CYBER INTELLIGENCE

THINK DELETING YOUR PHOTOS AND TEXT MESSAGES MEANS THEY’RE GONE FOREVER? THINK AGAIN. DIGITAL INFORMATION IS PERMANENT— AND THAT’S GOOD NEWS FOR THE OFFICERS OF ARMSTRONG’S CYBER FORENSICS WHO ARE ON THE FRONT LINES OF ONE OF THE FASTEST GROWING FIELDS IN LAW ENFORCEMENT.

KRISTEN SMITH | PHOTOGRAPHY BY RYAN GIBSON

It was late that cold January night when Lt. John Taylor got the call. Not that the time mattered. There were officers on post at Armstrong Atlantic State University’s police department 24/7. But this was Lt. Taylor’s night. And the call was from the FBI.

The Washington office of the bureau was aware that the university, an institution with just shy of 7,000 undergraduate students, had a campus police department with a new Cyber Forensics Division. “I think, in truth, they were probably on their last straw,” says Lt. Taylor, division commander and legal advisor of the CFD. “They were desperate. So they called us.”

Desperate because digital forensics labs throughout the country average a seven- to eleven-month waiting period. And this time-sensitive case just couldn’t wait.

“It was an international case, let me just put it that way,” he says. “The FBI had a confidential informant in this area who had a Blackberry device. There were pictures on the device that they had somehow lost. They weren’t sure what happened to them, but they were no longer there. And these were essential to the case.”

"The nice thing about digital evidence is it’s either there or it’s not. It’s so straightforward. And it looks great in court."

An FBI agent flew down from D.C. and arrived at the division with the Blackberry in hand. He muscled Lt. Taylor’s digital forensics analysts to the side. The agent hooked the phone up to the division’s Celebrite machine and scanned the device for the lost photos.

The search yielded nothing. The agent looked panicked as he ran out to call Washington. “These photos were critical and essential for this case to progress,” Taylor says. “He was a dejected young man.”

Knowing that not all digital devices store information in the same places, one of the officers took the phone apart and found a secure digital memory, or SD, card. Using another piece of equipment in the lab, the officer was able to harvest all of the incriminating photos in about 10 minutes.

“What you’ll find in digital forensics is that some people know how to use some equipment, but very few people know how to use or have access to all the tools,” Taylor explains. “One of the things that sets us apart is that all of my guys, even though they know how to use a Celebrite—which is actually a very simple machine to use—they’re also trained forensic analysts. All of them have had some level of investigative training, so they have a ‘never say die’ attitude. My guys wouldn’t accept ‘the Celebrite doesn’t work’ as the answer.”

WHO YOU GONNA CALL?

Since its inception earlier this year, Armstrong’s Cyber Forensics Division has worked with over 20 federal, state and local law enforcements on more than 100 cases, including:

FEDERAL AGENCIES
FBI
DEA
United States Secret Service
Bureau of Alcohol, Tobacco, Firearms and Explosives
Federal Protective Service

STATE AGENCIES
Georgia Bureau of Investigation
Georgia State Patrol
Georgia Department of Revenue
University System of Georgia Police

MULTI-JURISDICTION AGENCIES
Tri-Circuit Drug Task Force
County Agencies
Sheriff’s Office
Municipal Police
NOW YOU SEE IT

"The nice thing about digital evidence is it's either there or it's not," says Lt. John Bennett, one of the CFD's cyber forensics analysts. "It's so straightforward. And it looks great in court."

The term "digital evidence" covers a multitude of information: finding text messages and photos on smart phones is just the tip of the iceberg. "Any digital device obviously contains digital information," explains Lt. Bennett. But it also contains logs. A stolen iPod or laptop with WiFi capability, for example, is constantly scanning to connect to wireless internet. Analysts can evaluate the connectivity history of the device through its Mac address to determine where it was and when.

Location and speed-based logs in GPS devices can be used as tools in accident reconstruction. Lt. Bennett recently pulled data from a tractor trailer's GPS to determine the speed the driver was going (55.7 MPH in a 35 MPH zone) when the truck crushed a car in an intersection. The accident resulted in a fatality. The data resulted in a speedy trial and closure for the victim's family.

"We are hopeful that a lot of this good digital forensics evidence will lead to guilty pleas, because that moves everything along a lot quicker," says Taylor.

Even a video game console can be a key piece of evidence. In a murder investigation with which the CFD is assisting, one man allegedly shot the other at point blank range in his living room. The suspect claims that on the evening the victim was killed, the two of them were playing his PlayStation.

"What we can do is look at the logs, when they logged in, when they did certain things, if they connected to any other users over the internet," says Lt. Bennett. "They had headsets on where they could communicate with people across the network. One of the things the detective wants to know is if there are any witnesses out there that maybe heard something going on."

STARTING FROM ZERO

AASU's Criminal Forensics Division is the brainchild of Chief Wayne Wilcox, director of the Cyber Security Research Institute. When he came to Armstrong, the department was in turmoil. "We had no serviceable vehicles, no uniforms," the chief explains. "The Department had not grown with the university." He began forging partnerships with administrators and professors to increase the department's presence on campus. He also began quietly building the Cyber Security Research Institute that would house the Criminal Forensics Division, or CFD, a full-service cyber forensics lab. The plan was to staff the lab full-time with the department's officers—who would also be trained cyber analysts—and develop a hands-on internship for criminal justice students unlike any other in higher education.

"The university's president charged the chief a long time ago with two things: getting involved in the university's academic teaching mission and helping the university reconnect with Savannah," says Taylor. "As a police department, what a better way to do that than through our connections to the greater criminal justice community? We can make a meaningful contribution to safety and security in the local community and help out other agencies."

Still, the plan was met with skepticism. "At first, people really doubted the ability of a police officer to learn about computer stuff," says Lt. Bennett. "It's actually a lot easier to teach a police officer about computers than it would be to teach an IT guy how to be a police officer. The reality of it is, in the way we've been trained to think, we're inquisitive. We think outside the box. We don't give up on things."

The advent of the CFD is proof positive of that forward-thinking tenacity. "Many university police departments kind of fit that mold you know, being university police—whatever that is," says Chief Wilcox. "We have broken out of that mold and moved into something much more useful."
Useful is an understatement. Since that first case with the FBI in January, the CFD has worked with over twenty federal and state agencies on hundreds of cases. Quite an accomplishment for any agency, let alone a university police department that was staffed by fewer than 10 officers several years ago. The department now has 21 sworn officers, one third of which already have their master's degrees. "Find me another police department that has that!" Lt. Taylor quips.

Over 100 cases in, the accuracy and efficiency of the department's work are building a sterling reputation for the CFD—and cementing its importance as a tool for law enforcement agencies, both locally and nationally.

"There is more work, there is more work than there are people to do it," Lt. Taylor explains of the state of the digital forensics field across the country. "We're providing an in-demand service. Most labs run anywhere from a seven- to eleven-month delay. But that's not actually as bad as it gets in the digital forensics world."

"How long is a typical wait at Armstrong?" Taylor shrugs. "Metro brought a phone in yesterday, and John's already done with it."

"Yeah, they came and picked it up this morning," Bennett says. "Part of what that time frame gives back to detectives is actionable intelligence. They have intelligence within a day that they can go out and use."

"You can't wait seven to eleven months all the time," Taylor adds. "If you pick up a drug dealer on Christmas Eve at 10 P.M. and you find that he has a cell phone, and you think that there's police intel on there that you need in order to catch his supplier, you have no place to take that. Except you could come over here to Armstrong, and there is bound to be at least one officer on shift who can get that thing started and maybe get some information off of it for you right away."

Speaking of drug dealers: "One of the things you find on cell phones is you're able to put together drug networks. Who's who in the network? Who are the big suppliers, who are the street-level sellers, what their various rankings are. It gives you a tremendous amount of information," Taylor says.

Not only are dealers sending incriminating texts or amassing digital contact lists of criminals, they're taking video of felonious and criminal activities on their cell phones—doing drugs, driving stolen vehicles and bragging about the crimes they've committed.

"All we have to do is play that video, show that evidence in court and they're done. That's it," says Bennett.

MOVING THE LINES OUT

What started as an idea for an internship program to engage and prepare Armstrong's criminal justice students for the workforce has grown into something that is having a measurable impact on campus and with local, state and even federal law enforcement agencies.

"When we were moving into this area, we had a lot of people wondering, 'Can we really do this?'" Chief Wilcox says. "And then we have the first case, and then we have the second case, and the third case, and the fourth, fifth, sixth and seventh, until we're where we've handled 100-plus cases now. And we've been remarkably successful because we're not sitting there saying, 'We can only be within these lines.' We've moved the lines out."