More and more, when it comes to investigating vehicle crashes, distance measuring tapes and wheels, hand-drawn sketches, and ink pens are out and computers and lasers are in.

“The days of going out and measuring skidmarks and using calculus to determine speed are over,” says Troy Krenning, a program manager at the National Institute of Justice’s National Law Enforcement and Corrections Technology Center (NLECTC)–Rocky Mountain in Denver, Colorado. “These data are now captured in the vehicle’s black box.”

According to William Mael, a transportation safety consultant in Fort Collins, Colorado, the technology for analyzing vehicle crashes had long remained relatively unchanged. However, Mael says, “Starting about 3 to 5 years ago, much of the technology became computer-related or laser-related, requiring a higher level of training and exposure for law enforcement personnel.”

“Onboard vehicle data recorders and other high-tech tools promise to make crash scene investigation faster, more efficient, and more cost effective, but many departments lack the expertise to use them,” Krenning says. To help bring law enforcement agencies up to speed on current crash scene technologies, NLECTC–Rocky Mountain last year initiated a technology assistance program titled “Crash Scene Technologies,” which is available to law enforcement agencies at no cost.

Last year, Krenning says, approximately 120 officers from Colorado, Montana, and Kansas took the week-long course, a mix of classroom presentations and hands-on exercises designed for experienced crash scene investigators dealing with major accidents. NLECTC–Rocky Mountain also is offering technology assistance in specific areas, such as motorcycle crash analysis and advanced reconstruction techniques. The crash scenes technology course is presented by Mael along with Bob Rood, a Colorado State Patrol specialist in major collision investigations. It presents a broad spectrum of technologies, but without promoting specific products.

“There are probably 10 different companies that make measuring devices and 30 different companies that make computer-aided drafting (CAD) programs for law enforcement,” Mael says. “Police agencies are inundated with these things and don’t necessarily know how to choose which they want to use.”

In a recent television commercial a stressed-out office worker takes his laptop to a park and uses his wireless access connection to meet his deadline as he basks in the warm sunshine. Other television and radio advertisements promote the same message: wireless connections make life more convenient, faster, easier. But these commercials do not mention the hidden dangers that every consumer—and every law enforcement officer—should watch for.

Statistics released by the Federal Bureau of Investigation in 2003 show that “cybercrime” rates increased for the third straight year. Although most people know about financial fraud, identity theft, and the dangers hackers can pose to conventional systems and networks, most are unaware of the unique risks from the use of wireless access technology. Staff at the National Institute of Justice’s CyberScience Laboratory (CSL) in Rome, New York, know the risks and want to share this information with law enforcement agencies across the Nation.

Search the Internet for information on wireless technology and you will be overwhelmed by the huge amount of...
Many new laptop computers have built-in wireless adapter cards. These cards also can... How do you obtain wireless access? Wireless connections allow users to access a network from virtually anywhere: home, offices, and anywhere. Why use wireless? Wireless access technology uses radio communication to allow any computer, not only laptops and personal digital assistants (PDAs), to access a network. What basic steps can users take to protect themselves?... What is WarDriving? WarDriving derives from the term “WarDialing” used in the 1983 movie War Games, in which a teenager uses his computer to dial blocks of numbers in search of a way to break into a video game company’s systems. It refers to driving, walking, biking, or otherwise cruising around looking for open access points. WarDrivers often use one of many Wi-Fi detection programs available for free from the Internet. Although many WarDrivers do this simply for fun, others have malicious intent. WarDrivers generally...
antenna. Officers should also watch for GPS units and/or laptops connected to the GPS, the antenna, or a can. Anyone using a laptop in a car would arouse my suspicions, period, especially if the car is moving.

“If an officer pulls over someone whom they suspect of WarDriving, he or she should note the time and the license number and report it to whoever in their department handles cybercrime issues. It might prove to be useful information a week, or even a month later, because it might take the victim that long to realize something has happened,” he adds.

However, these subtle warning signals can be hard to spot. For that reason, CSL staff encourage officers—and consumers—to learn about wireless security and take all the steps they can to safeguard their wireless access. Officers can start by contacting CSL or registering at www.cybersciencelab.com to download Introduction to Basic Networking, Introduction to the 802.11 Wireless Network Standard, and Security Threats to the 802.11 Wireless Network. These three reports (one of which includes a glossary of basic wireless networking terms) meet the needs of most law enforcement professionals. CSL staff are preparing more advanced documents to supplement these reports.

“We’re just interested in getting the information out to State and local law enforcement. If you go to a company website, they’re going to plug their products. We’re not interested in doing that,” DeCarlo says. “We see ourselves as the resource in this area for law enforcement and corrections agencies that need help, and our specialists really know this stuff.”

For more information on wireless access and issues, cybercrime in general, or the CyberScience Laboratory, contact Joshua Bartolomie, 315–838–7057 or Josh@DolphTech.Com; Jeffrey Isherwood, 315–838–7064 or Ish@DolphTech.Com; or Robert DeCarlo, Jr., 315–330–2489 or robert.decarlo@rl.af.mil.

“IT’s the perfect way to perform identity theft.”

need to be within 300 feet of equipment to detect a wireless access point, although if they have high-powered antennas at their disposal, they could be miles away.

What is the IEEE?
◆ The Institute of Electrical and Electronic Engineers (IEEE) establishes standards for wireless use, including the 802.11 set of wireless access standards. Members of this group of academics and technology professionals work together to adopt and refine protocols and operational standards for many types of community technology.

What is the 802.11 standard?
◆ IEEE has approved three related standards for wireless networking: 802.11a, 802.11b, and 802.11g. (Other standards are in development.) Equipment that meets any of the 802.11 standards falls into the category of WiFi devices. Any equipment carrying the WiFi trademark from the Wireless Ethernet Compatibility Alliance is guaranteed to operate with at least base functionality.

◆ WiFi uses unlicensed spectrum in the 2.4 GHz range, except for 802.11a, which uses the 5 GHz licensed frequency range. This spectrum originally was left unlicensed so it could be used by microwaves and similar equipment, but many other devices now use this spectrum. The 802.11 standard specifies connectivity at 11 megabits per second (Mbps), compared to 9.6 kilobits per second for older cellular phones. Current phones can connect at hundreds of kilobits per second.

◆ Most wireless access equipment used in the United States meets the 802.11b standard, operating on a frequency of 2.4 GHz at a maximum speed of 11 Mbps. Devices meeting the 802.11a standard operate at a frequency of 5 GHz at speeds of up to 54 Mbps. Because 802.11b and 802.11a equipment operate on different frequencies, they are not compatible. Devices that meet the 802.11g standard operate at the 2.4 GHz frequency of 802.11b and the 54 Mbps speed of 802.11a; therefore, they are backwards compatible with 802.11b devices. Although all U.S. devices that meet the same standard should work together, this may not be true outside the United States.
TechBeat is the award-winning newsmagazine of the National Law Enforcement and Corrections Technology Center (NLECTC) system. Our goal is to keep you up to date with current and developing technologies for the public safety community, as well as other research and development efforts within the Federal Government and private industry. TechBeat is published four times a year.

**Individual Subscriptions:** TechBeat is available at no cost. If you are not currently on our mailing list, please call us at 800–248–2742, fax 301–519–5149, or e-mail us at asknlectc@nlectc.org.

**Domestic Department Subscriptions:** If your division, department, or agency has more than 25 individuals, we can drop ship as many copies as you require. All you have to do is provide us with the quantity needed, a shipping address (no Post Office boxes, please), and a contact name and telephone number. Your only obligation is to disseminate them once they arrive. If you require fewer than 25 copies, please provide us with the names and addresses of individuals who are to receive the newsmagazine and we will send copies directly to them. Contact Rick Neimiller, TechBeat managing editor, at 800–248–2742, for additional information or to subscribe.

**Address Correction:** Please notify us of any change in address or point of contact. Call 800–248–2742; fax 301–519–5149; or e-mail asknlectc@nlectc.org.

**Article Reproduction:** Unless otherwise indicated, all articles appearing in TechBeat may be reproduced. We do, however, request that you include a statement of attribution, such as: “This article was reproduced from the spring 2004 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the National Institute of Justice, 800–248–2742.”

**Awards:** TechBeat has received numerous awards, including the 1998 Best of Category, Excellence in Printing Award from the Printing & Graphic Communications Association; the first-place 1998 Blue Pencil Award for Most Improved Periodical from the National Association of Government Communicators; the 1999 Silver Inkwell Award of Merit from the International Association of Business Communicators; and the APEX 2001 Award of Excellence for Magazines and Newspapers–Printed.

**Photo Credits:** Photos used in this issue of TechBeat copyright © 2004 PhotoDisc, Inc.; Thinkstock; and Artville.

**Staff:** Managing Editor, Rick Neimiller; Writers, Becky Lewis, Jackie Siegel, and Warren Smith; Editor, Michele Coppola; Assistant Editor/Writer, Brian Higgins; Graphic Designers, C. Denise Collins and Tina Kramer.

For help establishing an Internet connection, linking to JUSTNET, or finding needed technology and product information, call the NLECTC Information Hotline at 800–248–2742.
An officer stops a car for a traffic violation and asks the driver for identification. The man says he must have left his wallet at home, but his name is John Smith and he lives at 222 Any Street. The officer nods, then pulls a compact device from his belt and asks the driver if he minds undergoing a fingerprint scan. The driver, who has heard about these scanners, grudgingly extends his finger, muttering that his name is really Bob Jones and he lives at 333 Some Street.

According to Lt. Steve Duke, word about these scanners is on the street, at least in Ontario, California, where officers began using the system in 2003. During its first 6 months of operation, officers used the department’s Information-Based Identification System (IBIS) [also known as Integrated Biometric Identification System] 3,737 times to identify 816 individuals and detain 164. In Hennepin County, Minnesota, during the same period, sheriff’s deputies used the system 679 times, identifying 110 individuals and detaining 37.

Developed and produced by Identix Incorporated through a grant program of the National Institute of Justice (NIJ), the system scans a subject’s finger and generates a forensic-quality fingerprint on the scene, then searches databases to return identification results within 2 to 3 minutes. Without this device, it can take an officer several hours to verify a subject’s identity. Both Duke and Robert Hamborg, Hennepin County’s program manager, say that in the past, field officers sometimes had to release subjects because of this delay.

“The longer it takes to identify a suspect, the more paranoid that person may become,” says Duke, who heads the Ontario Police Department’s Administration Bureau, which includes the Technology and Special Projects Unit. He might stand there thinking, ‘They’re trying to find who I really am,’ and decide to attack the officer or make a run for it. Anytime you can reduce the time involved in the identification process, it’s a good thing.”

“Susperts give false identities to officers on the street,” Hamborg says. “Establishing true identity can create a substantial amount of additional work. Also, the wrong person could be released from custody because of confusion about identity. We are looking to IBIS to alleviate these problems. The technology should increase law enforcement officer safety and speed up identification.”

Using a fingerprint identification system to speed up identification could prove beneficial not only to law enforcement, but also to average citizens, Duke explains. “We recently stopped a man who said he left his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home. When the officers just ran his name, the search turned up an arrest record under his license at home.

The Ontario Police Department has plans for a voluntary fingerprint database (separate from the police database) that could be used to identify people with Alzheimer’s disease and other kinds of dementia who are lost. If officers found a protected individual wandering the streets, they could use the system for identification and call a family member or appropriate care facility.

This represents just one potential use, Duke says. “Like everything else, technology changes constantly. Just when I think it’s done, then someone thinks of more things that the IBIS could do.”

“Additional funding is being used to improve the product and to keep current with evolving technology,” says Joseph Cecconi, NIJ program manager for the project, originally called Squad Car Unit Identification (SQUID). Other possible improvements and applications suggested by Duke, Hamborg, and Cecconi include—

- Adding a database of latent fingerprints from local crime scenes.
- Using a fingerprint system as a mobile booking station.
- Identifying people entering and leaving detention facilities.
- Improving internal airport security.

Adapting to changes in wireless technology and other improvements kept IBIS in development for several years. Both Ontario and Hennepin County began testing in 1999 and went fully operational in early 2003. Even after its system became operational, Hennepin County upgraded its fingerprint database and received more scanners. Hamborg says the process had glitches, including a hard drive failure. However, everything worked out and Hennepin County distributed scanners to an additional 20 partner agencies in the Minneapolis-St. Paul area.

That potential exists at least in part due to the ease of use incorporated into the system design. The scanner’s pistol grip allows for one-handed operation, and its wireless connection means officers need not return to their squad cars to access databases. Its design makes it usable by officers mounted on horseback, bicycle, or motorcycle, and its weight of less than 2.5 pounds includes the battery pack, which allows for 3 hours of continuous operation and 14 hours of standby operation.

Duke says learning to use IBIS takes only 2 to 3 hours, and his officers like that it does not compromise their ability to defend themselves.

Because of that ease of use as well as other factors, Cecconi says NIJ hopes that this program “will result in more widespread use by law enforcement agencies throughout the country.” Its present cost and durability might make it prohibitive for some law enforcement agencies, but that could change with future versions.

For more information on the IBIS program, contact Joe Cecconi, 202–395–7959 or ceccconi@ojp.usdoj.gov; Lt. Steve Duke, 909–395–2711 or sduke@ontariopolice.org; or Robert Hamborg, 763–525–6203 or Robert.Hamborg@co.hennepin.mn.us.
Contact NLECTC for:

Technology Identification
The NLECTC system provides information and assistance to help agencies determine the most appropriate and cost-effective technology to solve an administrative or operational problem. We deliver information relating to technology availability, performance, durability, reliability, safety, ease of use, customization capabilities, and interoperability.

Technology Assistance
Our staff serve as proxy scientists and engineers. Areas of assistance include unique evidence analysis (e.g., audio, video, computer, trace, and explosives), systems engineering, communications and information systems support (e.g., interoperability, propagation studies, and vulnerability assessments).

Technology Implementation
We develop technology guides, best practices, and other information resources that are frequently leveraged from hands-on assistance projects and made available to other agencies.

Property Acquisition
We help departments take advantage of surplus property programs that make Federal excess and surplus property available to law enforcement and corrections personnel at little or no cost.

Equipment Testing
In cooperation with the Office of Law Enforcement Standards (OLES), we oversee the development of standards and a standards-based testing program in which equipment such as ballistic- and stab-resistant body armor, double-locking metallic handcuffs, and semiautomatic pistols is tested on a pass/fail basis. NLECTC also conducts comparative evaluations—testing equipment under field conditions—on patrol vehicles, patrol vehicle tires and replacement brake pads; and cut-, puncture-, and pathogen-resistant gloves. NLECTC also has evaluated emerging products to verify manufacturers’ claims. The primary focus of OLES is the development of performance standards and testing methods to ensure that public safety equipment is safe, dependable, and effective.

Technology Demonstration
We introduce and demonstrate new and emerging technologies through such special events, conferences, and practical demonstrations as the Mock Prison Riot (technologies for corrections), Operation America (bomb detection technologies), and an annual public safety technology conference. On a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

Capacity Building
We provide hands-on demonstrations of the latest technologies to address such operational issues as crime and intelligence analysis, geographic information systems, explosives detection and disassembly, internal disturbances and riots, and computer crime investigation.

Technology Information
NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, news summaries, meeting/conference reports, videotapes, and CD-ROMs. NLECTC also publishes TechBeat, an award-winning quarterly newsmagazine. Most publications are available in electronic form through the Justice Technology Information Network (JUSTNET) at www.justnet.org. Hard copies of all publications can be ordered through NLECTC’s toll-free number, 800–248–2742, or via e-mail at asknlectc@nlectc.org.

Technology Commercialization
Our law enforcement and corrections professionals, product and commercialization managers, engineers, and technical and market research specialists work together to identify new technologies and product concepts. They then work with innovators and industry to develop, manufacture, and distribute these new, innovative products and technologies.

Technology Needs Assessment
Our national body of criminal justice professionals—the Law Enforcement and Corrections Technology Advisory Council (LECTAC)—ensures that we are focusing on the real-world needs of public safety agencies.

NLECTC—National
2377 Research Boulevard
Rockville, MD 20850
800–248–2742
asknlectc@nlectc.org

NLECTC—Northeast
26 Electronic Parkway
Rome, NY 13441–4514
888–338–0984
nlectc_ne@afmail

NLECTC—Rocky Mountain
420 East 7th Avenue
Denver, CO 80208
800–416–4866
nlectc_ro@jhu.edu

NLECTC—West
c/o The Aerospace Corporation
2350 East El Segundo Boulevard
El Segundo, CA 90245–4691
888–546–1618
nlectc_law-west.org

NLECTC—Northeast
300 C Street, Suite 304
Anchorage, AK 99503–3975
866–569–2969
nlectc_ne@nlectc.net

NLECTC—Southeast
5300 International Boulevard
North Charleston, SC 29418
800–202–4385
nlectc_se@nlectc-se.org

Border Research and Technology Center (BRTC)
1010 Second Avenue, Suite 1920
San Diego, CA 92101–4912
888–506–2922
info@brtc.nlectc.org

Rural Law Enforcement Technology Center (RULETC)
101 Bulldog Lane
Hazard, KY 41701
866–787–2553
ruletc@rail.com

Office of Law Enforcement Standards (OLES)
100 Bureau Drive, Stop 8102
Gresham, OR 97030
503–971–2575
oles@bfs.gov

NLECTC—Northwest
2350 East El Segundo Boulevard
Long Beach, CA 90801
888–338–0584
nlectc_nw@nlectc.net

NLECTC—Northwest
300 C Street, Suite 304
Anchorage, AK 99503–3975
866–569–2969
nlectc_nw@nlectc.net

Contact NLECTC for:
From the Department of Justice, it is pursuing $6...
For more than 5 years, the National Institute of Justice (NIJ) has sponsored two annual Technology Institutes—one specifically for law enforcement personnel; the other for corrections personnel.

Both Technology Institutes are held in Washington, D.C., and run for 5 days, during which participants receive information and assistance on existing and developing technologies, work through problems relating to technology implementation, and exchange technology lessons learned of importance to law enforcement or corrections. In addition, those attending receive briefings and demonstrations at various agencies and departments in the metropolitan area.

Participants from across the country bring to the Institute questions, technology problems and solutions, and a desire to do their jobs more efficiently and effectively.

There is no cost for either Institute, and all travel, food, and lodging expenses are covered. However, only 25 to 30 individuals are selected to attend (no previous attendees, please). Applications and additional information for both Technology Institutes are available online at www.justnet.org or by calling 800–248–2742.
The beep-beep of an emergency broadcast sounds on the radio...a funnel cloud has been spotted. Pleasant Valley Elementary School, in Calhoun County, Alabama, at once implements its severe weather plan. Administrators turn to a nearby computer and access vital information stored in the school’s SCORMAP program—information about student attendance, emergency exits, and utility shutoffs.

Although this scenario remains hypothetical, Pleasant Valley Elementary and other schools in Calhoun County have become the Nation’s test bed for SCORMAP, a mapping software program that uses Geographic Information Systems (GIS) and Computer Assisted Drawing (CAD) technologies to put detailed information at school administrators’ fingertips. Its objective is not only to promote school safety but to help administrators, school resource officers, and local law enforcement in emergencies.

SCORMAP is based on CORMAP, an application for correctional facilities developed in 1999 by the National Institute of Justice’s National Law Enforcement and Corrections Technology Center (NLECTC)-Southeast and the U.S. Department of Energy’s Savannah River Technology Center (SRTC). Until recently, a major hurdle to mapping multistory buildings such as prisons or schools was the duplicate, room-above-room construction, which GIS could not map alone. In cooperation with SRTC, NLECTC-Southeast overcame this problem by integrating CAD and GIS technologies. Now, multilevel areas can be displayed in a three-dimensional layout. Each room (or cell) on each floor becomes a separate, identifiable unit that can be displayed on a computer screen.

According to Lisa Russell, information technology director for Calhoun County Schools, school mapping began early last fall, but it will take several years to map every school in the county. With almost 20 schools in the system, Pleasant Valley Elementary School was chosen as the starting point because this small new school already had some of the necessary information digitized.

Rob Donlin, project manager for corrections and school safety at NLECTC-Southeast, says Calhoun County Sheriff Larry Amerson got the SCORMAP project rolling by introducing Russell to Donlin. “Sheriff Amerson knew about CORMAP because Rob Donlin helped him map the local jail. He knew we were forward thinking, and he put us together,” Russell explains. Donlin met with Russell and Calhoun County’s Safety and Security Director Mike Fincher in fall 2002. They agreed to start when the next school year began.

“Because the school system’s funds for this type of project are limited, we were very glad to receive technology assistance from NLECTC-Southeast,” Russell says. “All in all, this is a good partnership. Rob Donlin and his team have been helpful as a general school safety resource in addition to helping with the mapping.” NLECTC-Southeast helped Fincher attend a national conference on campus safety, and he came back with more ideas for improving safety in Calhoun County schools.

“This kind of partnership bleeds over into a lot of other opportunities,” Russell says. “Even though it will take several years to put [SCORMAP] completely into place, we couldn’t have done it on our own, because we don’t have the resources.”

Donlin says CORMAP required a few modifications to morph into SCORMAP, for the most part adding passwords so that only authorized personnel could access such student-specific information as medical records. Also, although CORMAP used inmates’ assigned beds as their “location address,” SCORMAP uses desks for elementary school students and lockers for secondary school students.

SCORMAP has the capability to store any information school administrators think they may need. “We map physical aspects, but we also track student characteristics,” Donlin says. “If a child turns up missing, the system can help track him down by showing, for example, that he didn’t get on the bus to go home.”

Information stored in SCORMAP includes fire evacuation routes, severe weather holding areas, water and electrical shutoffs, air conditioning and heating shutoffs, breaker boxes, and fire extinguishers. Russell says that she knows access to this information in an emergency could prove vital to Calhoun County’s school resource officers and local law enforcement.

For more information on SCORMAP and CORMAP projects, contact Rob Donlin at the National Law Enforcement and Corrections Technology Center-Southeast, 800-292-4358 or donlin@nlectc-se.org. For information on Calhoun County Schools’ experience with SCORMAP, contact Lisa Russell, 256-741-7475 or lrussell@calhoun.k12.al.us.
The course, Mael says, covers three basic areas:

- Mapping technology, including tools that capture data on the scene, and computer-aided drafting or mapping software that diagrams the scene. “We actually go outside and do a mock scene,” says Mael. “Then participants have to create a usable map.”

- Black box technology, including a field trip to a salvage yard to extract data from a black box onboard a wrecked vehicle. Depending on the manufacturer, the black box yields such information as how many people were in the car, how fast it was going on impact, and whether or not the seatbelts were buckled.

- Reconstruction management and calculation software that performs the calculations and analysis of field data. Mael says that one of the CAD programs that is demonstrated has the capacity to do the velocity equations as you do diagrams.

In the past, low-tech tools such as measuring tapes and scratch pads led to less-than-accurate results, Krenning notes. Today, a point-and-shoot laser rangefinder about the size of a radar gun can measure distances to within one-tenth of an inch and then download the data into a handheld unit similar to a personal digital assistant. With proper training, a single officer can diagram and chart an entire scene in a fraction of the time it would have taken a team of investigators using manual methods. The techniques also can be applied to other types of crime scenes.

This year, NLECTC–Rocky Mountain is offering the course throughout its 10-State region that includes Colorado, Kansas, Montana, Nebraska, New Mexico, North and South Dakota, Oklahoma, Texas, and Wyoming. In addition, courses geared toward prosecutors are in development.

For more information about “Crash Scenes Technologies,” including scheduling, contact Troy Krenning at NLECTC–Rocky Mountain, 800–416–8086, 303–871–4369, or tkrennin@du.edu.