital devices for potential evidence (2014). The United States Department of Homeland Security is one of several organizations that can provide training and equipment to local law enforcement (Musthaler, 2014). Musthaler explains the training provided is in high demand, and

Homeland Security does not have the budget to provide the training to every agency that requests it (2014).

Training available from FLETC. Federal Law Enforcement Training Centers provide several educational opportunities for law enforcement agencies in a wide range of topics (Federal Law Enforcement Training Centers, n.d.). Classes range from basic incident response to more specialized disciplines such as seized computer training (Federal Law Enforcement Training Centers, n.d.). The training provided by FLETC is generally available free of charge to the employees of any recognized law enforcement agency (Federal Law Enforcement Training Centers, n.d.). Most of the classes are in Glynco, Georgia requiring attendees to travel, but the travel costs are still significantly lower than many other forms of training (Federal Law Enforcement Training Centers, n.d.).

Training available from the National White Collar Crime Center. The National White Collar Crime Center (NW3C) provides law enforcement organizations with several different classes in varied disciplines. NW3C courses are free for law enforcement personnel and geared to examiners and first responders alike (National White Collar Crime Center [NW3C], n.d.). NW3C also provides online training, which can greatly reduce travel costs for smaller agencies (NW3C, n.d.). Law enforcement departments can also request the NW3C provide training at their site to allow allied personnel from nearby communities to attend (NW3C, n.d.). The NW3C has training available in widespread geographic areas that should make traveling easier for potential trainees to attend (NW3C, n.d.).

On the job and vendor specific training. Training for potential examiners is of paramount importance in any law enforcement organization. Sworn personnel receive little to no training specific to digital forensics while participating in police academies. The minimum

educational requirement for a deputy sheriff trainee with San Bernardino County is a high school diploma or GED (County of San Bernardino, n.d.). Sworn law enforcement personnel typically receive training in digital forensics only after assignment to that detail, some of which is on the job training. (County of San Bernardino, n.d.). After assignment to a position that requires specialized knowledge, employers will send staff to vendor specific training for programs such as EnCase or Forensic Tool Kit (FTK) in most cases (Reyes, 2007).

Minimal training required. To effectively present evidence and testify in court, an examiner needs to have at least a basic level of understanding of digital devices. The minimum requirements in regards to training and competency vary between jurisdictions. "Cyber crime investigators are primarily percipient witnesses. This means that although the analysis of a computer might have involved complex technical issues, the basic purpose for which the investigator's testimony is offered is to describe what he saw and did, rather than to offer complex technical information about computers or forensic software" (Reyes, 2007, p.51, para. 2). There is no expectation that a police officer using binoculars is an expert in optics to testify what they have seen through them (Reyes, 2007). An examiner that used forensic software to discover child pornography on a suspect's computer would not need to be an expert computer programmer to testify about the discoveries made using the program (Reyes, 2007). Examiners must have an understanding of computers to perform their investigation, but there is no need for an examiner to hold an advanced degree in computer science (Reyes, 2007).

Many investigators are concerned about testifying to complex details of the computer or forensic software used in the examination (Reyes, 2007). Furthermore, examiners are also worried about explaining how they can be sure that they did not alter or create any of the

evidence found on a suspect's computer (Reyes, 2007). According to Reyes, most of the worries that examiners have about testifying are unfounded and not cause for alarm (2007).

Investigators must have enough training to be able to establish a solid foundation that demonstrates competency in discovering and presenting evidence without contamination (Reyes, 2007). Proper chain of custody for potential evidence will support allegations of contraband residing on the suspect's computer (Reyes, 2007). Reyes went on to explain, examiners must also be able to show that the electronic devices analyzed were not contaminated by the process of examination (2007). Courts can qualify investigators as expert witnesses, but it is important for an examiner not to overstate their training or abilities (Reyes, 2007).

Common vendor training. EnCase is one of the more popular pieces of software available for computer forensics today (Guidance Software, n.d.). Guidance Software, the developer of Encase, provides several classes for examiners at all skill levels (n.d.). Classes are located in many geographic areas; online and onsite training is available as well (Guidance Software, n.d.). Vendor specific training, as explained Guidance Software, will allow the examiner an additional avenue to demonstrate working knowledge of industry standard software to the courts and jury (n.d.). Encase forensic software is accepted by the criminal justice system as a reliable and efficient tool for examination of digital devices (Guidance Software, n.d.).

Challenges for Agencies When Integrating Civilian Staff

There is a tremendous amount of digital evidence in the criminal justice system (Murphy & Fontecilla, 2013). Before presentation in a courtroom, examiners will spend a great deal of resources analyzing and cataloguing evidence (Carlton & Worthley, 2010). Law enforcement agencies across the country are struggling to keep up with the legal requirements of court-mandated deadlines (Flynn, 2015). Despite the hurdles that evidence backlogs create for the criminal justice system, defendants have the right to have their cases heard in a reasonable timeframe (U.S. Const. amend. VI). Some law enforcement organizations have attempted to alleviate the backlog challenge and other issues by integrating civilian personnel (Flynn, 2015). As detailed by Flynn, the integration of civilian staff has brought its own unique concerns to agencies attempting to ease the delays with processing potential evidence (2015).

Resistance to change. As William Young, Professor, Organizational Behavior, Indiana Wesleyan University discussed in "Effecting Change: Avoiding the Pitfalls" change in organizations is seldom easy; oftentimes initiatives will fail altogether or be compromised (2006). When organizational change fails, staff usually becomes weary, leadership gets frustrated, and there is wasted time and resources (Young, 2006). Planning can provide a solid path for successful change initiatives. As noted by William Young, Professor of Organizational Behavior, "People do not inherently resist change. Instead, they resist what they perceive as losses associated with the change" (2006, para. 1). Young has identified common perceptions of loss associated with change:

- Loss of status: will the change cause a reduction in title, seniority, rank, or responsibilities?
- Loss of money: will the change effect on-or off-duty incomes?

- Loss of comfort level: will the change create an uncomfortable environment (Young, 2006)?

As explained by Young, change will always be a concern for staff, but managing the perceptions associated with change will yield a better chance for success (2006).

As noted by Young, self-confidence should be a consideration when making organizational changes; staff successfully working an assignment can feel slighted with modifications to their duties (2006). Demonstrating the need for change, involving employees in the development of new policies and procedures, and management being mindful of staff feelings can create an atmosphere of acceptance (Young, 2006). Young explains doing a job well is a sense of pride for most employees; shifting of responsibilities after a number of years can invoke feelings of inadequacy if the employee was not involved in the planning of the change (2006).

Assuming that staff will see the logic and benefit to changes should be avoided (Young, 2006). As noted by Young, Planning should involve all of the staff affected by the proposed shift in paradigm (2006). Changes should have a clear benefit to the department; without goals to achieve employees are less likely to adopt new methods (Young, 2006). In addition, Young stated subordinates should have the ability to express ideas and concerns up the chain of command (2006). Setting deadlines for new procedures provides a sense of urgency to prevent staff from clinging to old ways (Young, 2006). Young explained creating a winning plan for change must include short, medium, and long-term goals with acknowledgements when meeting said goals, and the ability to accept and embrace change is vital for organizations needing greater efficiency (Young, 2006).

Union resistance. Some departments are attempting to ease the burdens created from electronic evidence by integrating civilian personnel to work alongside sworn staff (Flynn, 2015). As noted by Flynn, some police unions see this as an unwelcome change feeling that it should be sworn personnel working with potential evidence (2015). Many law enforcement agencies are suffering from lack of qualified staff to process digital evidence (Flynn, 2015).

Louis Cavaliere, New Haven Police Union President, argues, "It comes down to a labor issue. This is our work, and if they need extra people to collect evidence at a crime scene, then they should hire more detectives. That's going to be our argument" (as cited in Flynn, 2015, para. 26). According to Flynn, some union contracts prevent departments from converting any sworn positions to civillian personnel jobs (2015). Many departments see integration of civilains on forensics teams as a potential solution for the high turn over rate among sworn staff (Flynn, 2015). Flynn (2015) also explained that unions however diagree, arguing that if there are problems with turn over, detectives shold be paid more.

Legal challenges of civilian examiners. As noted in *Harris v. State* (1991) "It would be unreasonable to suggest that the actual physical gathering of the evidence, utilizing equipment and procedures requiring expert skill, and having a high potential for harm to the person being searched must be done by peace officers." Organizations such as the Arizona Department of Public Safety (AZDPS) use civilian analysts who testify in court on a regular basis (Arizona Department of Public Safety, 2014). Civilian examiners presently employed with AZDPS perform forensic examinations of electronic evidence, computer related equipment, network devices, and information systems (Arizona Department of Public Safety [AZDPS], 2014).

Culture clash. James B. Comey, Director of the FBI acknowledged in the article "C.I.A. Officers and F.B.I. Agents, Meet Your New Partner: The Analyst" by Shane Scott, New

York Times, there is an issue with agents and has set goals to achieve better integration with analysts (2015). Cultural challenges can arise with the integration of civilian and sworn personnel (Scott, 2015). As noted by Scott, law enforcement officers are generally viewed as exclusionary and untrusting of outsiders working alongside them (2015). Modern technology has forced changes in criminal investigations, yet there is a culture in law enforcement of civilians not doing police work (Scott, 2015). Scott explains organizations such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) have struggled to integrate civilian analysts with case agents because of cultural differences (2015).

The traditional measure of success at the FBI is building criminal cases, something that an analyst cannot do alone (Scott, 2015). As noted by Scott, special agents can overlook the value of an analyst that cannot rise up the ranks of the FBI in the same fashion they can (2015). Analysts and special agents do not share the camaraderie that agents have with one another, which can lead to strained working relationships (Scott, 2015). Jack Cloonan, former FBI agent, states, "At the end of my career, there was low-level tension between the agents and the analysts" (as cited in Scott, 2015). An analyst's role is putting pieces of the information puzzle together; with the amount of data available, agents face a difficult task without their assistance (Scott, 2015).

After September 11, 2001, the CIA loaned the FBI 40 analysts to aid in the agency's reorientation (Scott, 2015). As explained by Scott, before 2001, most FBI analysts were not qualified to work in an analyst capacity, some of whom were secretaries rewarded with promotion (2015). As noted by Scott, the FBI's promotion practices further fueled agent analyst discord (2015).

While the CIA has used analysts since its inception, work of the field operatives has generally kept the two sides separated (Scott, 2015). John O. Brennan, the CIA director, announced, "Analysts and operators would be combined in ten new mission centers, following the model of the agency's Counterterrorism Center" (as cited in Scott, 2015).

The changes at the FBI and CIA show the steady rise in the roles civilian analysts play in investigations (Scott, 2015). AS detailed by Scott, with the amount of data on smartphones and the Internet, government organizations need skilled people to comb through vast amounts of information (2015). A case office handling a case on their own would face an immense challenge with the wide array of digital devices and electronic information needing analysis (Scott, 2015).

Arranged marriage is a term used to describe the working relationship of the analyst and FBI agent (Scott, 2015). As noted by Scott, just as in an arranged marriage, there is no guarantee that the relationship will blossom and prosper (2015). The FBI now trains analysts and agents together, promoting a shift in culture and laying the foundation for a successful working environment (Scott, 2015).

Analysts are now working side by side in criminal as well as national security cases (FBI, 2011). Prior to the events of September 11, the FBI had about one thousand analysts; since then the number has tripled as responsibilities and requirements have changed (FBI, 2011). As noted by the FBI, Great strides have been made recognizing the importance and abilities that analysts can provide to FBI and CIA investigations (2011). While there is still more to do to improve the relationships between agents and analysts, the model used by the FBI and CIA can aid local agencies wishing to integrate civilian staff with their sworn counterparts (FBI, 2011).

A team approach. The sections below detail how some agencies have implemented civilian and sworn teams to process digital evidence. The Hillsboro Police department has had

success with the use of citizen volunteers. The new Jersey State Police have implemented a blended team to process digital evidence.

Hillsboro Police Department. The Hillsboro (Oregon) Police Department has implemented a program that enlists qualified citizens to serve as computer specialists (Harrison, et al., 2004). "The Hillsboro Police Reserve Specialist (PRS) program provides suitably qualified individuals from the community an opportunity to assist local police in criminal investigations" (Harrison, et al., 2004, p. 1 para. 1). The current focus of the PRS program is the gathering and processing of electronically stored evidence, as well as providing expert testimony in court (Harrison, et al., 2004). According to Harrison, et al., PRS members work the entire case life cycle from the execution of search warrants to analyzing evidence to testifying in court (2004). Reservists will also assist in the development of policies and procedures as well as training for the department (Harrison, et al., 2004). As noted by Harrison, et al., reservists are unsworn agents of the department who typically work under the detective assigned to the case (2004).

As agents of the police department, the Fourth Amendment governs PRS members just as it would sworn officers (Harrison, et al., 2004). As explained by Harrison, et al., reservists must have a working understanding of federal, state, and local rules regarding search and seizure of electronic evidence (2004). PRS members work within the same limits of search warrants as sworn officers and their methods are defensible in court (Harrison,et al., 2004). The department sees a great benefit from the communication between the reservist and the detective, allowing the department to take advantage of their combined skills (Harrison, et al., 2004).

As explained by Harrison, et al., reservists attend ten weeks of training to familiarize them with legal procedures with regulations such as search warrants (2004). This training helps PRS members more effectively assist the detectives with the case, as they can better understand

law enforcement procedures and have a better idea what evidence will best help detectives (Harrison, et al., 2004). As explained by Harrison, et al., detectives receive technical training, so that they can understand how best to use the skills of the reservists (2004). The training system in place in Hillsboro aims to raise the knowledge and abilities of both the sworn and civilian staff (Harrison, et al., 2004).

PRS members can expect to serve for at least two years, with time spent in the forensic lab as well as making themselves available for consultations when needed (Harrison, et al., 2004). As noted by Harrison, et al., with the assistance of the computer industry as well as academia, Hillsboro Police Department successfully integrated a civilian and sworn staff forensic analysis detail (2004). The PRS program has provided a great resource for the Hillsboro community, and the police department has plans to expand the program in the future (Harrison, et al., 2004).

New Jersey State Police. The New Jersey State Police Cyber Crimes Unit employs both civilian and sworn personnel in their investigations (New Jersey State Police, n.d.). The Cyber Crimes unit provides investigative services to federal, state, and local agencies where technology facilitated crime occurs (New Jersey State Police, n.d.). With ever-increasing use of computers and technology, the Cyber Crimes Unit has seen significant increases in requests for processing digital evidence (New Jersey State Police, n.d.).

Arizona Department of Public Safety. The Arizona Department of Public Safety is another organization that has adopted the team approach with having both sworn and civilian examiners. Civilian analysts with AZDPS perform forensic analysis to assist in criminal investigations (Arizona Department of Public Safety, 2014). AZDPS relies on their civilian

personnel to work with investigators and prosecutors in the preparation of search warrants and cases for court (Arizona Department of Public Safety, 2014).

Obstacles Preventing Local Agencies from Pursuing Accreditation

As explained by John J. Barbara, ASCLD/LAB inspector, in the article "ISO/IEC 17025:2005 Accreditation of the Digital Forensics Discipline", most states do not require accreditation, but there is a push to change that (2012). The accreditation of criminal laboratories is critically important to ensure a high degree of confidence in judicial proceedings (Barbara, 2012). As noted by Barbara, without following best practices, the odds of tainting evidence increases, possibly voiding the admissibility of potentially critical information (2012). Accreditation can provide a sound basis for building confidence in a laboratory's ability to process digital evidence (Barbara, 2012).

Accreditation. As noted by Barbara, accreditation is only a part of the overall quality assurance program (2012). Accreditation shows that a laboratory has taken steps to provide quality and reliable services to the community to which it serves (Barbara, 2012). As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, a group of forensic science experts, accreditation does not mean that a laboratory does not make mistakes; it means that the laboratory follows established standards while conducting examinations (2009). Accredited laboratories must have outside oversight to ensure that anomalies in operations do not bias the results of examinations (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, the process of accreditation provides a safety net to ensure there are no shortcuts when there are outside pressures and demands placed on the organization (2009). Laboratories that

have achieved accreditation promote the adoption of standards, foster community ties, and allow employees to gain exposure to other leaders in the forensic science community (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009).

The American Society of Crime Laboratory Directors (ASCLD) governs the accreditation of most criminal laboratories in the United States (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). Developed in the 1970s, ASCLD focused on the development of quality assurance standards (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As explained by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, ASCLD's focus is on the operation of the lab, personnel qualifications, and the physical building (2009). In order to become accredited, the organization must adopt accepted policies and procedures (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, procedures must address protection of evidence from cross contamination, loss, and deleterious change (2009). Laboratories must have validated and documented technical procedures and use appropriate controls and standards (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As explained by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, personnel working in accredited labs must complete competency testing as well as have documented training programs (2009). Personnel employed in an examination capacity in forensic labs are subject to reviews of their work product to ensure competency and quality (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009).

ASCLD accredits a lab for five years; during this cycle, labs are required to submit reports of changes in the labs operations, staff, and building facilities (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). All labs are required to maintain written copies of policies and procedures and sources of possible error (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, depending on the type of accreditation received, some labs are subject to a yearly surprise visit to ensure that proper procedures are being followed (2009). Violations found during inspections can result in penalties for the laboratory; the inspection process has a provision for appeals should a lab receive a penalty (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009).

Accreditation and certification. Accreditation is the assessment of a laboratory's quality, administrative, and technical systems (National Commision on Forensic Science, 2016). As noted by the National Commision on Forensic Science, Accreditation verifies that the organization uses accepted standards and practices to produce accurate results (2016). Accreditation assesses the laboratory as a whole; equipment, personnel policy, and procedures receive validation through the process (National Commision on Forensic Science, 2016).

The National Commision on Forensic Science explains certification is the assessment of an individual in their ability to perform competently in their field of expertise (2016). Certification programs validate attributes such as education, training and practical experience, requirements for continuing education, and an adherence to a code of ethics (National Commision on Forensic Science, 2016). Certification does not asses the quality of an

individual's work or the methods used by the individual in the execution of their duties (National Commision on Forensic Science, 2016).

Accreditation challenges. Detailed in the sections below is the most common challenges laboratories face while pursuing accreditation. Laboratories must address terminology and standards issues before becoming accredited. Evidence collection, along with how examiners operate in their day-to-day activities, will need updates to ensure the success of accreditation.

Terminology and standards. As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, there are terms used in forensic reports such as "match", "consistent with", "identical" and "similar in all respects tested" (2009). These terms influence judges and juries, yet there is no standard meaning between labs (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). Laboratory reports should be complete and provide details on the results as well as the methods used (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As detailed by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, the aim of the report should be to provide detail to a non-scientist reader that allows unbiased scrutiny of the conclusion (2009). Forensic reports, as well as courtroom testimony relying on them, should include clear characterizations of the terminology and methods used (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009).

Adoption of standards creates quality systems, policies, and procedures that promote consistency among practitioners (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). Accreditation and certification of laboratories and service providers can enforce these standards (Committee on Identifying the Needs of the

Forensic Sciences Community, National Research Council, 2009). As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, adoption of standards will allow the forensic science community to work collectively toward the same goal, providing accurate, consistent, and reliable data (2009).

Evidence collection. Practices of evidence collection vary greatly between organizations (Barbara, 2012). As noted by Barbara, some agencies will perform analysis of electronic devices after collection and seizure, while others will do an initial analysis on scene to collect volatile evidence (2012). Challenges arise for attorneys when deciphering evidence collected with various methods, making courtroom testimony ambiguous (Barbara, 2012).

Best practices have called for electronic devices to be unplugged, seized, and brought to a lab for examination, but this leaves potentially valuable evidence unavailable (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, recently entered passwords, encryption keys, and active files are stored in volatile memory, which is lost when there is a power interruption (2009). Best practices for various types of acquisitions are needed in the computer forensics discipline (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009).

Examination of a computer generally involves two steps: the acquisition phase and the examination phase (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). During the acquisition the contents of the subject hard drive is forensically copied to another drive, the copy is then compared to ensure an exact match (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As explained by the Committee on Identifying the Needs of the Forensic

Sciences Community, National Research Council, for the sake of preserving the original data, examination of the forensic copy is accepted best practice (2009). Analysis tends to focus on finding files of evidentiary value, but system files that can provide a timeline of events are also instrumental in building successful cases (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009).

The collection and processing of digital evidence did not develop in forensic laboratories (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, the beginnings of digital forensics were with police officers, who had some experience with computer systems examining them for potential evidence (2009). As the amount of digital evidence presented to courts grows in size and scope, it too must strive to reach the same standards as traditional evidence (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). The Committee on Identifying the Needs of the Forensic Sciences Community has identified three challenges that face digital forensics:

1. The digital evidence community does not have an agreed certification program or list of qualifications for digital forensic examiners.
2. Some agencies still treat the examination of digital evidence as an investigative rather than a forensic activity.
3. There is wide variability in and uncertainty about the education, experience, and training of those practicing this discipline (2009).

Courts have also presented legal challenges to the collection of digital evidence by adopting differing evidentiary rules between jurisdictions (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009).

The processing of digital evidence creates not only reports, but also discovers files, documents, and pictures that may have investigative value (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). As noted by Barbara, there is variation between organizations in the handling of this potential evidence (2012). Some agencies treat the files as exhibits, while others may classify them as potentially derivative requiring a chain of custody (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). With varying rules for the collection and preservation of digital evidence, adopting an agreed set of standards will be a formidable challenge (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009).

Challenges for the examiner. As noted by the Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, accreditation is typically thought of as something bestowed upon the lab; however, a lab is only as accurate as the personnel operating it are (2009). There are calls for minimum standards in education and training for staff working in accredited facilities (Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, 2009). Through cross-examination in court, an examiner's competency is tested, and the success of the case can hinge upon the examiner's testimony (Barbara, 2012). As noted by Barbara (2012), courts as well as the forensic science community must adopt standards that can answer some issues facing the reliability and competency of practicing examiners. Some of the concerns facing examiners include:

- Was the digital evidence tainted or compromised regarding how it was collected and where it was stored?
- Is the chain-of-custody complete and accurate?
- Is on-the-job training alone sufficient to qualify the examiner as an expert?
- Is the case file documentation complete and detailed such that another examiner can recreate the results of the examination(s)?
- Is the examiner competent to perform the examination(s)?
- Was the examiner proficiency tested (Barbara, 2012)?

Examiners must provide credible and complete answers to address these concerns (Barbara, 2012). As explained by Barbara, depending on the jurisdiction, examiners need to meet legal requirements for classification as an expert in the eyes of the court (2012). The pressing issue for the judicial system is, what standards are in place for the digital forensics community that successfully address the concerns stated above (Barbara, 2012)? A path for the successful adoption of widely accepted practices may lie in what other forensic disciplines have done to address these concerns (Barbara, 2012). As explained by Barbara, other disciplines have been able to mitigate concerns through the adoption of a comprehensive Quality Management System (QMS) (2012). A comprehensive QMS system should include documented training programs, examiner competency testing, documented procedures, and using appropriate standards and controls (Barbara, 2012). As noted by Barbara, the QMS can provide a method for delivering quality results that can withstand peer review and courtroom scrutiny (2012).

Challenges for the laboratory. As explained by Barbara, attaining accreditation is a challenging endeavor that takes significant work (2012). There are numerous factors to consider when applying for recognition as an accredited organization (Barbara, 2012). As explained by

Barbara, labs must achieve one hundred percent compliance with all of the applicable clauses in the requirements (2012). One of the many challenges in attaining accreditation is there is no guidance as to which of the 422 clauses are required for each discipline (Barbara, 2012). The applicability of the clauses can be ambiguous between forensic disciplines; it can be difficult for the laboratory staff to determine which of the clauses are required (Barbara, 2012). As explained by Barbara, it is common for organizations to misinterpret a clause causing an oversight or misunderstanding (2012).

Some laboratories will review the documentation of other organizations' and tailor their documentation in a similar manner (Barbara, 2012). Barbara explains using another organization's documentation can cause pitfalls as each facility has unique characteristics that must be accounted for (2012). The written policies of other labs can be a template but should not be copied verbatim to facilities seeking a new accreditation (Barbara, 2012).

Examiners should take an active role in the accreditation process; typically, they will be reluctant at first (Barbara, 2012). Barbara explains many examiners will have the viewpoint that attaining accreditation is for the lab and does not benefit them personally (2012). Complaints may arise that the process will burden them with more paperwork and take away time for performing analysis (Barbara, 2012). Examiners may feel that requirements of competency testing will question their abilities and skills (Barbara, 2012). As noted by Barbara, by enlisting the examiners in the accreditation process, the likelihood for success increases (2012). Having the examiners understand the reasoning behind the requirements of competency testing will ease the frustrations they may feel in the accreditation process (Barbara, 2012).

Discussion of the Findings

The purpose of this research was to assess the integration of civilian computer forensic examiners in law enforcement criminal investigations. How are sworn officers trained to handle complex digital evidence in local agencies? What challenges are present for agencies when integrating civilian staff? What obstacles prevent local agencies from pursuing accreditation for computer forensic laboratories?

Training of forensic examiners varies greatly between organizations. Some law enforcement agencies have adopted training and educational programs for their staff while others have relied on "on the job training." Jurisdictions that have adopted popular forensic software such as EnCase will typically send examiners to software specific training.

Local law enforcement agencies are struggling with the transitional nature of promotions and reassignments within their organizations. The almost constant state of change creates serious challenges for departments to keep qualified staff available to process digital evidence. Gaining proficiency in working with digital evidence can take years to achieve. Because of the special skills required to perform forensics analysis, staff attrition is a burden for almost all law enforcement organizations.

Compounding the challenges that agencies face with transitional staff are the vast amounts of devices that can contain potential digital evidence. Organizations need to adopt methods that allow competent staff to be available to process digital evidence. Staff that has not received proper training can no longer examine the evidence due to its complexity.

As noted by Reyes, many in law enforcement feel that the computer investigator need not be a computer expert to explain what they found while examining digital devices for potential evidence. Testifying in court about findings on a computer without a solid understanding of how

and why the evidence exists leaves the door open for potential challenges by the defense. Reyes explained that there are times the defense would not question testimony presented because it was not understood.

With the common occurrence of digital evidence in the judicial system, consider the consequences of an examiner with little formal training meeting defense council that was an expert in digital evidence. Cross-examination from an expert asking questions that an examiner struggles to answer can have an adverse effect on the jury. An examiner working in a team environment with formal training and experience will be better prepared to deal with defense council challenges.

The team environment will allow sworn personnel to gain insights into the complex digital world through their civilian counterparts. While working with a team of sworn staff, the civilian examiner will gain knowledge of investigative techniques and insights into the challenges that face law enforcement. The team approach allows the expertise of both sides to come together to process digital evidence in a more efficient and accurate manner.

Law enforcement agencies need to accept that digital evidence should be examined by staff that has had documented training, are competent, and have demonstrated an ability to produce accurate reports. Organizations should not discount the importance of processing digital evidence for the sake of better funding traditional law enforcement functions. Digital evidence plays a part in almost every case brought to court.

To help with budgetary challenges, departments can take advantage of the various training provided by federal agencies such as the W3C. Sending officers to training will give staff the confidence and training to perform their job well. An examiner with an in depth understanding of the subject matter can deliver courtroom testimony with authority.

Despite the availability of free training, law enforcement officers are still lagging behind in digital forensics training. Smaller agencies do not have enough staff trained to process digital evidence and should use regional laboratories to assist where appropriate. Until the agencies realize the importance of proper training, there will be greater chances for inaccurate evidence presented to the court system.

Superiors within law enforcement agencies should explore the benefits of adding civilian examiners to help alleviate the backlog of digital evidence. The literature reflects many of the obstacles presented with the integration are meritless and do not serve the best interests of the department's communities. Unions should be working with agencies to allow the acquisition of the best and most qualified staff to perform analysis of digital evidence. Managers should also work with sworn staff, so that changes to culture and paradigm are more likely to be accepted.

Incorporation of the thoughts of the existing sworn staff and taking steps to address areas of concern will give policy and procedural changes a better chance of success. Clearly defining goals, setting timelines, and open communication are further ways to ensure a solid foundation for change. Sworn staff is likely to resist any changes brought on suddenly and without their input. By allowing current staff to help drive the change, there are greater chances for success.

Building a strong team of civilian and sworn personnel will be a challenge, but with planning and a team approach, it is possible. Many agencies such as the FBI and CIA have long struggled with civilian analysts and their law enforcement counterparts getting the same recognition. In many organizations, the benefit of the civilian is not on the same level as their sworn counterpart. Despite civilian analysts providing valuable information to investigate cases, many organizations put most of the focus on traditional police roles.

Activities that have long been the primary focus for officers need to adapt with societal changes in this digital age. It is no longer reasonable to brush aside the importance of digital evidence. Sworn as well as civilian examiners should train together to develop a sense of team and foster a spirit of working together. It is critical that the evidence presented in the criminal justice system is accurate and reliable. It is reasonable to conclude that tension between sworn and civilian personnel would at times jeopardize evidence.

Integration of civilian examiners may cause some personnel to feel that they have not done a good job. Sharing examples of other agencies that have successfully switched to a team approach with digital forensics will help ease the integration process. Details regarding evidence processing times and backlogs can be great examples to illustrate that a shared workload will allow an operation that is more efficient.

Instead of adversaries, an integrated team will view each side as a valuable resource for guidance and advice. The team approach to integrated computer forensics examinations does not aim to replace sworn personnel with civilian staff. Rather, the team approach looks to build upon the strengths and unique skill sets that each side can provide. In general, sworn personnel will have a better understanding of investigative concepts where the civilian side will have more specialized knowledge in the intricate details of electronic evidence creation.

Some agencies have turned to their local citizens to aid in digital investigations and have seen success. Volunteer programs such as the one instituted in Oregon have given the local police a group of qualified and competent candidates to pull from to help with their ever-increasing digital caseload. Potential volunteers come from local businesses, academia, as well as retired computer experts. Based on the success that has occurred in Oregon, local agencies can look for potential civilian examiners at local colleges and universities.

To help with the backlog of evidence and the budgetary challenges that seem to accompany more evidence, agencies may see a benefit from incorporating an internship program. An internship program would foster the growth of a team approach to civilian and sworn personnel working together. Interns would gain valuable experience at the same time helping to ease the burden of processing evidence. Pulling interns from qualified forensics programs would ensure that competent individuals were handling potential evidence.

Digital evidence processed by a civilian examiner is no different from evidence processed by sworn personnel. Just as sworn technicians do not exclusively process DNA and blood evidence, digital evidence processed by a civilian is acceptable in the courtroom. Many jurisdictions have varying requirements for qualifying the admissibility evidence; however, the examiner being a sworn police officer is not required.

The computer forensics community needs a set of standards. Currently, there can be multiple law enforcement agencies operating within the jurisdiction of a court. Each law enforcement organization can have their own varying tools and techniques to acquire digital evidence. Because varying methods are in use for processing digital evidence, juries and attorneys have the burden of deciphering different styles of evidence presented.

The process of accreditation can help foster the development of standards for the computer forensics community. Moreover, accreditation can also foster the development of minimum qualifications and training for examiners. Smaller organizations will find the process of accreditation a formidable challenge. Examiners may give resistance to the idea of competency testing and requiring training; with adequate involvement, examiners can help work towards the goal of accreditation. Accreditation can be a way for the lab to show the local

community that they have taken the appropriate steps to ensure the evidence they process will be as accurate as possible and examined by competent and experienced individuals.

To improve the quality of reliability of digital evidence processing, organizations should adopt a set of standards for how the evidence is collected. Performing analysis with an accepted set of standards allows processing evidence in nearly the same manner as other labs. Evidence collected by different organizations presented to the court will have similar characteristics if accepted standards are used. The importance of examining evidence with standards is a great benefit to cases that involve multiple jurisdictions. Consider cases that involve the sending of contraband images across state lines; allied agencies collecting evidence could easily share information derived in a similar fashion.

Cross-jurisdictional cases are common in the judicial system. With the use of standardized evidence collection, multiple involved agencies can easily share investigative information. Electronic evidence collected based on accepted and published standards would allow multiple agencies to work a case simultaneously and with minimal delays based on the type of data collected.

Gathering, processing, and presenting evidence within a set of standards will improve the admissibility of evidence to the court system. Setting up minimum educational requirements for examiners will ensure the processing of evidence is a sound and scientific manner that gives the least amount of chance for errors. With the rapid influx of electronic devices in the lives of society and the vast amount of information available, it is imperative that competent personnel do the processing. The chance of contamination, mishandling, or presenting inaccurate evidence is too great a risk to leave to “on the job training.”

Digital evidence is complex, and without proper training and experience, faulty presentation of information in court can compromise a case. Evidence presented in the Julie Amero case was inaccurate and misleading. The examiner in the Amero case used nonstandard forensic analysis software, examined the actual hard drive instead of making a copy, and gave inaccurate testimony in the case.

Amero was facing a great deal of jail time if convicted, and her fate was in the hands of an undertrained and unqualified examiner that had no business performing computer forensics analysis. The examiner in the Amero case admitted there was a failure to examine the hard drive for virus or malware activity. Despite the faulty collection of evidence and subsequent examination, the case moved ahead without questioning as to the validity of evidence.

The Amero case is just one example where faulty digital evidence resulted in a conviction. The amount of digital evidence in the court system today leaves little doubt there are likely several more cases with inaccurate evidence. Care must be taken to ensure that inaccurate digital evidence is not presented to the court and examiners are qualified to process potential evidence.

The trial of Casey Anthony is yet another example of missing vital data in a forensic examination that had serious consequences. Analysis of the Anthony machine failed to examine the Internet history of all installed browsers. An examiner with formal training, competency testing, and practicing under a set of standards would be less likely to miss important data.

The potential evidence missed by not performing a full examination of the internet history could have had a powerful effect on the jury. The history from the other browser contained information relating to the circumstances of the murder. The timeline contained within the other browser provided strong evidence that Anthony made incriminating Internet searches.

Because of a breakdown in the methods used for the collection of evidence, this information did not reach the jury.

Digital evidence can have a profound impact in court cases and requires handling in a secure manner with a proper chain of custody. Without proper handling, altering digital information is possible, potentially changing critical evidence in the process. Presenting evidence in court that has the possibility of inaccuracies can open the door to doubt in the minds of the jury. The criminal justice system can better serve the community by adopting clear and accepted standards for processing evidence and training examiners.

Law enforcement organizations will benefit by adopting a team approach to staffing a digital forensics lab. The integration of civilian personnel working alongside sworn staff can provide consistency and a buffer to the near constant turnover rate due to promotions and transfers. Civilians and sworn staff will be able to share their unique perspectives with each other, providing support that lays the foundation to a strong team. Training the sworn and civilian personnel together can promote comradery and teamwork.

Consider the investment in time and resources to train an examiner to competency. Training in computer and digital forensics can take years and several thousands of dollars. Most local agencies do not have budgets or staffing resources to train new sworn personnel on an ongoing basis. Adopting a blended approach with digital evidence processing will ease the budgetary and personnel constraints that typically affect local law enforcement agencies.

Departments that adopt a team approach will see the efficiency and accuracy of their investigations increase. The team approach allows a buffer for the common problem of sworn staff transferring out of specialized assignments. Working together, staff can share information and experiences that can help keep departmental operations running smoothly. The team

approach allows for employees to advance in their careers without placing undue stress on the department or employees.

There is a common culture in law enforcement that the civilian analysts are not able to do "police work." This misconception propagates through feelings civilians are unable to handle evidence, are incapable of testifying in court, or there is simply tension between sworn and civilian personnel. These challenges are meritless, as several law enforcement agencies have used civilian laboratory analysts for a significant time in other disciplines such as DNA.

Using qualified civilian staff is imperative for the success of a team approach. Inserting unqualified civilian examiners into a lab with qualified sworn personnel will further fuel the difficulties that typically exist between sworn and civilian staff. To achieve success with the team approach, civilian examiners will need to be able to provide valuable skills and abilities to the department's current operations.

As noted by Scott, the FBI now trains civilian analysts along with their sworn counterparts (2015). Local agencies can reap the same benefits by adopting similar practices by promoting teamwork. The team approach to digital evidence cannot succeed without a professional bond between the civilian and sworn personnel. When sworn personnel and civilian staff can leverage the unique skillsets of their varied backgrounds, an integrated team approach will be a great benefit to the department.

Questions often arise when jurisdictions allow the use of civilians in tasks traditionally performed by sworn personnel. Using civilian computer examiners is no different from using civilians to process blood samples. There is no expectation that all personnel working in a department's crime lab are sworn law enforcement officers.

Despite the success of using civilian forensic examiners in disciplines such as toxicology, many agencies continue to question using civilians to process digital evidence. Courts will accept evidence processed by civilian examiners when presented in a sound and scientifically accepted process. The integration of civilian and sworn examiners is a benefit to departments that are facing backlogs of evidence to be processed. Civilian examiners bring specialized skills and training that can complement the skills and training of sworn staff.

Departments can alleviate the burden of transitional personnel by augmenting forensic operations with civilian personnel. Civilian staff members tend to transfer out of positions less frequently than their sworn counterparts do. Keeping consistent practices in the lab will aid in developing procedures for accreditation when appropriate.

Recommendations

Agencies should focus on attaining accreditation if possible. Laboratory accreditation will lay the foundation for sound and accepted practices that produce accurate and quality results. The challenges of accreditation are outweighed by the benefit of reaching this goal. Accreditation will require organizations to test personnel for competency, use accepted practices, and document policies and procedures.

Some personnel may show resistance to the idea of accreditation. Allowing staff to take an active role in the process can be a catalyst in driving positive change. Laboratory staff should be involved in the planning and development of the accreditation plan. As noted by Young, do not assume personnel will see the benefits of changing current operations (2006).

The use of accredited facilities will provide a buffer to procedural challenges presented by opposing attorneys. By using industry standard tools and techniques with documented methods, the ability to restrict the presentation of evidence in court will be reduced. Opposing

counsel will have greater difficulty questioning procedures when they are consistent and reliable. An examiner testifying in court from an accredited laboratory will be presenting evidence from a position of authority and recognition. Accreditation not only sets a high standard for accuracy for the laboratory but also to the staff employed there.

Local law enforcement agencies should take advantage of the free training provided at the federal level. As technology continues to evolve and change the way society communicates, the tools and methods for gathering and processing digital evidence will need to adapt to fit these needs. The need for examiners to remain competent and abreast of new trends in technology will continue to be necessary for quality results in the digital forensics community.

Despite the argument from Reyes (2007), that defense attorneys seldom question digital evidence in court, examiners should be prepared to defend their work with a sound technical understanding. Examiners need to have a current working knowledge of the operations that create potential evidence on digital devices. While a detective does not need an advanced degree in computer science to perform basic examinations, formal training should be required. Having an integrated team of civilians with advanced degrees working alongside sworn personnel will provide the best possibilities for accurate examinations.

Too often detectives rely solely on the abilities of the forensic software to perform an examination. It is bad practice to depend upon the defense attorney to forego questioning of the methods and procedures used in a forensic acquisition. Detectives should welcome cross-examination to further detail the accuracy and reliability of their work. The need for qualified individuals in digital evidence will fuel the increase in expert witnesses available for the defense, making cross-examination vital in the success of courtroom testimony. No longer will defense attorneys simply not question the process in which digital evidence is collected.

Law enforcement agencies can no longer leave the processing of digital evidence in the hands of undertrained and unqualified individuals. Almost all cases brought to court have digital evidence components. Digital evidence can have serious consequences on the lives of the accused; properly processed digital evidence will prevent issues with courtroom questioning.

As training methods and policies increase on the prosecutorial side so too will training and understanding grow on the side of the defense. Law enforcement agencies must keep up to date on the rapidly changing landscape of digital evidence. Failing to adopt standards and achieve accreditation will be a disservice to the communities in which law enforcement agencies serve.

Instead of seeing the process of accreditation as a burden, personnel should be encouraged to view the process as a benefit. The process will be challenging but the reward of documented policies and procedures can provide clear guidelines to processing evidence. These methods will provide consistency in the manner in which evidence is processed and presented to the court. Consistent methods and procedures can prevent lines of questioning of why methods vary form case to case.

Working with unions, current sworn personnel, and civilian staff to develop a blended team environment for digital evidence is the recommended approach. Staying with the status quo will further compound the evidence backlog problem that many local law enforcement agencies are facing. Working together is the approach that can bring positive change quickly and with least expense to organizations looking to better their digital evidence paradigm.

Future Research Recommendations

Technology will continue to evolve at a rapid pace, and research will need to keep up. Law enforcement and the criminal justice system will depend on future research to find new and innovative ways to gather and process evidence. With the widespread use of encryption and a greater sense of privacy, new methods to deal with the challenges of encryption need development. Consider cases of missing persons with encrypted smartphones; does privacy outweigh the safety of possibly endangered individuals? Finding a balance of privacy and the ability for law enforcement to conduct criminal investigations is a delicate situation to balance. Privacy groups lobby for greater protection against government intrusion, while the government claims that encryption protocols are making it nearly impossible to investigate certain cases. Compound the challenges faced by encryption with the necessity to conduct investigations across state and many times international lines, and it quickly becomes apparent that there is a need for international agreements on how to handle digital evidence.

There are different protocols that laboratories can use to gain accreditation some of which are becoming obsolete in favor of international based standards. The international standards can prove to be more of a challenge especially for smaller organizations. The future may see that smaller facilities are closing due to being unable to gain accreditation under the new international paradigms. Computer forensics laboratories will need to adapt and evolve on pace with the changing technology. If an organization is unable to keep up with changes in industry standards, the current backlog of digital evidence will continue to be a pressing concern for the criminal justice system.

What Challenges do Encrypted Devices Create for Law Enforcement?

Encryption on devices of missing persons can create a real burden for police investigations. Cellular phones can help investigators to determine places and locations that an individual may have visited as well as the people that the individual may have been in communication with. These critical details are unable to help investigators if the user has encryption on the device.

The recent events in San Bernardino, California highlight some of the challenges that face law enforcement in regards to devices with encryption. In this instance, two suspects had smartphones with encryption enabled. The FBI attempted to retrieve data from the phones and was unsuccessful. The FBI then attempted to negotiate the help of the phone manufacturer who refused to disclose how to bypass the phones security features. The FBI resorted to the courts to force the manufacturer to disclose how the phone worked. Just before the court ruling, the FBI found a vendor that was able to bypass the security of the phone at a considerable cost to the government.

Are there avenues that can keep the privacy concerns of citizens satisfied while at the same time allowing police investigations access to encrypted information? Successfully implemented encryption methods would be unreasonable to break with brute force methods. Based on the reliability of encryption protocols, the only methods that can bypass encryption in a reasonable amount of time are software and hardware exploits; manufacturers will patch these exploits as soon as possible. Relying on exploits to bypass encryption is not a solution for the long term, as these methods do not last long after public disclosure. Finding a balance between security and privacy is an area that could benefit from additional research.

What Concerns do International Accreditation Standards Present for Currently Accredited Labs?

Accreditation awards are for a defined period of time after which it is necessary to reapply. Laboratories that receive accreditation under a legacy program will need to transfer to an international program in the future. Accreditation is a challenge for any organization. There are numerous clauses where one hundred percent compliance is required.

Accreditation is something that all labs should pursue. Changing to an international set of standards will be an area of concern for many facilities. Determining which clauses are required for each discipline and determining why guidelines are non-existent is something that many labs could benefit from. Research into the areas of how accredited labs have overcome the struggles of changing to an international set of standards can assist more laboratories in gaining accreditation.

How are Anonymizing Browsers (TOR) Affecting Forensic Investigations?

Anonymizing systems such as TOR were originally developed for use behind the lines of oppressive governments. The use of TOR has grown beyond the borders of nations and is now in use worldwide. Anonymizing browsers are used for legitimate reasons but have also grown popular with individuals wishing to hide their identity. Systems such as TOR make it difficult to track a person on the Internet making the investigation of criminal activity difficult.

The Internet has allowed groups of people with similar interests to find and communicate with each other from all parts of the world. Internet chat rooms allow people to share ideas freely and at little to no expense. The ease of communication and low cost has a dark side as well; the Internet has allowed criminals from all parts of the globe to find and talk with each other as well.

Child exploitation is one area that has seen significant growth due to the advances in technology from systems like TOR.

TOR can protect the illegal trade and distribution of contraband images of children. The system presents difficulties for law enforcement agencies conducting criminal investigations. Users can trade in illegal goods and services knowing the hardships that police agencies will face in investigating their activities. Further research is needed on the effects these systems have and how they can be mitigated.

Conclusion

Law enforcement agencies are facing complex digital evidence without enough qualified personnel to handle this ever-growing task. Law enforcement organizations are oftentimes ill prepared to process digital evidence accurately. Inaccurate and incomplete processing of digital evidence can have a profound impact on the outcome of a case.

Society is producing digital information at an alarming rate. This information has the potential to be used as evidence in civil as well as criminal court cases. Many law enforcement agencies are struggling with a backlog of digital evidence to be processed and do not have enough qualified personnel to handle this task.

Some agencies have adopted the use of civilian examiners to ease this burden with great success. By building a strong team of sworn and civilian personnel, departments can process evidence efficiently and accurately. The team approach is a benefit to both civilian and sworn personnel as each side brings unique experience and skills to the challenges of increasingly complex digital evidence.

References

Alva, A., & Endicott-Popovsky, B. (2012). Digital Evidence Education in Schools of Law. *Journal of Digital Forensics, Security and Law*, 75-88.

Arizona Department of Public Safety. (2014, July 27). *Computer Forensic Analyst* . Retrieved from Arizona Department of Public Safety: http://agency.governmentjobs.com/azdps/default.cfm?action=specbulletin&ClassSpecID=868632&headerfooter=0

Barbara, J. J. (2012, Feb 23). *ISO/IEC 17025:2005 Accreditation of the Digital Forensics Discipline.* Retrieved from Forensics Magazine: http://www.forensicmag.com/article/2012/02/isoiec-170252005-accreditation-digital-forensics-discipline

Carlton, G. H., & Worthley, R. (2010). Identifying a Computer Forensics Expert: A Study to Measure the Characteristics of Forensic Computer Examiners. *Journal of Digital Forensics, Security and Law*, 5-19.

Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council. (2009). *Strengthening Forensic Science in the United States: A Path Forward.* Washington D.C.: The National Academies Press.

County of San Bernardino. (n.d.). *Classification Specifications*. Retrieved from San Bernardino County Human Resources: http://cms.sbcounty.gov/hr/EmploymentClassification/JobDescriptions.aspx

FBI. (2011, August). *Stories*. Retrieved from fbi.gov: https://www.fbi.gov/news/stories/2011/august/intelligence_081811

Federal Law Enforcement Training Centers. (n.d.). *Training At FLETC*. Retrieved from Federal Law Enforcement Training Centers: https://www.fletc.gov/training-catalog?combine=computer&field_locations_offered_value=All&items_per_page=20

Flynn, R. (2015, May 3). *Civilians seen as option for forensic units; union disagrees*. Retrieved from New Haven Register News: http://www.nhregister.com/article/NH/20150503/NEWS/150509854

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence.* Santa Monica: RAND Corporation.

Guidance Software. (n.d.). *Courses*. Retrieved from Guidance Software: https://www2.guidancesoftware.com/training/Pages/all-courses.aspx

Harris v. State, 401 S.E.2d 263 (260 Ga. 860 1991).

Harrison, G., Heuston, G., Mocas, S., Morrissey, M., & Richardson, J. (2004). High-Tech Forensics . *Communications of the ACM*, 49-52.

Murphy, J. P., & Fontecilla, A. (2013, January 14). *Social Media Evidence in Criminal Proceedings: An Uncertain Frontier*. Retrieved from Bloomberg Law: http://www.bna.com/social-media-evidence-in-criminal-proceedings-an-uncertain-frontier-by-justin-p-murphy-and-adrian-fontecilla/

Musthaler, L. (2014, January 2). *The National Computer Forensics Institute provides sorely needed training for cops*. Retrieved from Network World: http://go.galegroup.com/ps/i.do?id=GALE%7CA354824169&v=2.1&u=nysl_ce_uticacol&it=r&p=AONE&sw=w&asid=7ec964901d97357f65661a1860eb8a87

National Commision on Forensic Science. (2016). *Recommendation for the Accreditation of Digital and Multimedia Forensic Science Service Providers.* Washington D.C.: Department of Justice.

National White Collar Crime Center. (n.d.). *Cybercrime Courses*. Retrieved from National White Collar Crime Center: https://www.nw3c.org/training/cybercrime

New Jersey State Police. (n.d.). *Cyber Crimes Unit*. Retrieved from New Jersey State Police: http://www.njsp.org/division/investigations/cyber-crimes.shtml

Reyes, A. (2007). *Cyber crime investigations : bridging the gaps between security professionals, law enforcement, and prosecutors.* Rockland: Syngress.

Scott, S. (2015, March 26). *C.I.A. Officers and F.B.I. Agents, Meet Your New Partner: The Analyst* . Retrieved from The new York Times: http://www.nytimes.com/2015/03/27/us/cia-officers-and-fbi-agents-meet-your-new-partner-the-analyst.html?_r=2

U.S. Const. amend. VI. (n.d.).

Young, W. (2006, July). Effecting Change: Avoiding the Pitfalls. *The Police Chief.*