GUIDANCE SOFTWARE

CASE STUDY

Tinley Park Police Solve the "Craigslist Killer" Case Using EnCase® Forensic

Profile

Named one of "America's Best Places to Raise Your Kids" by Businessweek magazine, the Village of Tinley Park, Illinois, is a Chicago suburb with a population of about 55,000. The village has a low crime rate, but it does experience crimes of all types that in recent years increasingly involve digital devices. To combat crime, the Tinley Park Police Department works with the community and has 150 employees committed to serving the public.

Background

For the last decade and a half, Detective Anthony Balzanto was the Tinley Park Police Department's lone digital forensics examiner. Just recently, however, he's gained two additional investigators to pinch-hit on both computer and mobile-device forensic investigations. "We typically pull in between 70 to 100 cases per year that require some sort of digital investigation," Balzanto said. Lately the increase in usage of mobile devices among criminals as well as the general population has created a call for digital investigations backup.

"I've used every tool out there, but I always come back to EnCase."

- Tony Balzanto, Detective Tinley Park, IL Police Department

Growing Numbers of Data Sources Challenge Investigators

One of the biggest challenges for Balzanto and his team these days is the acquisition of the suspect's data from the cloud. "What I love about EnCase is the way the product has evolved to facilitate acquiring and analyzing data from many sources. We can look at the data in a case from different perspectives. The ability to use EnCase to examine the devices as if they were computers is really a big help. We can tear into SQL databases and get into archives. EnCase helps us get a full physical acquisition from each device by offender, then from the victim's iPhone, and so on."

Cracking the Craigslist Killer Case

Balzanto recounted a recent high-profile case from Tinley Park, which began with a local resident flagging down an off-duty police officer, pointing to a retreating car and saying, "The guy in that car just shot that guy." The off-duty officer saw the victim on the ground, called for backup, then pursued the gold Mercedes to a forest preserve outside of town. He and at least 40 officers from neighboring towns set up a perimeter, performed a search. Forty-five minutes later, the suspect was found hiding under a picnic table and taken into custody.

"When located, he was actually talking on a Samsung Galaxy device," Balzanto said. The well-trained officers left the phone where it was and called Balzanto to secure and isolate it. The crime-scene investigators did the same at the scene of the crime, retrieving the victim's phone.

After acquiring a physical and a logical image from the victim's phone, Balzanto reviewed everything from iTunes lists to the apps installed on the phone. "What really popped out at me was the Craigslist app, which stored a lot of photos and HTML text that I zipped up and brought into EnCase. I was able to see that the suspect had looked at an ad placed by the victim and had initiated a text-message conversation with him."

The victim had offered to trade his video game systems for an iPhone 5 and had supplied photos of the game system in the ad. The victim and suspect agreed to meet at a convenience store to make the trade. Upon handing over the video games, Balzanto said, "That's when the victim discovered that there was no iPhone 5. He tried to get his video games back out of the suspect's car. The suspect came up with a handgun and killed him on the spot."

Balzanto dug deeper into the data on the two phones and was able to show that the suspect had looked at the victim's Craigslist ad, then sent him text messages. The victim had texted return messages to the offender while at work.

A Timeline and the EnCase Smartphone Module Give an Assist

"With EnCase Forensic, I was able to build a timeline to show how it all happened over a period of time. The state's attorney said the suspect had never owned an iPhone, didn't have one to trade, and never found one to buy," Balzanto reported. "But we were able to show that he intended to commit an armed robbery and, in doing so, he murdered the victim. He couldn't claim self-defense because the digital evidence showed he intended to rob the guy." In the EnCase interface, Balzanto was able to bring in data from both devices and view them together, sort, and begin to see the conversation happening. "Then I could sort them by time and look from a chronological perspective at how the conversation happened. If I were working in another tool, I'd have to look at the data from one device at a time."

Of particular assistance in the investigation was the ability of EnCase to parse all the chat and text conversation within the smartphone module, turning it into a SQL database. "It's just a physical extraction," said Balzanto. "EnCase is looking at it as if it's a Linux computer. I could process the conversation data, run searches on it, and identify photographs. I saw the victim's video game equipment there and saw that the offender had viewed those ads, so I was able to actually rebuild them."

Balzanto used EnCase index searching to find all instances of the victim's phone number and even the Craigslist item number, then reviewed the related photographs in the gallery view. "Time is of the essence," he said. "We want to provide evidence to the state's attorneys in real-time and show them what we're working with. Two state's attorneys sat in on the interviews and were building their case as we were showing them evidence."

In the end, the suspect took a plea and received 42 years in prison. Balzanto using EnCase and training on it in 2001, and said, "The training I got from Guidance Software was above the bar. Tech support is also really responsive. The support given to Encase by Guidance Software has always been stellar."

In the end, Detective Balzanto said, "I've used every tool out there, but I always come back to EnCase."