Cyber Forensics Division, Armstrong State University Police Department

The Armstrong Police Cyber Forensics Division (CFD) is unique among local and state law enforcement agencies, as well as university police departments, in many respects. The division and its capability were created to provide Armstrong Criminal Justice and Computer Science students with a real time connection to the criminal justice community.

The CFD operates a state-of-the-art digital forensics lab that provides digital forensics analysis and investigative services to the FBI, Secret Service, ATF, DEA, Georgia Bureau of Investigation, Georgia State Patrol, Georgia Department of Revenue, Chatham County District Attorney, Savannah-Chatham Metro Police, and dozens of local agencies.

This lab is also used to provide Armstrong students with internship opportunities and to support teaching initiatives at Armstrong. The intensive 14-week internship with the CFD culminates with the opportunity for students to demonstrate their proficiency in digital forensics analysis and investigations by taking a national certification test in digital forensics. While Armstrong Criminal Justice students are not permitted to work on actual evidence during the internship, they are given access to the state-of-the-art lab and replicate complex real life cases. This process also gives students the opportunity to network with the federal, state, and local investigators.

Although the CFD has been in operation only 24 months, it has quickly become the largest digital forensics lab in the State of Georgia. While most of the state has a 7 to 12 month backlog of cases awaiting digital analysis, the wait in southeast Georgia has been reduced to less than 30 days. The CFD provides the following services:

• Case-by-case legal evaluation for each cyber investigative initiative
• Imaging of digital storage devices with confirmation of evidential integrity
• Data preservation and recovery services
• Identification and recovery of erased or deleted data (pictures, cell phone calls, email, text messages, files, and user activity)
• Document user and file activity
• Data sifting including advanced key word searches, date searching, and data segregation
• Data linking
• Authentication of data files
• Historical reporting of the content of files, including recovered data and files
• On-scene recovery and preservation of volatile memory in forensically sound manner
• On-scene preview of hard drives/computer systems
• Preparation and packaging of electronic storage devices for evidence
• Proactive computer system audits
• Data wiping service
• Complete cyber investigative analysis and documentation using a variety of state-of-the-art digital forensics tools such as FTK 5.5, MPE+ 5, Encase 7, Celebrite Touch, Celebrite Physical Analyzer, Lantern System, and other industry standard tools

• Expert court witness testimony

Awards and Recognition

The CFD Program has been recognized by the Criminal Justice Community:

- 2013 Georgia Governor's Public Safety Award for Innovation
- 2014 Dr. Curtis E. McClung/Motorola Award of Excellence

Publication Excerpts:

Armstrong and digital forensics: Right under our noses

Excerpted from *Savannah Morning News*
February 26, 2014
By Bea Wray

Armstrong [Atlantic State University]'s police department has the largest cyber forensics staff in the state and is the only university and police department in Georgia, if not the nation, working collaboratively to enhance their school's educational programs. Armstrong police officers work with the university's criminal justice department at the undergraduate and graduate level to provide a track in cyber forensics, run an undergraduate internship and provide a graduate practicum.

One Armstrong police officer teaches the cyber law class in the school's graduate program.

Armstrong's police department is also the largest digital forensics lab in the state of Georgia. The size is defined by amount of equipment as well as investigators. The extensive equipment includes five FRED (Forensic Recovery of Evidence Devices), FTK (Forensic Toolkit) software and numerous technologies specific to mobile devices. Nine cyber forensics investigators are employed at the unit.
Count that again: Nine full time cyber forensic investigators right here in Savannah. In 2013, Armstrong's cyber crime forensics unit examined hundreds of computer and mobile devices for federal, state and local criminal justice agencies throughout southeast Georgia. As a result of their willingness to look outside the box, Armstrong and its police department have decreased evidence processing time for cyber investigations from 12 months to less than 30 days for agencies throughout the state.

While Armstrong's students are not permitted to work on actual case evidence, they do have the opportunity to network with police investigators. Savannah has quietly become the center for digital forensics in Georgia. Armstrong and its police force are not content with standing still. While their collaborative effort has established a name for their police department within the law enforcement community, they are making plans to bring these same skills to the private sector. According to [Armstrong Police Chief Wayne] Willcox, the business community can use digital forensics audits to detect fraud and internal theft, thereby preventing the loss of millions, even billions, in revenue every year. Armstrong plans to offer the services of its police officer/digital forensics analysts to the private sector in the near future and is looking into partnerships with private industry that will open up research opportunities for their faculty and students.

Cyber Intelligence

Excerpted from *South Magazine*
August/September 2013
By Kristen Smith

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.

"The [university's] president charged the [police] 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 [Lt. John] Taylor. "As a police department, what 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 community and help out other local agencies."

The Cyber Security Research Institute 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.

What started out 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.

Since its inception [in 2013], 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 Protection Service

State Agencies
• Georgia Bureau of Investigation
• Georgia State Patrol
• Georgia Department of Revenue
• University System of Georgia Police

Multi-Jurisdictional Agencies
• Tri-Circuit Drug Task Force
• County Agencies
• Sheriff's Office
• Municipal Police