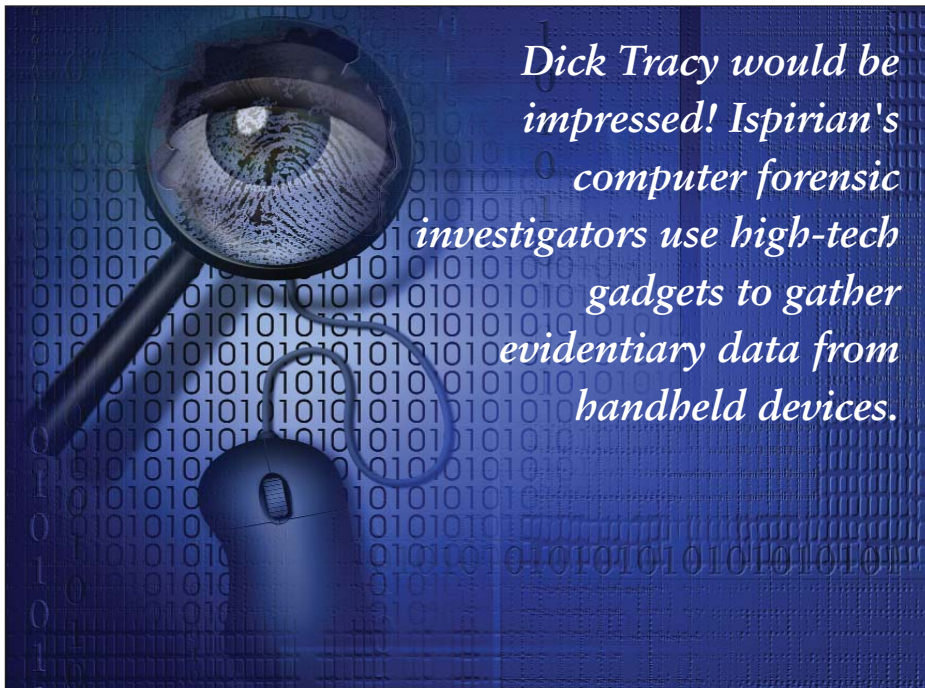


St. Louis Technology News

THE TECHNOLOGY SPIRIT OF ST. LOUIS™

TECHNOLOGY SOLUTIONS AND STRATEGIES FROM ISPIRIAN, SYLLOGISTEKS® AND ULTRATECH

Digital Detectives



Dick Tracy would be impressed! Ispirian's computer forensic investigators use high-tech gadgets to gather evidentiary data from handheld devices.

With his use of forensic science and sophisticated gadgetry, comic strip sleuth Dick Tracy was in many ways ahead of his time. His famous two-way wrist radio foreshadowed the modern cell phone, and computer forensic investigators now use Dick Tracy-like gear to tap the data stored on today's handheld communications devices.

Cell phones, GPSs, PDAs and other handheld devices are really tiny computers that contain a wealth of information. Any incident involving computer forensic investigation may require the seizure of handhelds, which must be handled differently than PCs or servers.

"You have to protect against unwanted wireless signals that could otherwise contaminate the evidence that might be stored on these types of devices," said Ispirian's Tom Smith, a forensic scientist and a member of the American College of Forensic Examiners Institute of Forensic Science. "We use very specialized tools to protect the

continued on page 2

St. Louis Technology News

PRSR1 STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146



Most commercial or free software is designed to not only view data but to upload data. This is not a safe way to perform a forensic evaluation. In fact, even some software marketed as forensic software warns of possible data loss. The software we use does not allow evidentiary data to be changed on the device.



Digital Detectives

continued from p. 1 ...

data until it can be examined using proper forensic procedures.”

Blocking Signals

At the outset of an investigation, computer forensic specialists must establish the proper “chain of custody” of the digital media. The case may not be going to trial, but the investigator must ensure that the media is not damaged or changed so that the extracted data can be used as evidence in court, if necessary. That means handheld devices must be shielded from radio frequency signals.

For examinations involving handhelds, Ispirian investigators can use a tool that is based on the science of the Faraday Cage — an enclosure made of a conducting material that blocks out external electrical fields. Many substances can block or hinder electronic transmissions, which is why your cell phone typically won’t work in an elevator. Probably the most familiar example of a Faraday Cage is the housing of a microwave oven, which prevents microwaves from escaping into the environment.

The Faraday Cages used in computer forensic investigations work on the same principle, except that they’re designed to keep signals out rather than in. One type of cage is constructed of .090-gauge aluminum, utilizing preci-

sion-machined tolerances to seal off radio frequencies.

“The entire interior is lined with RF absorbent foam, and the heavy-duty RF-sealed cover hinges open and close with a precision air piston,” said Smith. “The investigator has complete, hands-on access to the contents of the box using specially designed, silver impregnated, ultra-fine mesh gloves that offer excellent manual dexterity. A large viewing window overlooks the entire working area within the enclosure, which has built-in low-voltage lighting. It also includes a six-outlet power supply, since volatile data could be lost if the devices lack power.

“For field work as “first responders”, we typically use special evidence bags made of nickel-, copper- and silver-plated nylon woven fabric. This fabric shields the devices from unwanted wireless signals that could otherwise contaminate or eliminate data. When necessary, we also attach a battery powered remote charger to provide power, ensuring that seized devices remain powered and potential evidence is preserved.”

Extracting the Data

Once the devices are secure comes the task of extracting the data. Ispirian's lab policies advocate physical connections to the devices via plug-in cables, since Bluetooth and other wireless methods are inherently insecure and are inconsistent with the goal of protecting the devices from unwanted sig-

nals. In addition, physical acquisition yields more high-quality data than other methods, according to Ispirian.

Smith and other Ispirian forensic examiners then use sophisticated software to acquire and analyze the extracted data. The software used is designed specifically for computer forensics, and supports a broad range of devices.

“Most commercial or free software is designed to not only view data but to upload data. This is not a safe way to perform a forensic evaluation,” Smith said. “In fact, even some software marketed as forensic software warns of possible data loss. The software we use does not allow evidentiary data to be changed on the device.”

Smith and his team don’t battle villains like Pruneface and Flattop Jones — in fact, computer forensics is more likely to involve civil litigation or employee misconduct than dark crime. Nonetheless, Smith’s investigations have a sort of Dick Tracy flair, particularly when it comes to securing electronic devices.

“Whenever there is a handheld device involved in an incident, there are special procedures we follow,” said Smith. “We have to secure the device from unwanted wireless signals that could contaminate the data, control the chain of custody and use special software to extract the data without altering it. The key is to protect critical evidence that could make or break the case.”