

By Warren Harrison, George Heuston,
Sarah Mocas, Mark Morrissey,
and John Richardson

F HIGH-TECH FORENSICS

*An Oregon police department
successfully enlists tech-savvy citizens
to serve as police reserve specialists.*

Today, the overwhelming majority of police officers are unprepared to deal with crimes involving either the direct or the indirect use of computers. The average officer receives little or no instruction in computer forensics during training at the Police Academy. Local digital forensics labs tend to be staffed by detectives who have been assigned to a high-tech crime unit with limited specialized preparation. Given the financial constraints most local law enforcement organizations work under, this situation is unlikely to change. Clearly, if electronic evidence is to be used in developing criminal cases, there is a need for law enforcement to explore different paradigms for processing it.

The Hillsboro (Oregon) Police Reserve Specialist (PRS) program provides suitably qualified individuals from the community an opportunity to assist the local police in criminal investigations. The program evolved from the Hillsboro Police Department's (HPD) initial concept to train private-sector experts for emergencies. Under the philosophy that the best preparation is to assimilate a volunteer force through ongoing, active investigations [2], it was quickly discovered the program provided a pool of expertise in areas where police chronically lag behind criminals, specifically where computers and advanced technology are employed as tools in a crime.

As society has become more computerized, we have witnessed an increase in high-tech crimes such as online identify theft and computer hacking, as well as traditional low-tech crimes such as fraud, drug dealing, and larceny that include a good deal of digital

ILLUSTRATION BY PETER AND MARIA HOEY

The focus of PRS training is, in large part, to
FACILITATE CLEAR COMMUNICATION AND UNDERSTANDING
between the reservist and the investigator to exploit their
combined knowledge sets.

evidence. The dramatic proliferation in cases involving digital evidence requires prosecutors and law enforcement agents to deal with artifacts such as computer logs, email, word-processing documents, image files, and so on. Without an understanding of computer technology by the police and prosecutors, many cases may never reach trial and those that do may not lead to recovery of assets or damages. Some estimates of losses due to cyber thieves are as high as \$100 billion, and there is evidence that as many as 97% of these offenses actually go undetected [1].

In the most general sense, the function of a PRS is to augment, broaden, and increase the effectiveness of the police department in its mission to protect the community [3]. The current focus of the program has involved gathering and processing electronically stored evidence, which entails assisting in the entire investigative life cycle—from the preparation and execution of search warrants to preserving and analyzing digital evidence as well as providing expert testimony in court. Reservists also participate in the development of training, policies, and procedures in these areas as well as work with the community to develop educational programs on the safe and ethical use of computer technologies for K–12 students.

Officially, reservists serve as unsworn agents of the police working under the direction and auspices of the HPD. As agents, they have focused and limited authority for use when and where specialized skills are needed. Specifically, all reservists work under the direction of a case officer, who is usually the detective in charge of the investigation.

Digital forensics involves the application of legally sufficient methods, protocols, and techniques to gather, analyze, and preserve computer information relevant to a matter under investigation [4]. From this definition, it follows that not all technically feasible techniques can be legally used to gather evidence. For example, it may not be appropriate to follow Internet connections to machines not specified in a warrant even though it is possible to do so. As technologists,

we continually wonder “Is it possible to do this?” A reservist, however, must ask “Will this activity jeopardize or assist in this investigation?”

As agents of the police, reservists are governed by the Fourth Amendment¹ as well as a variety of federal and state statutes that apply to the search and seizure of digital evidence.² While it is not the reservists’ responsibility to have in-depth knowledge of the law, it is necessary for them to gain a perspective on the legal considerations so their assistance does not jeopardize the prosecution of the case. Reservists must realize that well-constructed warrants are specific and limited in scope and that a search must remain within the technical and defined limits of a warrant. The methods used for seizing and processing data must be defensible in court and not lead to evidence being excluded. The focus of PRS training is, in large part, to facilitate clear communication and understanding between the reservist and the investigator to exploit their combined knowledge sets.

An Example Case

Two reservists were assigned to a felony fraud and forgery investigation. Earlier inquiries to the Washington County District Attorney’s Office responsible for prosecuting the case had cleared the way for the reservists to assist in the investigation. Because representatives from the DA’s Office had participated in the PRS training, they were confident the reservists would contribute to the case in a meaningful way.

The case began with a briefing attended by the detectives assigned to the investigation, two PRS volunteers, and the PRS management coordinator for

¹The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

²U.S. Federal guidelines for search and seizure of computers and data are contained in *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation*. Computer Crime and Intellectual Property Section. U.S. Dept. of Justice; www.usdoj.gov/criminal/cybercrime/s&csmanual2002.htm.

the HPD. The limits of the warrant and types of evidence the detectives were expected to find on the computer systems were outlined. After the briefing, both reservists went to the HPD Forensics Lab, where computers seized earlier in connection to the case were housed. Following best practices, exact images were made of the disk drives so the investigation would not taint original evidence. They then executed searches within the scope of the warrant. After analyzing the contents of the imaged drives, they found forged documents and the programs that produced them. Their findings were carefully documented, including a log of their procedures, in a report to the case detectives for use in prosecution. The case is currently scheduled for trial.

The reservists remain available to the detectives and DA's Office to answer technical questions and follow up with any subsequent searches merited through the development of the investigation. Additionally, the reservists may be asked to testify at the trial regarding their procedures, especially if the defense chooses to challenge the admissibility of the evidence extracted from the computers.

PRSs are by no means experts in every aspect of computing but, to date, they have demonstrated on several occasions how their knowledge and expertise far surpasses that of the normal investigating team. Moreover, reservists are valuable right out of the box; in fact, they have proven to offer more help than was ever anticipated.

Program Boot-Up and Training

The concept of the PRS program was first presented by the Hillsboro Chief of Police at a meeting of a local organization called Computer-Related Investigations, Management, and Education (CRIME). Founded in 1998, CRIME is composed of people from law enforcement, industry, and academia with an interest in computer security and digital forensics. Shortly after the meeting, PRS program applications, vitas, and letters of intent were solicited.

Twelve applicants were eventually selected out of an initial group of 40. The first group consisted of eight people working in the computer/software industry, two of whom had extensive legal backgrounds (one a former deputy district attorney), three computer science academicians, and a retired executive. Individuals were selected based on their technical expertise and their ability to participate in the formation of the program. The expectation was that any applicant was already an expert in some area and their training would primarily cover how to apply that expertise appropriately.

The first group of volunteers, along with represen-

tatives from the DA's Office, assisted the HPD in developing and delivering the initial training. Over a 10-week period, participants received practical training on police procedure and law, including search and seizure, evidence handling, chain of custody, court testimony, privacy issues, conflict of interest, ethics, and communication. The primary objectives were twofold: to teach reservists enough about law enforcement objectives so they would know when to stop and ask questions of the investigators; and to enable the reservists to provide the investigators with enough technical knowledge to ask the right questions of subjects and witnesses. It is this balance that provides both depth of understanding and investigative leverage—crucial aspects in solving complex high-tech cases. Implicit in the objectives is also ongoing training in technology for law enforcement officers so they are best able to utilize the reservist's skills. The process of education is intended to be a two-way street that raises the level of knowledge on both sides.

PRSs commit to a minimum term of two years of service. Most are expected to spend some time in the lab, especially as they become more involved in the program. Some, however, may only need to be available for a quick consultation or in crisis situations depending on their area of expertise

Potential for Replication of the PRS Program

The rapid development of the PRS program can be attributed to several factors. First, the existence of CRIME yielded a group of people from industry and academia that had long-standing interactions with the law enforcement community. Therefore, a high level of communication and trust was in place. Second, the HPD has an ongoing history of extending the boundaries of community policing, especially with respect to technology. Finally, due to the significant presence of many computer and software companies in the Portland area, a large pool of potential volunteers was available.

These unique circumstances made the development of PRS especially smooth, but there is no reason to believe that the program could not be duplicated elsewhere. Probably the key ingredient is the establishment of communications between the technical and law enforcement communities. Traditionally, law enforcement has been reluctant to call on private-sector individuals for assistance in investigations. However, the dramatic increase in cases involving digital evidence combined with the lack of technically skilled officers to process this evidence is creating a different environment.

The PRS training was specifically developed so that

The PRS program has provided a UNIQUE OPPORTUNITY FOR FORENSICS RESEARCHERS TO UNDERSTAND THE OPERATIONAL AND LEGAL CONSTRAINTS placed on investigators in a law enforcement environment.

This provides insight for researchers into the current and potential technical issues encountered by practitioners.

it would be stable, applicable to all future PRS training, and exportable to other agencies interested in duplicating the program.

Near- and Long-Term Impact

While the PRS program is already producing positive results, much more is planned. The next area to address is to review the policies and procedures for obtaining and processing digital evidence. The exponential increase of PC capacities and digital storage require new approaches to searching for relevant information. The connectivity of computers, both locally and to the Internet, will require new techniques for isolating appropriate data. With evidence stored on computers accessed by many users, such as email servers, the courts may not allow the system to be removed, nor data of other users to be copied. The reservists will be analyzing methods and means to focus on only the relevant data, to find that data in a sea of storage, and to minimize time needed to extract it.

The PRS program is expected to have broader impact. Newly developed techniques will raise the level of digital forensics practices. With close cooperation between reservists, experienced police officers, and the DA's office, these new techniques could be essential in creating new case law that will impact locally, regionally, and even across the U.S.

The PRS program has provided a unique opportunity for forensics researchers to understand the operational and legal constraints placed on investigators in a law enforcement environment. This provides insight for researchers into the current and potential technical issues encountered by practitioners.

Social Considerations

The relationship between society and technology is symbiotic and evolving. To date, the advancement of technology has offered huge advantages with minimal personal threat. Organizations like Computer Professionals for Social Responsibility (CPSR) and

the Electronic Frontier Foundation (EFF) have worked diligently to ensure the public and policy makers have a realistic assessment of information technologies and how they affect our civil liberties and our society, but little attention has been paid by the technologically educated community to the impact of technology as it is used in criminal activities. The PRS program is an example of one way in which individuals with technical expertise have an opportunity to play an effective role in the evolving give-and-take between technology and societal demands. ■

REFERENCES

1. Bennett, W. and Hess, K. *Criminal Investigation*. Wadsworth, Belmont, CA, 2001
2. Heuston, G.Z. Police reserve specialists. *Law and Order* (Sept. 2002), 260-263.
3. Hillsboro, OR. Guidelines for the Police Reserve Specialist program. Draft general order.
4. Kovacich, G.L. and Boni, W.C. *High-Technology Crime Investigator's Handbook*. Butterworth-Heinemann, Woburn, MA, 243-244
5. *Merriam-Webster Collegiate Dictionary*. Merriam-Webster Inc., Springfield, MA, 2002

WARREN HARRISON (warren@cs.pdx.edu) is a professor of computer science at Portland State University, and has served as a HPD PRS. He is currently a deputy sheriff with the Clackamas County Sheriff's Office Reserve Battalion and the editor-in-chief of *IEEE Software Magazine*.

GEORGE HEUSTON (georgeh@ci.hillsboro.or.us), FBI (retired) is a management analyst at HPD and founder of the PRS Program.

SARAH MOCAS (sarah@cs.pdx.edu) is an assistant professor of computer science at Portland State University. She is also a HPD PRS.

MARK MORRISSEY (markem@cs.pdx.edu) is an instructor in the computer science department at Portland State University. He is also a HPD PRS.

JOHN RICHARDSON (jwr@intel.com) is the technical liaison to Governments for Intel's IT Risk Management and Compliance team. He is also a HPD PRS.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

© 2004 ACM 0001-0782/04/0700 \$5.00