

## **TechBeat January 2016**

The following stories are from the January 2016 issue of *e-TechBeat*, the newsmagazine of the National Law Enforcement and Corrections Technology Center System, a program of the National Institute of Justice under Cooperative Agreement #2014-IJ-CX-K004 awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Lockheed Martin. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.

## Field Search: Field-Based Computer Forensics Software Widens Its Scope

By Becky Lewis

*A soldier doing a field check on a computer recovered at an IED explosion site. A police officer doing a “knock and talk” investigation. A computer forensics expert doing triage on a number of suspect computers. A federal agent searching for intelligence related to counterterrorism activities. And a probation and parole officer, checking up on a sex offender’s Internet use.*

*What do they all have in common? They’re all using Field Search, the free forensics software provided by the Justice Technology Information Center (JTIC), a component of the National Law Enforcement and Corrections Technology Center (NLECTC) System.*

When the NLECTC System began providing Field Search in 2006, probation and parole agents who needed a nontechnical tool to check up on client computers while in the field made up the target audience. As the software has morphed through five iterations — the most recent (5.0) released in early January 2016 — more and more users in a wider variety of criminal justice fields, and even the U.S. military, have found that Field Search meets needs far beyond the suite’s original scope.

Field Search, provided by JTIC to only vetted active professionals, allows users to quickly and efficiently search a target computer and create a detailed report of the findings. Originally developed with funding from the Office of Justice Programs’ National Institute of Justice and since upgraded by the developers at no charge to the federal government, Field Search can be launched from a USB drive and works live on a suspect computer to quickly find potential evidence such as Internet histories, images, multimedia files and results from text searches.

For Version 5.0, software developer Jim Persinger completely recompiled, recoded and rebuilt Field Search to improve its compatibility with today’s hardware and software. Although those changes aren’t apparent to the end user, the end result still allows the software to run a complete scan of a hard drive, analyze the contents and produce a report in less than an hour, even though the hard drives of 2016 are much larger than those of 10 years ago, and even though the Field Search of 2016 has vastly expanded capabilities compared to those of the original version.

“[Jim Persinger and I] originally developed Field Search to help monitor sex offenders and protect children,” says project coordinator Jim Tanner, who has also provided numerous train-the-trainer sessions to criminal justice professionals over the years, equipping them to return to their agencies and share their knowledge as Certified Field Search Instructors. “As its use expanded into the law enforcement, military, border security and counterterrorism arenas, we realized the need and importance of providing quality tools for nontechnical users at no cost, and even after the initial funding ended, we remain committed to this project because it’s the right thing to do.”

Although many of Version 5.0’s changes run behind the scenes, it includes a number of new features and upgrades that will directly benefit users. One of the most significant expands the keyword search function to include the capability to search for a word or phrase in any language.

Not just any language that uses the Latin alphabet; that function came with Version 4.0 in 2012 (see “In Any Language, Field Search Translates to Success,” *TechBeat*, Summer 2012, [https://justnet.org/InteractiveTechBeat/summer\\_2012/FieldSearch.pdf](https://justnet.org/InteractiveTechBeat/summer_2012/FieldSearch.pdf).) Rather, Version 5.0 adds the capability to query in any language spoken on this planet, whether it uses the Latin alphabet, the Arabic, Cyrillic or Eastern language characters, or anything else.

“That’s a huge, huge change. We’re seeing more and more usage in investigations in domestic counterterrorism, and the U.S. military has been asking for this function for years,” Tanner says.

The military began training soldiers in the use of Field Search approximately five years ago, for use in battlefield forensics to quickly analyze data when there is neither time nor ability to bring a recovered computer back to a lab.

A second major change adds chat history tools to allow users to examine activity for Skype, Windows Live, ICQ and Yahoo Messenger. The tool provides information on who the user sent messages to, what they said and when they said it. Another new addition is a search function that provides the ability to scan a drive for hits against HASH sets. A HASH, Tanner explains, is a virtual “fingerprint” of a computer file. Each computer file, via a mathematical algorithm, produces a unique set of letters and numbers that identifies it; change one letter in a file or one pixel in a picture, and the file generates a new HASH. The National Center for Missing and Exploited Children maintains a HASH database of all known child pornography files, and if a law enforcement agency has access to that database, analysts can use Field Search to compare the files on a computer hard drive and locate matches. This function can also tell probation and parole officers if clients have downloaded software they are not permitted to access.

Yet another significant change makes Field Search fully compatible with Windows 8 and 10, as well as the most current versions of Internet Explorer, Edge, Opera, Chrome and Mozilla/Firefox. The software maintains compatibility with older versions as well.

Additional new features/upgrades include:

- Pictures in the Image Gallery can now be sorted by date accessed, allowing Field Search users to see which pictures were accessed most recently.
- When a user is running Field Search off one computer and remotely searching a hard drive, the registry tool now pulls the registry information (e.g., when a drive was installed, the user’s email address) from the remote drive rather than from the computer running the software. Tanner explains that originally, Field Search was intended to be run only in the field, and thus would only need to look at the registry for the computer on which it was running. However, as computer forensic experts moved to using it for preliminary triage prior to using more sophisticated software, the need arose for an expanded registry tool.
- Improved reporting speed and greater ability to export reports as PDFs.
- Improved and faster media rendering.

“Digital evidence represents a critical element in the investigation of new crimes and also in the pre- and post-conviction supervision process. Most agencies appreciate this reality; however, many struggle with funding issues and as a result, lack capacity in this area,” says Joe Russo, JTIC Corrections Technology Lead. Russo served as deputy director for corrections at the former NLECTC-Rocky Mountain Center during the software’s initial development, and later as the director of the Corrections Technology Center of Excellence through several upgrades.

“The upgraded Field Search software allows agencies access to an easy-to-use, yet powerful, forensics tool, and the best part is that it is completely free,” he says. “We are deeply indebted to Jim Tanner and Jim Persinger for their tireless dedication to the Field Search effort. They both have a deep desire to support public safety and have each volunteered countless hours to improving Field Search and keeping it viable.”

*Field Search is available free of charge to qualified professionals. For more information on Field Search, including how to download a copy, please visit [www.justnet.org/fieldsearch/fs\\_main.html](http://www.justnet.org/fieldsearch/fs_main.html).*

## **Want to Start a UAS Program? The Arlington Police Department Has Lessons Learned to Share**

By Becky Lewis

*What's a COA and why do we need one? Do we need trained pilots to run these devices? What are they good for, anyway?*

*When it comes to unmanned aircraft systems (UAS), many law enforcement agencies have lots of questions, and aren't sure where to get all the answers. The Arlington (Texas) Police Department, which has been running a UAS program for several years, offers to share some of the answers figured out along the way, because, program manager Sgt. Brook Rollins says, "The more agencies that want to, and do, use UAS, the easier it will be for all of us to develop and follow standard procedures."*

After completing a two-year testing, evaluation and training process, Arlington received its official Certificate of Authorization (COA) to operate a UAS program from the Federal Aviation Administration (FAA) in February 2013, making it one of the first law enforcement agencies located in a densely populated urban area to receive such approval. The COA grants Arlington permission to fly unmanned aircraft under certain restrictions, including:

- Must fly under 400 feet from the ground.
- May fly only in daylight.
- Must be in sight of the operator and a safety observer at all times.
- Must maintain contact with the control tower at Dallas-Fort Worth Airport.
- May not be used for pursuit or for traffic enforcement.

Even with those restrictions, Arlington finds ways to use the miniature helicopters, which are approximately five feet long and can fly for approximately 15 minutes on battery power.

"We use it for accident and crime scene reconstruction. We use it to track missing persons, like elderly persons with dementia, and at the very minimum can rule out locations for ground search," Rollins says. "One of our very first cases involved using it to for exterior observation in an active shooter barricade situation.

"Has our program been successful since it became operational? Successful is a difficult word to categorize. We are bound by some difficult FAA guidelines and we strictly abide by their rules, and I feel like we're pretty respected in the FAA hallways. They use us as a model agency. So, yes, we are quite successful, but vigilant of FAA rules and upcoming changes."

Rollins adds that maintaining full compliance means Arlington's deployments are reduced, and that all officers involved in the program have pilot's licenses because all flights take place in controlled airspace. Arlington also is in the process of applying for an additional COA for a smaller, lighter quadcopter that seems better suited to its needs, because, he says, "As with any technology, it keeps improving. You buy a new computer, you walk out of the store, and it's out

of date. The same is true of UAS; they keep getting a little smaller, a little faster, a little less expensive to operate.”

Because an agency must first buy equipment, then apply for a COA, Rollins says Arlington probably started off with more UAS equipment than it needed.

“With most equipment, you test and make sure of what you want before you buy, but the FAA says buy first, then apply for the COA. We now have an opportunity to lessen the equipment and reduce the burden on the taxpayers, and we want to take advantage of that.”

In addition to what they’ve learned about upgrades in technology, Rollins and his team have learned other lessons about operating a UAS program:

- Know your political climate. Rollins says Arlington has a reputation for procedurally just policing, and its residents feel there is a sense of legitimacy in department operations.
- Maintain open communication with the community.
- Don’t consider a UAS to be a surveillance tool. “In its most rudimentary form, it’s a camera that will lift off the ground and help reconstruct a crime scene or check out a rooftop. It’s not designed to violate anyone’s privacy,” Rollins says.
- Be aware of FAA restrictions and follow them. Create good two-way communication with the agency.
- Take your time and shop your vendors. Establish a good relationship with continued communication.
- Expect to have to replace parts; for example, a windy landing may flip the UAS over and break the rotor blades. Remember that UAS are small and have many breakable parts.

“We’re very fortunate that the community backs our use of the UAS, and we’re very happy to have our program, even with the restrictions,” Rollins says. “As more agencies establish programs, we feel upcoming FAA rulemaking will reduce many of these restrictions.”

*To learn more about Arlington’s UAS program, contact Sgt. Brook Rollins at [UAS@arlingtontx.gov](mailto:UAS@arlingtontx.gov). For more information on use of UAS and other aviation technology by law enforcement, contact Mike O’Shea of the National Institute of Justice at [michael.oshea@usdoj.gov](mailto:michael.oshea@usdoj.gov).*

## **Technology Enhances Capture of Latent Fingerprints and Other Forensic Evidence**

By Michele Coppola

*A Florida sheriff's office is using sophisticated imaging technology to assist with the location, collection and processing of latent fingerprints and other crime scene evidence, such as bodily fluid and gunshot residue.*

The Pinellas County Sheriff's Office obtained the lab station and mobile versions of the full spectrum imaging system in early 2015, using a grant from the National Institute of Justice Paul Coverdell Forensic Science Improvement Grants Program.

Using the system, forensic science specialists can locate and view untreated fingerprints and other evidence using a range of options, from shortwave ultraviolet light to visible light to infrared. Fingerprints that are found are photographed using a 16 megapixel camera, capturing images at 1,000 dpi, resulting in a digitally superior latent print.

The system allows forensics investigators to find latent fingerprints on surfaces and documents that have not been treated with conventional powder or chemicals, thus preserving the integrity of the evidence, according to Greg Mason, forensic science manager.

"It gives us another tool or processing technique to locate latent fingerprint evidence that has been untreated and, therefore, it is nondestructive to the evidence itself," Mason says. "We go into a lot of people's homes where someone has broken into a house and gone through important documents. If we were to use a chemical process on a document that was touched by a perpetrator, we could potentially destroy it due to the nature of the chemical. So, this gives us a chance to get the perpetrator's prints without destroying the evidence."

"And it is fast," he adds. "Most chemical processing techniques take up to 24 hours for best results. With this technology, once we get evidence in the lab, we can scan the item using the shortwave UV light and have any results to latent print examiners in 10 to 15 minutes, if required."

If needed, latent print evidence can be processed further with powders, chemicals or dye stains after initially using the imaging system.

The technology can also be used to locate bodily fluids, hair, bone fragments and other forensic evidence. Use of the technology is not case specific, and investigators have used it in a variety of crimes including homicides, robberies, burglaries and grand theft auto. Since purchasing the system, forensic science specialists have used the system in more than 200 cases, but it is not always successful.

"We don't always get positive results when viewing evidence because there is not enough fingerprint residue on the actual evidence," Mason explains. "Everyone has a different chemical makeup and that is true for fingerprints as well. Some people have more fingerprint residue, which is made up of water, oil, amino acids and chlorides, to name a few. Therefore, it depends

on the residue left behind on a piece of evidence that plays a huge factor in locating the untreated fingerprint evidence.”

The system’s infrared capabilities helps investigators determine if documents have been altered, such as checks or cash; if blood spatter or blood stain patterns are present on dark or multicolored surfaces; if possible gunshot residue is located on an item of clothing; or even bruising to a person. The cost of the lab version was approximately \$40,000, and the mobile system was slightly higher. The federal grant covered the cost of both systems.

Pinellas County, with a population of about 938,000, is located on the west coast of Florida. It has one of the largest forensic divisions in the southeast United States, with 27 forensic science specialists, seven supervisors and a division manager.

*For more information, contact Greg Mason at [gmason@pcsonet.com](mailto:gmason@pcsonet.com). For information on the National Institute of Justice Paul Coverdell Forensic Science Improvement Grants Program, go to <http://www.nij.gov/topics/forensics/lab-operations/capacity/nfsia/pages/welcome.aspx>.*

## **TechShorts January 2016**

TECHshorts is a sampling of the technology projects, programs and initiatives being conducted by the Office of Justice Programs' National Institute of Justice (NIJ) and the National Law Enforcement and Corrections Technology Center (NLECTC) System, as well as other agencies. If you would like additional information concerning any of the following TECHshorts, please refer to the specific point-of-contact information that is included at the end of each entry.

In addition to TECHshorts, *JUSTNET News*, an online, weekly technology news summary containing articles relating to technology developments in public safety that have appeared in newspapers, newsmagazines and trade and professional journals, is available through the NLECTC System's website, [www.justnet.org](http://www.justnet.org). Subscribers to *JUSTNET News* receive the news summary directly via email. To subscribe to *JUSTNET News*, go to <https://www.justnet.org/app/puborder/subscribe/subscribe.aspx>, email your request to [asknlectc@justnet.org](mailto:asknlectc@justnet.org) or call (800) 248-2742.

Note: The mentioning of specific manufacturers or products in TECHshorts does not constitute the endorsement of the U.S. Department of Justice, NIJ or the NLECTC System.

### **Technology to Help Police Communicate With the Hearing Impaired**

*Columbia Police Department*

A Missouri police department now has a technology tool to ease communication between officers and people who are hearing impaired.

The portable, wireless device has two keyboards and two screens, allowing face-to-face instant message communication between individuals, according Bryana Larimer, a spokeswoman for the Columbia Police Department. Users sit across from each other and the setup can ease direct contact between officers and the public.

"We have sign language interpreters, but we were also using pencil and paper to communicate with hearing-impaired individuals, which is not a very personable or direct way to communicate," Larimer says. "The device provides a means of building a rapport and enables us to have efficient interaction. We are not doing away with interpreters; the device will augment that capability."

Officers can use the device at the police station or in the field. Sometimes it can take a while for an interpreter to arrive at the station to help an officer communicate with a hearing-impaired person. Using the device, officers can begin communication before the interpreter arrives. The conversation can be saved, printed and attached to the case file.

Larimer, a civilian employee with the department, is familiar with the device because she used it a bit when she worked at the Thirteenth Judicial Circuit, Juvenile Division.

"It is extremely user friendly," she says. "Direct messaging, typing on computers is something many people are familiar with."

The Columbia Police Foundation purchased the \$2,000 tool for the police department in fall 2015. The foundation raises funds to support programs or purchase equipment for the department.

The department is authorized for 165 officers and currently has about 82 officers who work patrol, serving a population of about 116,900 people.

For more information, contact Bryana Larimer at [bgmaupin@gocolumbiamo.com](mailto:bgmaupin@gocolumbiamo.com).

### **FBI Active Shooter Report**

#### *Federal Bureau of Investigation*

An FBI study of active shooter incidents is intended to provide data to help first responders better prepare for and respond to such incidents. The report could also help others who could be in an active shooter situation by providing a better understanding of how these situations play out, according to the FBI.

The report, *A Study of Active Shooter Incidents in the United States Between 2000 and 2013*, examines 160 active shooter incidents that occurred between 2000 and 2013. The FBI, with assistance from Texas State University's Advanced Law Enforcement Rapid Response Training Center, studied each incident separately to identify its characteristics, and then correlated the data to obtain a fuller picture of active shooter incidents in general.

According to the report, the study is not intended to explore all facets of active shooter incidents, but rather to provide a baseline to guide federal, state, tribal and campus law enforcement, along with other first responders, corporations, educators and the general public, to a better understanding of active shooter incidents.

To read the report, go to <https://www.fbi.gov/news/stories/2014/september/fbi-releases-study-on-active-shooter-incidents/pdfs/a-study-of-active-shooter-incidents-in-the-u.s.-between-2000-and-2013>.