

\*\*\*\*\*

**Agency Name:** Walnut Creek Police Department  
**Technology Program Name:** High Technology Project  
**Competitive Category:** Response to Computer Related Crime  
**Agency Size:** Medium  
**Contact Name:** Captain Craig Zamolo  
**Address:** 1666 North Main Street  
**City:** Walnut Creek, CA 94596  
**Telephone Number:** (925) 943-5844  
**Fax Number:** (925) 943-5811  
**Email Address:** [zamolo@walnutcdreepd.com](mailto:zamolo@walnutcdreepd.com)  
**Home Page Address:** [www.waslnutcreekpd.com](http://www.waslnutcreekpd.com)

**Executive Summary:**

Beginning in 1999, the Walnut Creek CA., Police Department undertook development of their own High Technology investigative operations including development of a stand-alone computer forensics investigation laboratory. It was partially funded by an USDOJ-OJJDP block grant, and the basic structure was in place and operational by late 2001. By 2003, the operation had moved to a new police facility, and featured three independent forensic workstations and an undercover Internet access point.

From our research, we learned that the term "high technology" was a loosely used, and not well-defined term, and found that from a law enforcement perspective, high technology operations actually encompasses three areas: (1) operation of the computer forensic examination facility, including maintenance; (2) actual high technology cases, such as identity theft, stalking, harassment, fraud, and (3) undercover operations such as intelligence gathering, and investigation of child sexual exploitation. While overlaps exist, trying to combine all of the above into one position or have it be done by one person alone was not an effective or desirable use of resources or capabilities.

Starting with the grant, and eventually moving to our own funding, we built the facility and began efforts in all areas of high technology. Significant cases include stalking, counterfeiting, harassment, child pornography, threats, and in one case, surreptitious installing of spyware on business computer. We have encouraged our examiners to consider detectives as their clients, and to expedite turnaround of digital media having it available for analysis moments after it comes in from searches and seizures. In another notable development, high technology investigative personnel recognized that a gap existed in California State Law regarding grounds for issuance of search warrants.

We met with a local legislator who successfully sponsored an amendment to the California Penal Code, to our specifications, to enhance our abilities to enforce high technology crimes.

**Program Narrative:**

By 1999, administrators at the Walnut Creek, CA. Police Department concluded that we needed to address high technology and computer-related crimes. One by one, the stories of serious felonies being committed by use of computers began to emerge, coincidental with the increasing popularity of the Internet. What was once activity limited to hackers now was a ready means to commit crimes not limited to just a few technological misfits.

After studying the problem and doing extensive research with other agencies in the greater San Francisco Bay Area, we were able to reach some preliminary conclusions, and saw there was a

fundamental decision to be made. Should we encourage creation of, and participate in a regional task force, and in doing so, hope that the combination of expertise and economies of scale would make up for the inevitable loss of some control and accountability, or did we want to set up our own high technology operation, which would clearly take additional costs and effort, but in the end, provide administrators with control, and the ability to shape the direction of the efforts.

Clearly, the precedent for high technology task forces existed, and was an attractive option.

But we were also aware that relying upon a task force for getting computer evidence analyzed was uncertain. Because of delays and complexities of computer analysis, it was highly likely, if not a certainty, that the search warrant return of evidence, normally required within 10 days under California procedures, had to be routinely delayed for digital evidence. But the greater complaint past the legal technicalities was the loss of the time value of the evidence. When detectives make an arrest, and then craft a search warrant where computers are taken, if the preliminary view cannot be made that same day, and a complete analysis and report within just a few days, the value of the forensic evidence diminishes rapidly and moves to being irrelevant.

Finally, after looking at the nature of high technology crime it became apparent that both the investigation and any forensic analysis needed strict controls and oversight almost requiring the operation to be run directly at the local agency. There was no working task force either appropriately located within a logical center of jurisdictions and one spanning many of the diverse counties within the Bay Area seemed too broad to be of much use.

For all those reasons, the decision was made to go local.

We learned that the term high technology as it applied to law enforcement really broke down into three distinct work areas, those being, (1) construction, operations and maintenance of the computer forensic analysis facility, (2) actual high technology investigation, including identity theft, frauds, child exploitation, online threats, thefts, and the like, and (3) undercover operations, typically involving child sexual exploitation and frauds. Any successful law enforcement high technology response had to effectively address all three areas, and the challenge was where to begin, and how to staff for it and effectively place it within the organization. We decided to begin with the most challenging part, the development of a computer forensics facility, as it represented what we were most lacking, and what was consuming most of the time. Not having a facility meant imposing on another agency; in our case, San Jose, CA. PD, who admirably responded to our needs, but involved a day out of the office and a 50 mile trip each way. Their dropping their work to do ours was an imposition we did not want to make. When the preliminary analysis was done, any additional searches were difficult, if not impossible, and any court proceedings would necessarily involve the costly and disruptive appearances of members of those agencies to validate the search and findings.

But there were no simple directions as to how to build a lab, and more so, what equipment and software to acquire, and where to get training. Agencies seemed to structure their individual analysis facilities very differently. In studying equipment in use at the time, as this effort moved into 2001, we decided on a high end server-grade PC, equipped with almost every accessory we could determine would be of potential use, and chose EnCase as our base forensic analysis software. We also selected the EnCase FastBloc as the interface structure. In this way, we had a versatile setup with court-validated software and a substantial company to back up the validity of our conclusions. Looking at the cost of what we eventually wanted to build, including equipment and training, it appeared as if it were going to be a significant budget item (some \$40,000) over a couple of years. Even more important, it was clear that operation of a forensic facility would require a full time commitment of personnel resources.

We became aware of grants provided by the Department of Justice, Office of Juvenile Justice and Delinquency Prevention Programs (OJJDP) to establish high technology facilities at those locations having none, with the primary purpose being protection of children, typically from online child exploitation. This grant made monies available up to approximately \$40,000 to be used over a two year period, designated for high technology equipment and training, but not for actual salaries, necessarily requiring the agency to make that commitment. In 2000 we submitted the application; by late 2000 we learned it had been accepted, and monies would become available in 2001.

In early 2001, a senior officer was identified who had done much of the early research in high technology, and was temporarily assigned to design and build the lab, and get the project started. This involved the first release of bid requests for the forensic examination machine, and since the Police Department was soon to move to remodeled facilities, design of the new lab facilities. By August of 2001, the first machine and software was received, and cases came shortly thereafter. We acquired an additional forensic analysis machine from the State of California at the conclusion of a training offering and both EnCase Intermediate and Advanced course offerings were completed.

In early 2003, the Police Department moved from its old facilities, and the forensics lab, which had been temporarily located in a storeroom, now was set up in the new building.

As the laboratory now stands, we have 3 complete computer forensic analysis workstations, each of which is equipped with its individual version of EnCase, and its own standalone FastBloc interconnect device. There is also an investigative undercover computer in the laboratory, and we have trained a second detective in forensic analysis.

Noteworthy cases and accomplishments include recovery of significant evidence in several driver's license counterfeiting cases, recovery of evidence and identification of new victims in stalking cases, identification of owners of stolen recovered computers, child pornography and abuse cases, business frauds, recovery of evidence in e-mail harassment cases, and the recovery of evidence from a malicious planting of spyware in a business computer. One other most interesting accomplishment was the realization by high technology investigators that California State search warrant law left a gap of coverage that would not authorize issuance of search warrants for a particular class of computer crimes. Although we were told it was nearly impossible to have search and seizure laws amended, especially at the initiation of law enforcement, we made contact with a local assemblywoman who sponsored, and successfully passed an amendment to the California State Penal Code to solve the problem.