The Bill Blackwood
Law Enforcement Management Institute of Texas

Digital Evidence Recognition, Preservation, and Collection: The Need for Standardized Training for First Responders

An Administrative Research Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Jason T. Bailey

The University of Texas Southwestern Medical Center at Dallas
Police Department
Dallas, Texas
November 2005

ABSTRACT

The growing number of crimes being committed by criminals who utilize computers and other technology to help them facilitate their crimes has caused law enforcement to adapt their tactics in order to successfully prosecute them. Currently there are no specific standards to direct law enforcement in this endeavor, particularly with respect to the abilities of the first responder called to a digital crime scene. Standardized training is necessary for first responders so they are prepared to recognize potential sources of digital evidence, collect that evidence, and preserve it for successful criminal prosecution. To study this issue, a survey was sent to law enforcement agencies throughout the Dallas / Ft. Worth Metroplex area. The results of this research indicated that a majority of law enforcement officers feel they should be given standardized training in the recognition, collection, and preservation of digital evidence in order to keep up with the criminal they are pursuing. In order to successfully standardize this training for Texas law enforcement officers, criteria must be met that takes into account the lessons learned up until this point with the flexibility to adapt to future changes.

TABLE OF CONTENTS

INTRODUCTION

Since the introduction of the personal computer, there has been a dramatic evolution in the way people use them. At their inception, the general public viewed computers as tools that were used in the business sector to increase productivity. In today's society, however, the utilization of computers for work and recreation has become commonplace for a large number of people. The technology available today, including the ability to network multiple computers together in order to communicate, collaborate on ideas, or locate resources that would not otherwise be accessible, is a major reason computer usage is this prevalent. The proliferation of cellular telephones, Personal Digital Assistants (PDA), digital cameras, and other technological devices has extended well beyond the segment of the population who, historically, had easy access to a computer. The cost of ownership for computers and these other electronic devices has also lowered to a point where far more people are able to afford the benefits of this technology.

The people who perpetrate crimes have found the use of computers to be beneficial to them as well. When a computer is used to commit a crime or to aid in the commission of a crime, it creates a special problem for law enforcement by creating digital or electronic evidence. In most cases, this evidence must be collected and examined by a specially trained computer forensics examiner so that its integrity can be maintained throughout the entire process. Most first responding law enforcement officers are trained in the methods of recognizing, preserving, and collecting physical evidence, but little standardized training is devoted to the special needs of recognizing, preserving, and collecting digital evidence. Digital evidence is inherently very fragile in

nature, and an overzealous officer could unintentionally alter or destroy the evidence of a crime by not receiving some standard and accepted specialized training in this field.

Law enforcement should standardize the training and procedures used by first responding officers to recognize, preserve, and collect digital evidence when necessary. Even though most law enforcement agencies will have access to someone specifically trained to collect and analyze digital evidence, it is important for first responding officers to be able to accurately identify the need to get this person to the crime scene before any evidence is lost. The standardized procedures and training for first responders should include a basic recognition of the devices typically used by criminals to commit crimes or contain evidence pertinent to the investigation of a crime. A first responding officer should know the importance of preserving possible evidence for analysis by a trained forensic examiner, whether that person is a member of the officer's department or someone from an outside agency. Although most first responding officers will not be responsible for the collection of devices containing electronic evidence, they should be knowledgeable of the accepted procedures for doing so without altering or destroying data.

Very little research is available that concentrates on the effectiveness of first responders in identifying and preserving digital evidence. Facts supporting the standardization of the training and procedures used by first responding officers to recognize, preserve, and collect digital evidence will primarily come from books, journals, and Internet publications concerning this topic. Since so little research is readily available, a survey was used to gauge the attitudes of law enforcement officers around the state of Texas.

The intention of this research is to show that a need exists for law enforcement to standardize the training and procedures used by first responders to recognize, preserve, and collect digital evidence. To reach this conclusion, it will be necessary to 1) examine the potential pitfalls that are unique when dealing with digital evidence collection and preservation, 2) analyze the first responders ability to readily identify potential sources of digital evidence, and 3) look at the accepted methods the first responding officer can utilize to safely preserve the digital evidence for analysis by someone trained in computer forensics, without destroying it in the process.

First responders who are properly trained in standardized procedures to recognize, preserve, and collect digital evidence will assist in the prosecution effort of criminals who use technological devices to commit crimes or as a tool to aid in the commission of a crime. As these devices are used by a wider segment of society on a daily basis, it will be important for law enforcement officers to keep up with the tools available to detect, identify, and stop the criminal element in a technological environment that is consistently changing.

REVIEW OF LITERATURE

When analyzing the issue of standardizing the procedures surrounding the recognition, preservation, and collection of digital evidence, it is important to look at the crime scene where this will occur. Crime scenes are generally very fluid in nature, and often require a first responding officer to focus on several different issues simultaneously. In addition to this, the success or failure of a criminal investigation is often dependent on the actions taken by the first responding officer (Fisher, 1993).

Since the crime scene is often the location where a criminal case is won or lost, the ability for first responding officers to be able to recognize potential sources of evidence and preserve those evidentiary items is invaluable.

Matthew Meyers and Marc Rogers (2004) hypothesize that the lack of standards when investigating computer related crimes needs to be remedied while computer forensics as a discipline is still in its infancy. Meyers and Rogers point out that the lack of standards in the computer forensics field has caused inconsistencies within the judicial system as well (Meyers & Rogers, 2004). While Meyers and Rogers primarily focus their research on computer crime and computer forensics specifically, the same outlook should be applied to other forms of digital evidence as well. One of the important legal issues that Meyers and Rogers focus on is search and seizure laws and how their application in the judicial setting has been impacted by computer related crime. Meyers and Rogers point out that the legality of the search and seizure of digital evidence is typically the first thing to be contested in the judicial process. If the search and seizure was not completed properly, the evidence could be withheld from trial. Meyers and Rogers also delineate an important distinction between standard “non-digital” cases and “digital” cases, in that courts can use precedents to guide the decisions being made about search and seizure issues in these “non-digital” cases. They contend that since digital cases are still emerging with the adoption of new technology, the same precedents cannot be used, causing the courts to focus on the methodology law enforcement utilized during the investigation (Meyers & Rogers, 2004).

In an effort to minimize problems law enforcement might face in court, several Federal agencies have published guidelines for law enforcement agencies to follow when searching and seizing electronic evidence. The United States Department of Energy Computer Forensic Laboratory published a manual entitled First Responder's Manual (n.d.), which is designed to be a guide for the initial responders to a computer incident. Similarly, the United States Department of Justice Computer Crime and Intellectual Property Section published a manual entitled Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2002), which discusses important case law dealing with the issues surrounding search and seizure. The United States Secret Service published a guide entitled Best Practices for Seizing Electronic Evidence (2002), which is a quick reference for law enforcement officers to utilize when faced with searching and seizing digital evidence. Lastly, the Technical Working Group for Electronic Crime Scene Investigation authored a manual entitled Electronic Crime Scene Investigation: A Guide for First Responders (2001), which is also meant to assist state and local law enforcement agencies establish practices and procedures to follow when investigating electronic crime.

All of the publications listed above share similarities, but are intended to be utilized differently. Unfortunately there are enough differences as well to make standardizing procedures difficult (Meyers & Rogers, 2004). One key difference among the listed reference guides is the level of detail that they go into when explaining what to do in different situations. For example, one source explains that floppy disks present within a computer should be removed and packaged separately to avoid damage to potential evidence (Electronic Crime Scene, 2001). None of the other publications go

into as much detail and do not warn the reader of the potential to damage vital evidence. Similarly, one guide explains to press the “down arrow” key should a first responder encounter a screen saver (First Responder’s, n.d.). Another guide suggests never to press and keys on the keyboard because of the potential to alter or destroy evidence. Instead it suggests to move the mouse slightly, and if no change occurs, photograph and document the screen (Electronic Crime Scene, 2001). The differences in the established guides and manuals are significant enough to cause potential problems or challenges in the judicial process.

Recognizing, collecting, and preserving digital evidence requires a certain level of experience and training to accomplish safely. It is commonly recommended for local law enforcement agencies to seek assistance from experts in the field that can assist them should they be needed (Electronic Crime Scene, 2001). The recognition or identification of potential digital evidence is the first step in the investigative process and can be crucial to the successful outcome of an investigation (Best Practices, 2002). The next step in the process is the collection of the identified digital evidence. The procedures used in the collection of digital evidence are covered most frequently in published literature because of the importance these procedures can have on the entire investigation. When problems occur in this stage of the process, the evidence will be closely scrutinized in the judicial process (Ciardhuáin, 2004). Proper preservation of digital evidence is also vital to the successful prosecution of a criminal case. First responders should document the chain of custody on digital evidence much like they would on other forms of physical evidence. Because of the fragile nature of the electronic hardware, special attention should be made to ensure that the evidence is

safe from environmental factors that could damage or destroy it (Electronic Crime Scene, 2001).

The special concerns associated with digital crime scenes are enough to require a certain level of training for officers that might be involved in the process of identifying potential sources of evidence, collecting that evidence without destroying it in the process, and safely preserving the digital evidence so that it remains viable when it comes time for criminal prosecution. Are the published guidelines mentioned above that outline best practices for law enforcement agencies to follow good enough in most cases?

METHODOLGY

Is there really a need to standardize training for first responders in the area of digital evidence recognition, collection, and preservation? It is believed that there is a deficiency in the level of training for all officers and the need for standardized training exists, particularly for first responders. To help answer this question, a brief questionnaire was sent to subscribers of the Crime Analyst Email Listserv, which is an email based mailing list used to collaborate about crime trends and disseminate other valuable information to subscribers. At the time the survey was sent, the member list was comprised of six hundred eighty-three law enforcement officers and Crime Analysts representing one hundred seventy-one law enforcement agencies throughout the state of Texas. The listserv was started by a Crime Analyst from the Irving Police Department, and quickly spread in popularity by word of mouth. Because of this, most of the subscribers are affiliated with law enforcement agencies in the Dallas / Ft. Worth

Metroplex area. Of the six hundred eighty-three people subscribing to the listserv, forty-two people responded to the survey (6.1%) from thirty-seven unique law enforcement agencies (21.6%).

The answers to the survey questions were evaluated and analyzed independently. The respondents were asked to provide basic demographic information such as their name, department name, and number of sworn officers their department was authorized to employ. The survey then asked questions that would help quantify the respondent's level of training and the level of training offered by the respondent's employer. The survey also asked subjective questions about how the respondent felt about standardizing training through the Texas Commission on Law Enforcement Officer Standards and Education.

FINDINGS

There was a diverse difference in the size of the law enforcement agencies that responded, ranging from four officers on the low end to twenty-nine hundred officers on the high end. The respondents represented twenty-eight unique municipal law enforcement agencies (75.7%), three hospital districts (8.1%), three educational institutions (8.1%), one airport (2.7%), one state law enforcement agency (2.7%), and one federal law enforcement agency (2.7%).

Three survey questions asked the respondent to answer based on current training within their agency. The first question asked if their agency employed anyone trained in the collection and preservation of computer or other technological evidence. The responses to this question were evaluated based on unique agency responses.

The answers from respondents from the same agency were compared with each other. When the answer was the same, the similar responses were counted as one answer. When the answer was different, the differing responses were not included in the results. Of the thirty-seven unique law enforcement agencies represented by the respondents, thirty-six answers were included in the results for this question. Nineteen respondents (52.8%) reported that their agency did employ someone trained in the collection and preservation of computer or other technological evidence, while seventeen respondents (47.2%) reported that their agency did not employ anyone trained in the collection and preservation of computer or other technological evidence. The second question asked if the respondent's agency offered any training to patrol officers or first-responders so that they were able to recognize potential sources of evidence relating to computers or other technological devices. The responses to this question were evaluated in the same manner as the previous question. Of the thirty-seven unique law enforcement agencies represented by the respondents, thirty-five answers were included in the results for this question. Eleven respondents (31.4%) reported that their agency did offer training to patrol officers or first-responders, while twenty-four respondents (68.6%) reported that their agency did not offer any such training. The third question was subjective in nature, so all responses were evaluated. The survey asked if the respondent had received any training specific to the collection, preservation, or recognition of computer or technological evidence. Of the forty-two total respondents, twenty-three (54.8%) reported receiving specific training in this field, while nineteen respondents (45.2%) reported not receiving any specific training. Since a majority of the participants of the Crime Analyst Email Listserv work in an investigative function for

their agency, it is not surprising that a majority of the respondents reported receiving specific training in this field.

Two survey questions asked the respondent to answer based on their feeling about the standardization of training in this field and whether or not this training should be required for all officers. The first questions asked if the respondent felt that the Texas Commission on Law Enforcement Officer Standards and Education (TCLEOSE) should standardize training in the collection, preservation, or recognition of computer or technological evidence. Since this question asks for the officer's opinion, all responses were evaluated. Of the forty-two respondents, thirty-nine (92.9%) felt that TCLEOSE should standardize training in the collection, preservation, or recognition of computer or technological evidence, while three (7.1%) felt that TCLEOSE should not standardize training in this field. A follow-up question to this asked whether respondents who answered yes to the previous question thought this standardized training should be required for all officers. This question is also subjective, so all responses were evaluated. Of the forty-two respondents, twenty-three (54.8%) felt that this standardized training should be required for all officers, thirteen (31%) thought that it should not be required, and six (14.3%) did not respond to the question.

The last survey question asked respondents to rate their department's ability to investigate an offense requiring the collection of computer or other technological equipment without the assistance from an outside agency. The rating scale used for this question ranked a value between one and five, where one represented their department was not at all capable of investigating an offense of this nature without assistance from an outside agency, and five represented that their department was very

capable of investigating an offense of this nature without assistance from an outside agency. Since this was a subjective question all responses were evaluated. Of the forty-two respondents, eight (19%) rated their departments ability to investigate these offenses at the lowest level, eight (19%) rated their department at a level two, thirteen (31%) rated their department at a level three, eleven (26.2%) rated their department at a level four, one (2.4%) rated their department at a level five, and one (2.4%) did not respond to the question.

CONCLUSION

With the proliferation of computers, cellular telephones, PDAs, digital cameras, and other technological devices in today's society and a trend of continued growth in the future, there will be a continual need for law enforcement to adapt their methodology to keep up with the criminal element that is also benefiting from the use of these devices. Today a larger number of criminals are utilizing technology to commit their crimes (Searching and Seizing, 2002).

Taking this into account, is there really a need to standardize training for the first responders that will be tasked with processing these digital crime scenes? Since there are no set standards for first responders to follow when faced with a crime scene containing digital evidence, it is the purpose of this research to show that a need for standardized training exists. It is believed that first responders in most law enforcement agencies lack the level of training required to recognize potential sources of digital evidence, collect that evidence in an appropriate manner, and preserve the evidence for future criminal prosecution.

The results of the research showed that less than one-third (31.4%) of the respondent's law enforcement agencies offered any training for first responders to help them recognize potential sources of evidence relating to computers or other technological devices. Similarly, over two-thirds (69%) of the respondents rated their department's ability to collect computer or technological evidence between "somewhat capable" and "not at all capable", with over one-half (55.2%) of those falling below the "somewhat capable" category. Slightly less than one-half (47.2%) of the respondents reported that their department did not employ anyone trained specifically in the collection and preservation of digital evidence. The results of this research indicate that most law enforcement agencies are not prepared to meet the unique demands associated with the proliferation of crime committed with some type of technological device. An overwhelming majority (92.9%) of the respondents felt that training should be standardized in this field, while over one-half (54.8%) of the respondents felt that this standardized training should also be required for Texas law enforcement officers.

The results of the research support the argument that there is a definite need for standardized training for first responders when it comes to recognizing, collecting, and preserving digital evidence. The limited amount of research available on this topic also supports the need to standardize training and resources available in the law enforcement and scientific communities. Since this is such a new field and the courts are still deciding the appropriate course of action relating to search and seizure, as well as procedural issues, now is the time to standardize this training (Meyers & Rogers, 2004). It is difficult to specify exactly what this standardized training should entail, but these standards will be addressed individually.

The standardized procedures and training for first responders should include a basic recognition of the devices typically used by criminals to commit crimes or contain evidence pertinent to the investigation of a crime. A first responding officer should know the importance of preserving possible evidence for analysis by a trained forensic examiner, whether that person is a member of the officer's department or someone from an outside agency. Although most first responding officers will not be responsible for the collection of devices containing electronic evidence, they should be knowledgeable of the accepted procedures for doing so without altering or destroying data.

While the number of guidelines and manuals that have been published previously are a good starting point, there is not any one standard that all of them follow. This only creates confusion and leads to potential problems when it is likely too late to address the issue. The adopted TCLEOSE standards should fall within the search and seizure guidelines that have already been established in previous court cases, while remaining flexible enough to address future issues that arise in this developing field. Because of the inherent fragility of digital evidence and the ease with which the evidence could unintentionally be altered or destroyed if not collected properly, first responders need to be educated to avoid making mistakes that could jeopardize the ability to successfully prosecute a criminal case.

The criminal element has adapted and taken advantage of the influx of technology in modern life and it is time for law enforcement to address the issue as well. Law enforcement should standardize the training and procedures used by first responding officers to recognize, preserve, and collect digital evidence when necessary.

REFERENCES

Ciardhuáin, S. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence, Volume 3* (Issue 1). Retrieved September 15, 2005 from http://ijde.org/docs/ociardhuain.pdf.

Department of Energy Computer Forensic Laboratory. (n.d.). First Responder's Manual. Retrieved June 18, 2002, from http://www.linuxsecurity.com/resource_files/documentation/firstres.pdf

Department of Justice Computer and Intellectual Property Section. (2002). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Retrieved September 4, 2002 from http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf.

Fisher, Barry A.J. (1993). Techniques of Crime Scene Investigation (5th Edition). Boca Raton, FL: CRC Press, Inc.

Meyers, M., & Rogers, M. (2004). Computer Forensics: The Need for Standardization and Certification. *International Journal of Digital Evidence, Volume 3* (Issue 2). Retrieved September 15, 2005 from http://ijde.org/docs/meyersrogers_ijde.pdf.

Technical Working Group for Electronic Crime Scene Investigation. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. *NCJ 187736*. Retrieved June 18, 2002, from http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

United States Secret Service. (2002). Best Practices for Seizing Electronic Evidence. Retrieved September 15, 2005 from http://www.secretservice.gov/electronic_evidence.shtml.

APPENDIX

\

LAW ENFORCEMENT MANAGEMENT
INSTITUTE OF TEXAS
ADMINISTRATIVE RESEARCH PAPER SURVEY

1. Name:
2. Department:
3. Number of sworn officers authorized in your department:

4. Does your department employ anyone trained in the collection and preservation of computer or other technological evidence?

☐Yes ☐No

5. Does your department offer any training for patrol officers or first-responders so that they are able to recognize potential sources of evidence relating to computers or other technological devices?

☐Yes ☐No

6. Have you received any training specific to the collection, preservation, or recognition of computer or technological evidence?

☐Yes ☐No

7. Do you think that TCLEOSE should standardize training in the collection, preservation, or recognition of computer or technological evidence?

☐Yes ☐No

8. If you answered “Yes” to question 6, do you think this training should be required for all officers?

☐Yes ☐No

9. Overall, how would you rate your departments ability to investigate an offense requiring the collection of computer or other technological equipment without assistance from an outside agency.

☐1	☐2	☐3	☐4	☐5
Not at all Capable		Somewhat Capable		Very Capable

Comments:

Email completed surveys to jason.bailey@utsouthwestern.edu
(don’t forget to attach this document)
or fax to: