

**Source:** Spinal Column Newsweekly

## Police using specialists to catch tech-savvy criminals

by Leslie Shepard-Owsley

August 26, 2009

While the proliferation of technology has paved the way for criminals to use digital media as a clandestine means to execute their crimes, law enforcement is keeping pace by using the services of forensic computer crime units. Both the Oakland County Sheriff's Department and the Michigan State Police employ computer forensic specialists capable of decrypting and uncovering sensitive information buried in computers without altering the original evidence. The units have gained ground in recent years, earning recognition and status for their exemplary conviction rates. They are routinely sought out by high profile groups such as the Federal Bureau of Investigation (FBI) and Secret Service for assistance or training.

Cyber crimes are currently among the fastest growing crimes in the nation, and computer crimes units are flooded with cases, resulting in significant backlogs. The sheriff's department computer crime unit currently has a six-month backlog of computer forensic exams, with 20 more waiting in the wings.

The department's computer crime unit, formed in 1999, currently employs two computer forensic specialists and one Internet investigator. During 2006, the unit conducted 68 computer forensic examinations that included 305 pieces of evidence. In 2008, the unit investigated 66 cases. So far in 2009, the unit has completed 25 computer forensic exams. The unit expects to exceed last year's numbers by a significant margin.

Four investigations are conducted simultaneously. Exams vary in length and intensity due to the type of case, the amount of media brought in, and what type of information is being examined; but it generally takes two to three weeks to complete one computer forensic exam because computer hard drives have dramatically increased in size over the years.

According to Detective Carol Liposky, CFCE of the sheriff's department computer crimes unit, standard protocol begins with investigators handing over computer media to the department with instructions on what he/she may be looking for. A specialist then makes a forensic copy of the computer hard drive in a sterile environment.

"We never work on the original," she said. "Rather, we take out the hard drive, make a copy and replace the hard drive for evidence. We work solely off the copy. It takes time to make a forensic copy and then conduct the analysis. We conduct file signature searches during the exam. A picture, for example, could take less than a day, but it takes longer for documents."

The case officer may require an examination of various computer media including instant messaging, pictures, video, spreadsheets, or financial records. Cell phones are also commonly examined. In other cases, investigators may ask the unit to specifically search for e-mails, child pornography, or evidence of online chats between the suspects and/or victims.

No crime is immune from the computer forensic specialists' expertise, but child pornography cases are the most prevalent, according to Detective Sgt. Joe Brian, the county computer crimes unit Internet investigator.

"My job is to investigate child predators and assist other agencies in executing search warrants or taking over cases when the Internet is involved," he said. "We do a lot of child pornography (investigations) but the team also investigates a wide range of crimes including identity fraud, homicide, financial theft, eavesdropping, auto theft, and narcotics cases. We take more cases now than ever. People are using computers more and more; therefore, cops are bringing us more to investigate."

Computer forensic specialists are savvy enough to recover a computer's deleted files, but that is interdependent on how the information is used, the type of operating and file systems the computer uses, and the size of the computer's hard drive.

"There are a lot of 'ifs' when it comes to deleted files," Liposky said. "We recover items through forensic software but sometimes we can't. It just depends on the situation."

The unit also uploads decrypting software to break user passwords. At times stronger measures are needed, such as interviewing a suspect or gaining insight into background information to crack codes.

"Every once in a while a perpetrator makes an excellent attempt at thwarting the investigation or may pitch the hard drive and install another," Liposky said. "If the hard drive is gone, there is nowhere to get the evidence. And then once in a while we'll run into an (information technology) guru or a programmer, but if the information is on their computer, we'll find it."

When a computer forensic exam is completed, the specialist prepares a CD or DVD for the investigator in charge with a narrative of what was uncovered. The investigator and the computer forensic specialist then discuss the case and whether the recovered evidence can be used.

Computer forensic specialists must undergo stringent training prior to certification. Typically, they attend a highly intensive two-week conference through an agency such as the Internal Association of Computer Investigative Specialists, where they learn the methodology behind the job. They learn various computer operating systems, how to recover deleted objects, and how to extract artifacts such as temporary Internet and link files.

At the next level, a rookie is assigned a coach that takes the trainee through a series of six hypothetical scenarios that must be passed before taking a 125-question final exam for certification. The process takes about two years. Every three years specialists must be retested to stay current with rapidly changing technology.

"The only thing constant about technology is that it's always changing," Brian said.

Hard facts and pictures speak volumes; therefore, computer forensic exams often have the ability to get a solid conviction.

"A lot of the time, these exams are the only reason we can get a conviction," Brian said. "Though we can't quantify the numbers, we are realizing many more pleas if one of our specialists is involved, and that means less cases go to court. Let's face it: If a father is abusing his child but continually denies it and then we lift the pictures off his computer, he's not going to go to trial, he's going to cop a plea."

Since Internet use is international, all law enforcement agencies get involved and collaborate to solve computer-based crimes.

"Everybody's fingers are on computer crimes, including local, state, and federal agencies," Brian said. "If the case doesn't meet a certain threshold, another agency might jump in to assist. For example, if the FBI begins a case but might not pursue it because it doesn't end up fitting their criteria, they may bounce it back to us. Depending on what we find we could hand it back to the feds or keep it for state charges, or we could split the charges. In a rape and child porn case, there is no federal rape statute, so we would prosecute the rape and let the feds handle the child porn if it crosses state lines. We have a great working relationship with the feds."

In 2003, the county's computer forensic crime unit was responsible for the arrest of 21 perpetrators who molested 64 victims. Clarkston resident Guy Lendrum allegedly chatted online with an informant about wanting to trade his son for sex. Lendrum was taken into custody and his computer was examined, leading law enforcement to the apprehension of 23 more child molesters through an international investigation. The trail continued, leading agencies to the arrest of a man in charge of the child porn site called Star Kids. By the time the investigation ended, law enforcement had incarcerated a Saginaw resident who was sexually molesting his own twin sons and had compiled a 300-person buddy list of trading partners, including an Illinois foster caretaker.

"That investigation has grown even more by now," said Liposky, who has the details of the investigation plotted

out on a chart above her cubicle to remind her of how many seedy perpetrators she's helped put away.

One example occurred in the lakes area earlier this year, when former Walled Lake Schools Assistant Superintendent for Labor Relations Craig Aleo was charged with possessing and producing child pornography.

On March 26, Aleo and his wife were stopped at the border between Canada and New York for a secondary inspection by U.S. Customs agents who reportedly found a laptop computer, memory cards and two thumb drives containing 13 apparent child exploitation images and one movie file. The graphic images and video all allegedly contained pre-pubescent females performing sexual acts.

Following his arrest, a warrant was obtained to search Aleo's home. The search reportedly uncovered two computers, multiple optical disks and other forms of stored electronic media, including two cameras, allegedly containing more than 100 images of child pornography. The CDs and DVDs recovered also allegedly contained child pornography videos.

Like the county unit, the Michigan State Police Computer Crime Unit provides computer-related investigative expertise and hand-in-hand assistance to law enforcement agencies across the state.

The department has two computer crime units covering the east and west regions of the state. Ten computer forensic specialists are dispersed between five satellite offices located in Livonia, Lansing, Midland, Grayling, and Grand Rapids. Unlike the Oakland County Sheriff's Department, the State Police employ three civilians as specialist and the rest are state troopers.

According to Michigan State Police Computer Forensics Specialist Charlene Gilbert-Warner, computer crimes continue to climb in number, and the need to stay abreast of technology is paramount to staying a step ahead of perpetrators.

"There are underground groups of very savvy perpetrators whose goal is to obstruct us and to protect illegal endeavors or sell to those criminals," Gilbert-Warner said.

In 2008, the state computer forensic unit conducted 850 exams. This year the unit has already conducted 580 exams and expects to complete 1,200 by the end of the year, according to Gilbert-Warner. The unit currently has a one-year backlog of cases.

"We are talking about terabytes of information that can take a couple months to examine," Gilbert-Warner said. "If the information is burned or deleted it could take even longer. Cyber crimes are growing. I've been here 10 years and see that as technology expands and society ingrains itself further, these types of crimes will continue. So much communication is transacted through digital devices."

The state computer crime unit personnel operate strictly according to the search warrants executed.

"If it's a child porn case, for example, unless we think they are selling pictures or videos, we don't have the right to investigate financial records," Gilbert-Warner said. "Everything must be justified in accordance to the type of case and what the search warrant covers."

Like the county unit, the state unit utilizes training but will take on FBI and Secret Service agents to work on a computer forensic task force so each law enforcement agency is uniformly trained.

"We bring others on board so we learn to do things the same way, so each person can pick up a report and see what each has done and be able to interpret it," Gilbert-Warner said. "We learn from each other and have multi-jurisdictional cases that we need to collaborate on. The FBI comes in if we have to take an investigation to a national level. The Secret Service can conduct investigations into crimes related to child porn, trafficking, homicides, and terrorism. We are one of the few agencies nationally that is setting the standard and doing as many forensic exams as we do."

The state unit attributes its high success rate to networking with other people and/or agencies.

"By working along with other law enforcement agencies, we have gained notoriety in our field," Gilbert-Warner said. "It's rare that we encounter a case that we can't crack. In only two cases the persons used encryptions and we were unable to retrieve the passwords."

The state unit routinely receives grant money used to train officers in cyber crimes. According to Gilbert-Warner, the cost of multiple types of software, high-end computers, and training up to the point of certification can add up to \$30,000 — and that's just the beginning.

"Trainees undergo basic, intermediate, and advanced training," she said. "That's why it takes so long, but we want to make sure they're ready."

"We've sent the Oakland County Sheriff's Department deputies to training with grant money," she said. "All agencies in Michigan remotely involved in computer crime investigations network together."

Both the state and county computer crime units educate communities about Internet safety.

"We do stewardship for communities through Internet Crimes Against Children, for example," Gilbert-Warner said. "Our outreach goes far because the Internet can go anywhere."

The Oakland County Sheriff's Department has hosted 32 Internet safety presentations this year alone, mostly with school and parent-teacher association groups.

The following is a look at how the lakes area law enforcement agencies deal with computer savvy criminals.

## **WIXOM**

Wixom Police Department conducts several computer forensic exams each year to secure evidence, extract drug transaction records, and document child pornography.

According to Wixom Public Safety Director Clarence Goodlein, the department performed two exams last year to identify where the child pornography was located on a suspect's computer.

The department employs one officer who has completed 12 weeks of training on forensic exams. Last year the department purchased one desk-top computer and software package designed for computer forensic investigations. The officer works in conjunction with the sheriff's department.

"The (sheriff's department) is as qualified an agency as the FBI in conducting these exams," Goodlein said. "The rise in cyber crimes has caused us to use extraordinary means to lift data from hard drives. We have never encountered a situation when we could not lift data from an encrypted computer."

With technology constantly changing, Goodlein said he foresees cyber crimes as a growing trend that can be difficult to eradicate.

"The FBI arrests a few hundred perpetrators on child pornography charges a year, and law enforcement officials think that's just the tip of the iceberg," he said. "Much more goes on than what's even imagined. The most harmful situations are the chat rooms that kids access. There are groups that trade and share child porn or collect child porn images and movies. It's a peculiar sub-culture and sometimes it's difficult to penetrate."

Various obstacles may prevent local law enforcement departments from training officers to handle computer forensic exams, according to Goodlein.

"The equipment, software, and training is pretty expensive," he said. "Most departments might not have the resources to spend on the initiative. When we sent our officer for the training, that was 12 weeks of salary with

the inability to assign him to the streets. Altogether the venture cost \$7,000 paid out of forfeiture funds."

### **WOLVERINE LAKE VILLAGE**

The Wolverine Lake Police Department leaves the computer forensic exams to the experts in the Oakland County Sheriff's Department.

According to Police Chief Joe George, there is rarely a need for computer forensic exams in such a small community as Wolverine Lake, and he couldn't recollect the last time the department required the sheriff's department to conduct an exam. He said he doesn't anticipate training an officer to conduct computer forensic exams in the near future.

"The (sheriff's department) is a very strong support system for us and there won't be a real need (to train a local officer) in the near future," he said. "As small as we are here in Wolverine Lake, we probably wouldn't send anyone for training, but we could possibly suggest getting with other departments to combine services and train an individual. However, I speculate that would behoove larger agencies. Right now, it isn't warranted and it would take quite an effort to stay up to date with the training."

### **ORCHARD LAKE**

As in Wolverine Lake, the Orchard Lake Police Department relies on the sheriff's department and State Police to conduct computer forensic exams.

Though situations rarely arise that require such scrutiny, just this month Orchard Lake police engaged the county's computer crimes unit in a case involving a juvenile victim in a child exploitation investigation.

"An out-of-state person has been communicating via Facebook, Myspace and a cell phone with the juvenile," said Orchard Lake Police Sgt. David Sims. "The (sheriff's department) has assisted us in the investigation in trying to ascertain the person's age. We executed a search warrant for the computer to see the IP address these communications are coming from. We can do the same for the phone to locate the person. We may also need to enlist the help of out-of-state law enforcement agencies."

Orchard Lake Police Chief Fred Rosenau said he has seen an upward trend in computer crimes, which may in the future necessitate training local officers in computer forensic examinations.

"As things escalate it's altogether possible that we may opt to train an individual," he said. "We'll have to wait and see. The training is time-consuming; however, there may be a need in the future. Right now there are few or far between cases that require that level of expertise."

### **WALLED LAKE**

The Walled Lake Police Department rarely uses computer forensic specialists during an investigation. When needed, the department enlists help from the county or state computer crime units.

According to acting Walled Lake Police Chief Brent Liddy, the last time the department utilized the sheriff's department for a computer examination was nearly 18 months ago, in a possible child pornography case. Since the need for assistance is infrequent, he said there are no plans to train local officers in computer forensic exams.

"Since it's not very common in Walled Lake, we will continue to utilize the county's or (State Police) resources," Liddy said. "Obviously more people have home computers and if we want to investigate that form of digital technology as a tool for prosecution, we'd ask for their assistance, but thus far it has been rare."

### **WHITE LAKE TOWNSHIP**

White Lake Police Department Lt. Edward Harris said when the department needs to conduct a computer forensic exam, it sends all the evidence to either the sheriff's department or State Police.

"It really depends on the case, on whether or not we need a computer forensic exam," he said. "We usually send several cases a year to one of those two agencies."

#### **WEST BLOOMFIELD TOWNSHIP**

The West Bloomfield Police Department has a cyber crimes unit that was formed last December.

The unit has three officers trained to conduct computer forensic exams, including Sgt. Robert Spencer, Officer Tim Lillard, and Officer Brian Tash.

Spencer said he was trained by the FBI and the Secret Service at Eastern Michigan University for 12 weeks in 2007. The class was paid for by a grant from the U.S. Department of Homeland Security.

"It was intense training," Spencer said. "We started from the ground level. We learned how software is stored and how to reconstruct data."

Lt. Carl Fuhs said the department uses forensic exams in cases ranging from fraud to identity theft.

"It runs the gambit," he said.

However, Spencer said the department rarely conducts full computer forensic exams, noting there have been only five conducted since December.

According to Spencer, the most notable case came in December, when the local unit was able to track down an employee in a Beaumont Medical Center office who was using patients' Social Security numbers to open up lines of credit and utilize credit cards. She was later charged with identity theft.

"We can do an on-scene check of a computer, or look through a registry," Spencer said.

The unit also relies on a forensic recovery of evidence device — or FRED for short — which is a super computer which records evidence when a hard drive from a suspect's computer system is plugged into it.

#### **MILFORD**

Milford Police Detective Kevin Knauss said his department usually conducts computer forensic exams about six times a year with assistance from an outside source.

"We've been getting assistance with forensics recently from the FBI," he said. "We've had problems with Oakland County — they're backlogged so bad, and we've had to wait many months to get results from them. We had one contact with Livingston County that we used on occasion."

Knauss said the State Police can also assist with the exams.

According to Knauss, forensic exams are usually done in cases involving child pornography, while in some instances they are also used when investigating fraud cases.

"They're important in child pornography cases because they prove intent by the suspect when they download this information and they're storing it on their computers — that shows criminal intent," he said.

He noted a case in December when Milford Police conducted a search of a residence on Holden Avenue, where a Milford High School student allegedly was creating counterfeit money on a scanner-printer. The department analyzed the suspect's computer during the investigation.

"We're trying to get somebody within our department who is going to be skilled at doing this, but that's in the works right now," Knauss said.

**WATERFORD**

Waterford Township Police Department sources didn't respond to calls prior to press time.