Super Sleuths

Pioneering the depths of digital forensics for law enforcement

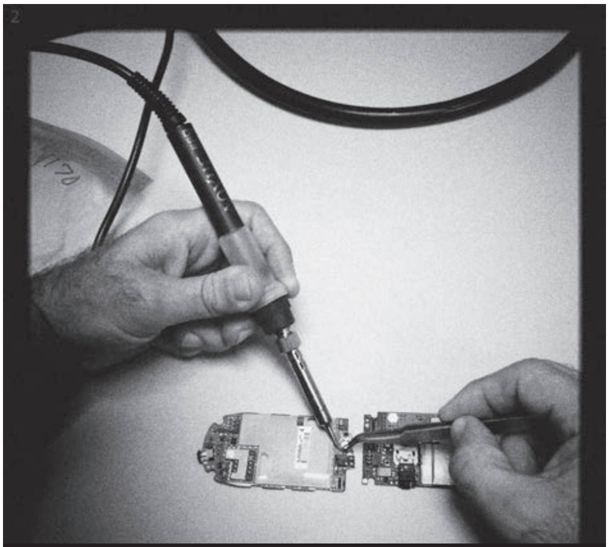
BY MARCY MASON

In 2007, only a few months after Sam Brothers joined U.S. Customs and Border Protection's newly formed Digital Forensics Unit, he realized the importance of the work that he was doing. Brothers, a computer scientist, had traveled out to a U.S. port on the southern border to test a few of the tools that he had been using to extract data from cell phones at the CBP Springfield, Va., research laboratory.

"At that time, there weren't a lot of tools, only five," said Brothers. "And there were no cell phone forensic analysts to really speak of. There were very few people doing this kind of work."

But the agency's chief technology officer, Wolf Tombe, had read news reports about people who were crossing the border with potentially dangerous data in their cell phones. Tombe wanted to ensure that the information wouldn't jeopardize U.S. security.

So when Brothers headed out into the field, he had a couple of objectives. He wanted to see what kind of data was entering the country on cell phones and he wanted to determine which tools would best meet the agency's needs. "The unfortunate thing about cell phones," said Brothers, "is that no one tool can retrieve all of the data that's stored in a phone."



★ A member of CBP's digital forensics team explores the inner workings of a cell phone.

Brothers set up a makeshift workstation in one of the offices at the port. He placed his tools and a few laptop computers needed to perform the testing on a table and waited for the port's CBP officers to bring him randomly selected cell phones from incoming travelers who were crossing the border. Similar checks with paper documents had been conducted by CBP for years as a way of protecting the country.

Much to Brothers surprise it didn't take long before something surfaced. The second phone he analyzed contained suspicious material. There was a video stored on the phone in a foreign language that Brothers didn't understand. He shared the video with a special agent from the FBI who was at the port. After briefly listening to the audio recording, the agent asked Brothers if he realized that it was an al-Qaida training video.

"I told him that I had no idea," said Brothers, who was amazed by what he had found. "This was the second phone that I was given to analyze and already I had found highly sensitive information. It was at this point that we started realizing that we had hit upon something here."

Not long after Brothers returned from his trip, he acquired a partner. William Abaunza, known to most as "Will," was also a computer scientist who was tapped from CBP's local area network engineering group just as Brothers had been. The two had worked on building the agency's computer operating system. Now together, they would pioneer the field of digital forensics, earning a reputation for CBP that is second to none. For the last four years, the two have helped many of the top federal law enforcement agencies solve cases by recovering data from computers, cell phones, GPS units, and other digital devices when all seemed hopeless. “We want to assist all types of law enforcement,” said Abaunza. “We want to provide this capability to those who need it.”

Burgeoning field

Until a few years ago, the field of digital forensics didn't exist. “There wasn't a real need for it,” said Brothers. “Everything was communicated on paper.” But that all started to change with the transmission of data through digital technology and the push toward becoming a paperless society.

Digital forensics is the extraction of data in a manner that keeps the original as pristine as possible. “Sometimes there's no way to retrieve data perfectly,” explained Brothers. “But regardless of whether it's a cell phone, a computer, or a GPS unit, we try to extract information without doing anything to the original data, and then present that information as we find it.”

“It's a reputable process that can be repeated,” said Abaunza. “We're not inserting data onto the machine or changing the information. It's an accurate presentation of what was in that machine to begin with. The person whose device we're looking at deserves that respect,” he said.

Moreover, Brothers added, “it's important for us to not only do what we do, but to document what we're doing.” Oftentimes, the digital forensic team's findings are used as courtroom evidence. “If a prosecutor needs to present our findings as part of his or her case, he or she should be able to repeat the same process and get the same results out of the same device,” he said.

At first, Brothers and Abaunza worked exclusively on CBP cases. Brothers primarily focused on cell phones; Abaunza tackled GPS units, an uncharted territory that few, if any, had ever dabbled with; and collectively they explored computers and other digital devices. They soon realized that, even between the two of them, they couldn't work on all of the agency's cases, so they decided to expand their reach and train officers and agents out in the field how to do a basic analysis. The more complex cases were still sent to Brothers and Abaunza at the CBP laboratory in Springfield, Va., where the two of them are based.

“We started deploying specific tools out to the ports so that the CBP officers could do what's called a ‘triage analysis,’” said Brothers. “Based on the results of that triage, it allows them to make an intelligent decision within a matter of minutes on whether or not to do further analysis on a seized device.” In short, he explained, “it helps them as officers to do their jobs better.”

The training had other benefits, too.

★ CBP's digital forensics team can extract deleted, hidden and not easily recoverable data from cell phones.

In one instance, shortly after attending one of Brothers' training classes, a CBP officer realized that something was amiss as he saw a gray object thrown from the passenger window of a vehicle attempting to enter the U.S. Then he saw one of the individuals inside the car chewing something.

Upon closer inspection, the officer noticed tiny gold flecks outside of the man's mouth. He recalled seeing something similar in Brothers' presentation. The pieces of gold looked like the gold-colored contacts that are used to make an electrical connection on a cell phone's SIM card, or subscriber identity module. The SIM card stores all kinds of information including a listing of the cell phone's incoming and outgoing calls.

The officer held out his gloved hand and asked the man to spit out the chewed pieces. The pieces and the discarded cell phone were sent to Brothers and Abaunza. “We reconstructed the SIM card and pulled the data out of the phone,” said Brothers. “There was information of very high value.” The data revealed the inner network of a narcotics ring. “We were able to identify the individual's boss's boss and three or four levels within the organization's hierarchy,” said Brothers.

To date, Brothers and Abaunza have trained more than 500 CBP officers and Border Patrol agents nationwide. They also have trained personnel at each of the seven CBP field laboratories in San Francisco, Los Angeles, Houston, Chicago, New York City, Savannah, and San Juan. “We train them on phones, computers, and a little bit on GPS units, so when cases come into those regions, they are sent to the labs first. If they can't be handled there, then the lab will send it to us for advanced analysis,” said Brothers.

Crucial evidence

Word spread within the law enforcement community, and before long, the expertise of the digital forensics team became known. A number of federal, state, and local law enforcement agencies began sending Brothers and Abaunza their most challenging cases.

One of the first cases came from the Department of Justice. In June 2007, the U.S. attorney's office for the southern district of New York received information about a man who was accused of molesting a five-year old girl and taking pornographic pictures of her with his cell phone camera. “We obtained a search warrant and we seized the cell phone,” said Adam Hickey, an assistant U.S. attorney from the southern district of New York. “There were pornographic pictures on the phone, but the defendant said that the pictures had been emailed to him, and that he hadn't actually taken any sexually explicit photos.”

The man was arrested, but Hickey still had two basic questions he needed to resolve. He wanted to find out the identity of the victim and to see if there was a way to disprove that the pictures had been emailed to the defendant. “We wanted to prove that the pictures that were on his phone were taken by the phone’s camera,” explained Hickey.

The prosecutor turned to Brothers for help. He had heard about CBP’s digital forensics team from the Immigration and Customs Enforcement agent who was investigating the case. “My case agent knew about the lab because of the affiliation between ICE and CBP and sent the phone there,” said Hickey. “At the time, it was pretty cutting edge and novel to do this kind of stuff.”

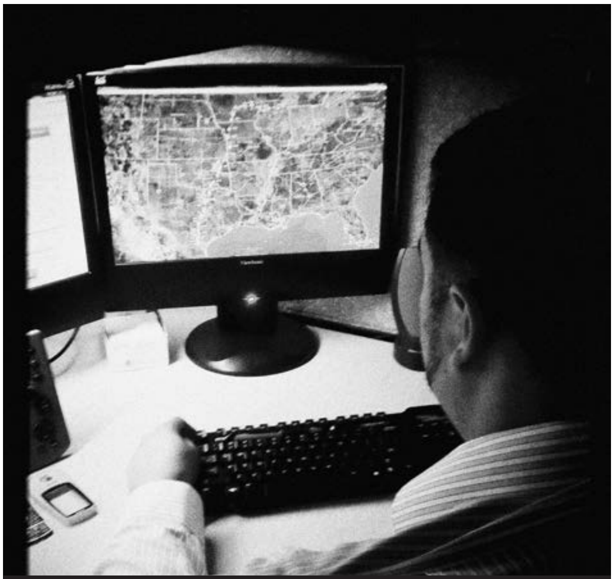
At first, Brothers was asked only to extract data out of the phone. “That was the easy part,” said Brothers. But then, nearly a year later, before the case went to trial, Hickey asked Brothers to take things a step further to see if the images were taken with the cell phone’s camera. To do this second investigation, Brothers’ work was groundbreaking. Using a process called digital image ballistics, he was able to determine where the images came from.

“Sam came up with about 12 different ways of testing whether the phone had taken these pictures or if they had been emailed,” said Hickey. For example, “he found emails carrying the pictures from the phone to an outside email address, but no emails going into the phone.” Brothers also analyzed aspects of the photos including the resolution and naming conventions. “They all matched up with other pictures in the phone,” said Hickey.

Brothers was thorough, too. “As he was processing the phone, he took pictures of the screen of the cell phone so that it would be very, very clear how the cell phone worked and where the pictures were stored,” explained the prosecutor. “He was meticulous about all these little details, even something as simple as being careful to track the serial number of the phones so that our chain of custody was clean,” proving that this was the evidence that was seized from the defendant, said Hickey. “From beginning to end, he handled this as perfectly as you could ever hope a law enforcement agency would handle a piece of evidence. I mean, it was textbook.”

In Brothers’ testimony, “he was able to render an expert opinion about whether the phone took the pictures or whether the pictures were emailed. That was critical,” said Hickey. “When the time came for trial and the defense had Sam’s opinion, they changed their defense. Based on his work, it was clear that the defendant lied when he was arrested.”

After a two-week trial in September 2008, the defendant was convicted and sentenced to 30 years in prison. Hickey noted that Brothers’ contributions to his case were crucial. “There certainly was other evidence in the case, but this directly answered questions in a way that no other evidence could ever do,” he said.



★ Will Abaunza plots navigational coordinates from a GPS unit, recreating the path taken by human traffickers.

Coast Guard curriculum

The Coast Guard was another agency that sought the digital forensic team’s help. For years, the Coast Guard had been extracting data from GPS receivers for criminal prosecution and trend analysis purposes, but the agency didn’t have a program to train new analysts. “One of the first things they ask when you take the stand as an expert witness is ‘What kind of training have you received?’” said Robert Wood, a senior chief operations specialist at the Coast Guard’s Intelligence and Criminal Investigation Team in Miami. “We needed a program to train and certify GPS forensic analysts so they could be deployed to the field where the capabilities were desperately needed. The training and certification had to be topnotch to ensure that the analysis was precise and could withstand any scrutiny the defense might have.”

Wood searched for a course, but came up dry. “There were all kinds of courses for computers and cell phones,” he said, “ but there was nothing that was geared directly toward GPS receivers.”

After checking around, “we heard about the Digital Forensics Unit and how they had a superb reputation for technical ability and professionalism,” said Wood. “So we asked if they could leverage what we were doing with what they were doing.”

The result was that Abaunza agreed to design a curriculum specifically for the Coast Guard. “Will created digital forensics certification courses for different levels of complexity,” said Wood. “He then provided the training to multiple Coast Guard sectors and districts throughout the nation. This allowed the field units to conduct more timely and effective digital forensics on the majority of criminal investigation requests in our area of responsibility.” The more extensive cases that required accredited laboratory support would be sent to Abaunza in Virginia.

The Coast Guard’s first digital forensics certification training was given in January 2009. Four other similar courses were offered throughout the year. “It’s been a huge step forward for us,” said Wood. “The Coast Guard’s ability to gather intelligence and provide support to operational partners has grown tremendously. In the past, we had one person extracting data for the entire agency. We had no program to certify or train additional analysts to meet the intelligence and criminal investigation demands,” said Wood. “Now, there’s a mixture of more than 22 people from CBP and the Coast Guard performing our digital forensics work. We have a certification process with three different levels and we have policies, procedures, and guidance in place.”

Shortly after Wood received his digital forensics training and certification, he put his new skills to work. In June 2009, the Coast Guard intercepted a speeding vessel that was traveling from the Bahamas toward the southeastern U.S. The vessel had two suspected smugglers and three Haitian migrants onboard. The suspected smugglers claimed that they came across the Haitians while on a fishing trip and had acted as good Samaritans. "They said that they had saved the Haitians who were lost at sea," said Wood. "They said they had never been in the Bahamas and that they came across the Haitians in international waters."

But after Wood did an analysis of the vessel's GPS unit, he discovered that the boat had, indeed, been in the Bahamas. "When we presented them with the facts that we planned to share with the jury, they pled guilty," said Wood. "This was a huge win because we didn't have to go to trial, which is a very lengthy process. Our digital forensic capability has given us a real powerful tool. Without the training and certification I received from CBP's Digital Forensics Unit, the Coast Guard would not have had the capability to deliver such rapid and effective results."

Assisting law enforcement

Abaunza and Brothers have assisted law enforcement on hundreds of other cases. The two have used their expertise to track the movements of suspects, find hidden files, recover deleted data, and search for criminally linked information among other pursuits. The cases pertain to everything from murders, suicides, and accidents to human trafficking, drug smuggling, terrorist plots, and stalking victims.

In one recent case, Abaunza helped local police identify the whereabouts of potential suspects in a murder investigation. The police had located a GPS unit that was linked to the victim's stolen car and brought it to Abaunza to do an analysis. "After the homicide occurred, the victim's vehicle was stolen with the GPS unit inside the car," said Abaunza. "We were able to determine the locations of where the unit had been, which gave the police additional evidence, leading them to the suspects." Last November, the suspected gunman in the murder was convicted and sentenced to 40 years in prison.

In another case, the digital forensics team was able to determine that a government employee had been using his computer at work for unauthorized purposes and had been stalking a colleague. "He was using his credentials to research information about another employee. He found her address, her license, and the exact location where she lived," said Abaunza. "He stored the data that he was accumulating on a server at work."

★ SIM cards used in cell phones store all kinds of information including incoming and outgoing calls, text messages, and phone directory contacts.

Abaunza was able to recover pictures, videos, contact information, and personal documents including the woman's passport and citizenship information. "He had his entire phone bill itemized on the computer, showing when he had called her," said Abaunza, who also recovered videos of the victim while she was at a local shopping mall. "He would follow her at the mall and stalk her—even going so far as to dress up like a mall security guard to steal video tapes from the property. He took stalking to the next level," said Abaunza. "Our findings confirmed that the employee had misused his computer and that the victim had a valid complaint."

Complex case

One of the most complex cases the digital forensics team has worked on involved a diver who lost both of his legs in a boating accident. The diver had been swimming near several ships and it wasn't clear which ship was responsible for his injury. The Florida Fish and Wildlife Conservation Commission, the agency investigating the accident, asked Abaunza for help. The commission sent Abaunza GPS units from each of the ships in question to clarify which one was at fault. "It was an accident reconstruction case," said Abaunza. "They gave me the navigational coordinates and I extracted all of the information from each unit."

Abaunza then plotted out his findings so that he could see where the vessels had been located. The case became extremely complex because Abaunza needed to retrieve data from so many different GPS models. "I needed to use different tools and create new methods to acquire the data because there aren't any tools designed for this purpose," Abaunza explained. "GPS units are intended to have data programmed into them, not extracted out." Ultimately, Abaunza was able to determine which of the GPS units had come closest to the diver and severed his legs.

The digital forensics team also is frequently involved in tampering cases. "Somebody from CBP or another agency will travel to a foreign country, and while they're in that country something 'funny' happens to his or her laptop computer or another device," said Brothers. "So they bring it to us and we check to see if the software code has been modified or the device has been tampered with in other ways."

Unidentified electronics is another area that Brothers and Abaunza often tackle. "Law enforcement agencies will send us electronic devices they've seized and ask us to tell them what's stored on the device or what it does," said Brothers. "We can't find the device in a store or call a manufacturer." Instead, the duo relies on their experience and ingenuity. "Many times when we have a new device sent to us, there is no tool to get the data out of that specific device," said Abaunza. "So we'll develop a tool or a process and then document it in a white paper that we'll publish for the law enforcement community."

In one instance, Brothers and Abaunza were told that the unidentified electronic device that they were given was a "distance finder." "We were told that the device was a graduate level science project that would calculate the distance between the device and a wall," said Brothers. The law enforcement agency that seized the device wanted Brothers and Abaunza to find out if that's what the device really did and if they could verify their findings. "We didn't have all the components necessary to do the testing, so we had to improvise and develop the tools that we needed," said Abaunza. As it turned out, the two discovered that the device did, in fact, calculate distance, but it also was an information gathering tool that could pose a problem for the national security of the U.S.

"Most people don't have the opportunity to see as much as Sam and Will do," said Ira Reese, executive director of CBP's Laboratories and Scientific Services division, who also chairs the World Customs Organization's scientific subcommittee. "CBP is the biggest law enforcement agency in the country. We have millions of people crossing the border every day, so they're going to see a lot more media than digital evidence people at other law enforcement agencies. These two have pioneered the field. Very few people have their breadth of knowledge and expertise."

Creative backgrounds

Interestingly enough, neither Brothers nor Abaunza planned to go into the field of digital forensics. Both discovered that they had an aptitude for computers quite by chance. In Brothers case, he had been singing since the age of three and thought he would study music. "I was supposed to be a music major. I was classically trained in voice and piano for six years," he said. But then, during his sophomore year in college, Brothers changed his mind. "I decided that it was not going to pay the bills. Some of my friends, who were the best singers and guitarists I'd ever heard, were graduating and pumping gas in their hometowns. I'm not a money hungry type of person, but that's not how I wanted to live," he said.

Brothers became interested in computers during college when his computer started to break down. His father, a computer savvy retired Air Force major, sent him the parts and Brothers did the repair work. "I figured out how to replace everything all by myself," said Brothers, who over time rebuilt the entire machine. "The only thing that I didn't replace was the case," he said.

★ Sometimes members of the CBP digital forensics team have to dig a little deeper for the key piece of evidence.

Word spread and Brothers talent for fixing computers became known. "This pretty girl from up the street called me and said, 'My computer is dead. My paper is due in six hours. I heard you're a computer guy.' So I went over to her apartment and had her computer back up and running within 15 minutes," said Brothers. Much to his delight, he landed a date with the girl. "That's when I realized this was cool," he said. "But it wasn't just the pretty girl. I liked the rush of being able to help that person and knowing that I could do this."

Abaunza also had creative leanings. "I used to be a graphic designer. I can draw anything I look at, but I always wanted to be an engineer," he said. Abaunza's interest in computers was sparked when he was 15 years old and he accidentally infected the family computer with a virus. "I knew I had to fix it before my mom came home," said Abaunza. "It took me about an hour to figure it out, and then I reinstalled the operating system," he said. "It was pretty cool. That's when I started building my own computers."

Brothers, now 42, graduated with a bachelor's degree in computer science. Abaunza, 32, earned a bachelor's in information technology and last year, he completed his master's degree in information assurance. Between the two of them, Brothers and Abaunza hold 40 certifications in digital forensics.

Among their numerous achievements, Brothers and Abaunza have written several best-practice documents for the Scientific Working Group for Digital Evidence, one of the country's most respected digital forensics organizations. Both are active members of the Digital Forensics Steering Committee, which is part of the National Institute of Standards and Technology, an agency within the U.S. Department of Commerce. Together, Brothers and Abaunza have developed the standards that are used by the CBP digital forensics laboratories, which have been shared with other federal government agencies. Additionally, Brothers and Abaunza created a system to determine levels of digital forensics analysis used by universities and colleges nationwide. The two also have published dozens of articles and whites papers in addition to regularly speaking at conferences.

"There's a lot of satisfaction in knowing that we did something that nobody on this planet has ever done before," said Abaunza. "What makes us feel even better though is being able to share this knowledge with others and inspire them to help as well." ■

CBP photographer James Tourtellotte snapped all images in this story with his smartphone.