High Tech Forensics: Serving as a Police Reserve Specialist

Sarah Mocas[1], George Heuston[2], Warren Harrison[1], Mark Morrissey[1], John Richardson[3]

The Hillsboro (Oregon) Police Reserve Specialist program provides suitably qualified individuals from the community an opportunity to assist the Police in criminal investigations involving computers and other digital evidence. The Police Reserve Specialist (PRS) program evolved from the Hillsboro Police Department's initial concept to train private–sector experts for use in emergencies. Under the philosophy that the best manner of preparing for emergencies is to assimilate a volunteer force through on–going, active investigations [Heuston, 2002], it was quickly discovered that the program also 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.

Computers and Crime

As the computerization of society has increased, both high tech crimes such as on–line identify theft and computer hacking, as well as "ordinary crimes" such as drug dealing and larceny that include a significant component of digital evidence have become more and more prominent. The dramatic increase in cases involving digital evidence requires prosecutors and law enforcement agents to deal with artifacts such as computer logs, electronic mail, word processing documents, image files , etc. Without a command 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 offenses actually go undetected [Bennett, 2001].

Police Reserve Specialists

In the most general sense, the function of a member of the Hillsboro Police Reserve Specialist program is to augment, broaden and increase the effectiveness of the Police Department in its mission to protect the community [Hillsboro, 2002]. The current focus of the program has involved gathering and processing electronically stored evidence. This entails assisting in the entire investigative lifecycle, from the preparation and execution of search warrants to preserving and analyzing digital evidence as well as providing expert testimony in court. The Reservists also participate in the development of up–to–date policies and procedures in these areas as well as working with the community to develop educational programs on the safe and ethical use of computer technologies for K–12 students.

Officially, Hillsboro Police Reserve Specialists serve as agents of the police working under the direction and auspices of Hillsboro Police Department (HPD). An *agent* is one who is authorized to act for or in the place of another, for example, as a representative, emissary, or official of a government [Merriam–Webster]. As agents, Police Reservists have focused and limited authority to be used when and where specialized skills are need.

---

[1] Portland State University
[2] Hillsboro Police Department
[3] Intel Corporation

Specifically, all Police Reserve Specialists work under the direction of a case officer, who is usually the detective in charge of the investigation.

Digital Forensics

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* [Kovacich and Boni]. From this definition, it follows that not all technically feasible techniques can legally be 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 ask the question "Is it possible to do this?" When assisting in an investigation as a Reservist however, the question becomes "Will this activity jeopardize or assist in this investigation?"

As agents of the Police, both the Fourth Amendment[4] as well as a variety of Federal and State statutes apply to the search and seizure of digital evidence by the PRS. While it is not the responsibility of the PRS to have in–depth knowledge of the law, it is necessary that the Reservist gain a perspective on the legal considerations of his/her actions so that assistance rendered 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 because the scope of the warrant was exceeded. In all cases it is expected that the Reservist rely on the judgment of the law enforcement personnel that they are assisting. The focus of PRS training is, in large part, to facilitate clear communication and understanding between the Reservist and the investigator.

An Example Case

To illustrate the scope of a Police Reserve Specialist duties, we can discuss a recent, representative case. Two Reservists were assigned to a felony fraud and forgery investigation. Earlier inquires to the Washington County District Attorney’s Office which was responsible for prosecuting the case had cleared the way for the Reservists to assist in the investigation. Because representatives from the District Attorney’s Office had participated in the PRS training, they were confident that the Reserve Specialists would be able to contribute to the case in a meaningful way.

The case began with a briefing attended by the Hillsboro detectives assigned to the investigation, two PRS volunteers and the PRS management coordinator for HPD. The limits of the warrant and types of evidence the detectives were expecting to be found on the computer systems were outlined. After the briefing, both Reservists went to the HPD Forensics Lab which contained computers seized earlier in connection to the case.

---

[4]The 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.

Following best practices, exact images were made of the disk drives so that the investigation would not taint original evidence. They then executed searches within the scope of the warrant. After analysis of 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 District Attorneys office to answer technical questions and follow−up with any subsequent searches merited through the development of the investigations. 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.

The PRSs are by no means world experts in every aspect of computing but, to date, it has been shown through several situations that the knowledge added by the Reservists far surpasses that of the normal investigating team; that Reservists are valuable right out of the box and that Reservists have more to offer then they anticipated.

Program Boot−up and Training

The concept of the Police Reserve Specialist program was first presented by the Hillsboro Chief of Police, Ron Louie, on May 2002 at a meeting of an informal organization called Computer Related Investigations, Management and Education (CRIME). CRIME, founded in 1998, is composed of people from Law Enforcement, Industry and Academia with an interest in computer security and digital forensics. CRIME participants meet monthly for talks from experts and also communicate regularly through a mailing list. Shortly after the May meeting, PRS program applications, vitas and letters of intent were solicited.

Of the initial group of forty applicants, twelve where selected. The first group consisted of eight people working in the computer/software industry, two of these with extensive legal backgrounds (one a former deputy district attorney), three academicians (from Computer Science), and a retired professional of the Northwest Natural Gas Association. 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 an area and that the training would primarily cover how to apply that expertise appropriately.

The first group of volunteers, along with representatives from the Washington County District Attorney's Office, assisted the Hillsboro Police Department in developing and delivering the initial training. Over a ten 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 the Reservists enough about law enforcement objectives so they would know when to stop and ask questions of the department investigators; and to enable the Reservists to provide the investigators with enough technical knowledge so the right questions may be asked of the subjects and witnesses. It is this balance that provides both depth of understanding and optimal investigative leverage, a crucial aspects in solving complex high tech cases. Implicit in the objectives is also ongoing training in high technology for law enforcement officers so that they are best able to utilize the Reservist's assistance. The process of education is intended to be a two–way street that raises the level of knowledge on all sides.

Police Reserve Specialists commit to a minimum term of two year of service. Most Reservists are expected to spend some time in the lab, especially as they get 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

In addition to assisting in investigations, members of the initial group are also expected to help refine and assist in delivering the training to future PRS candidates.

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 Law Enforcement. Therefore a level of communication and trust was in place. Second, Hillsboro Police Department has an ongoing history of extending the boundaries of community policing, especially with respect to technology. In 1998, HPD developed a High Tech Crime Team which has evolved into one of the most widely known such teams in the United States. Finally, due to the significant presence of computer and software companies in the Portland and Washington County areas, 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 else where. 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.

With the idea of replication in other locations, the PRS training was specifically developed so that 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 the review and re–thinking of the policies and procedures for obtaining digital evidence. The explosion of the capacities of personal computers and digital storage demand new approaches to searching for relevant information. The connectivity of computers, both locally and to the Internet, will require new techniques for isolating the appropriate data. With evidence stored on computers accessed by many users such as e–mail servers, the courts may not allow the system to be removed, nor data of other users to be copied. The PPS's 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 envisioned 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 district attorney's office, these new techniques could be essential in creating new case law that will have impact locally, regionally, and even across the country.

The tools and relationships developed for the PRS program will also be critical in times of crisis. The skills matrix will provide instant access by law enforcement to experts in key areas. The training and trust, represented through PRS credentials, will ensure identification and access to skilled individuals during confusing times.

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. Organization like CPSR (Computer Professionals for Social Responsibility) and EFF (Electronic Frontier Foundation) have worked diligently to ensure that the public and policy makers have a realistic assessments of information technologies and how they effect 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 Police Reserve Specialist program is an example of one way in which individuals with high tech expertise have an opportunity to play an effective role in the continuing give and take between technology and evolving needs of society.

References

- *Police Reserve Specialist: Answering the Call in Community Policing*, by George Heuston, submitted Law and Order Magazine
- City of Hillsboro, Draft General Order, Guidelines for the Police Reserve Specialist Program
- G.L. Kovacich and W.C. Boni , *High−Technology−Crime Investigator's Handbook*, p. 243−244
- Bennett, W. & K. Hess. *Criminal Investigation*. Belmont, CA: Wadsworth, 2001
- Merriam−Webster Collegiate Dictionary, Merriam−Webster Inc., Springfield, MA, 2002

SIDEBAR: U.S. Federal guidelines for search and seizure of computers and data are contained in the U.S. Department of Justice's January 2001 publication *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation* (published by the Computer Crime and Intellectual Property Section ("CCIPS") of DOJ's

Criminal Division) and *The U.S. Patriot Act of 2001* see
http://www.linuxsecurity.com/articles/general_article–5422.html.

SIDEBAR: 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 Academy training. 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.