

Expert: 'Flasher' technology digs deeper for digital evidence

New cybersleuthing technology, already solving crimes in Europe, has the potential to unlock valuable information in thousands of crimes every year in the United States, says a Purdue University expert.

The "flasher boxes" provide deeper access to data -- complete extraction and examination of all the information on a wide range of cell phones. Rick Mislan, an assistant professor of computer and information technology, has integrated the flasher boxes into coursework for a digital forensics class in Purdue's College of Technology.

"The fact is that cell phones are ubiquitous in today's world, and nearly all crimes have a digital component to them," Mislan said. "To be savvy at solving these crimes, we must be one step ahead of criminals in terms of finding, retrieving and interpreting evidence they may be trying to hide in digital devices.

"To get ahead, we must think out of the box, and that is just what we've found that our European counterparts are doing."

The difference between a flasher box and methods now used to retrieve information from digital devices is that the flasher technology allows direct access to everything stored in memory, such as incoming and outgoing calls, text messages and deleted files.

"Currently, investigators are relying upon software that allows them only to issue a specific command and receive only that information," he said. "With the flasher box technology, investigators can plug the cell phone into the box and the entire contents -- including contacts, call history, and deleted images and videos -- spill out into the computer.

"Having direct access to everything that may have existed in the phone is extremely important in criminal cases."

Mislan, a former U.S. Army electronic warfare officer, said another advantage of this method is that some cell phone models don't respond to current command-based forensics methods, but the direct memory access method would eliminate most of those problems.

"Using a flasher box is like taking a snapshot of the cell phone," he said. "This method shows a lot of promise."

Mislan learned about the technology from Steve Hirst and Steve Miller, both constable detectives for the West Yorkshire Police Department who specialize in high-tech crimes. He met the two through a mutual friend during a visit to Michigan. The detectives shared some of the methods that they have been using for several years.

"The United Kingdom and most of the rest of Europe are, and always have been, far ahead of us in terms of mobile forensics because their networks are standardized as GSM (Global System for Mobile Communications)," he said. "In the United States, we work with several different cellular network technologies - GSM, CDMA (Code Division Multiple Access) and iDEN (Integrated Digital Enhanced Network) - which makes any method of retrieval more challenging."

Mislan said the technology works by plugging the cell phone into the flasher box and downloading the files onto a computer. What results is a mass of letters and numbers that, to the naked eye, make no sense. With

the right mathematical translation, however, an investigator can turn the code into valuable information.

He said the key to success with this particular method is finding the correct software and cables that match the wide variety of phones on the market today. Mislan believes that the flasher box technology can work on a wide variety of cell phones, but it's currently a matter of understanding the memory mapping of the cell phone and then writing the software for the extraction of that memory.

He said students in his class are being exposed to the latest technology in digital forensics investigation and are learning information that many professionals aren't yet familiar with.

"We're giving them real-world experience that not even the law enforcement community in this country is familiar with," he said. "We're the only university in the country that I am aware of that is testing the flasher box technology."

He said a \$240,000 grant he received last year from the National Institute of Justice is allowing him to purchase many of the latest models of cell phones to help increase their knowledge about the various technologies.

In addition to investigators from the United Kingdom, Mislan has been learning about this technology from Ronald van der Knijff, an expert in embedded forensics from the Netherlands Forensic Institute, and Svein Willassen, formerly of the institute. An article co-written by van der Knijff that details this technology will be published in the May issue of the *Small Scale Digital Device Forensics Journal*, of which Mislan is an editor. The journal can be accessed online at <http://www.ssddfj.org>.

Mislan said he frequently helps investigators, including those from various surrounding local and state police and sheriff's departments, retrieve digital information from cell phones, PDAs and smartphones, and this new technology will allow possibilities for even more collaborations.

"Our ultimate goal with this is to be able to train officers to use this technology on a regular basis," he said. "Our country in general is far behind when it comes to cell phone investigations, but by sharing information and collaborating with those overseas, the good news is that we can emulate a lot of what they are doing and stay on top of the ever-changing world of cell phones."

Digital forensics is a graduate program in the college's Department of Computer and Information Technology. The department provides training for police officers, crime scene investigators, federal agents and other law enforcement personnel and has partnerships with the National White Collar Crime Center and the National Institute of Justice's Electronic Crime Partnership Initiative.

Source: Purdue University

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.