Suffolk County Police personnel performing an annual calibration on some of the department's personal radiation detectors (PRDs).

Digital Evidence

By STUART CAMERON, M.S.

As today's officers know, sources of electronic data have grown exponentially with the popularity of, for instance, text messaging, social networking, and e-mail. This variety of data represents a key component of police investigations and a potential source of evidence that could prove critical in supporting the prosecution of different types of crimes. This highlights the importance of not only collecting such digital evidence but also having up-to-date procedures for its proper handling, archival, and maintenance, particularly to ensure its suitability for presentation in court.

Generating Data Files

Many types of equipment resulting from advances in technology exist that create additional electronic data files. For instance, the transition from conventional film photography to electronic methods has resulted in digital pictures that are electronic data files as opposed to negatives on a tangible piece of film. Similarly, each time personnel use a conducted energy device, such as a TASER, the unit creates a data file that

documents the number of times it was fired and the duration of each use. As yet another example, many departments now employ digital video cameras in their patrol units where the image actually is a series of ones and zeros as opposed to a magnetic recording on a piece of tape.

A lot of the detectors and sensors now used by hazardous materials response teams and bomb squads also create electronic data files. In an age of terrorism, suspects could go free if personnel do not properly document and save the digital evidence of these criminal acts. Terrorists who attempt to employ a weapon of mass destruction may face a trial in a conventional courtroom, rather than some other type of tribunal, such as a military commission. If this occurs, authorities will need to preserve and maintain the integrity of the evidence generated by these units in a manner acceptable under the criminal rules of evidence.

Additionally, newer instruments used by law enforcement, such as radiation detectors, radioisotope identification devices (RIID), gas meters, hazardous materials identification systems, and digital bomb X-rays, generate electronic readings and provide the opportunity to export them via a data cable or electronic memory card. While equipment operators certainly can testify, for instance, to what a meter said, prosecutors clearly would benefit from having the electronic file available to confirm this testimony. Agencies should identify all equipment they possess that creates this type of electronic data and have appropriate standard operating procedures in place.[1]

Preserving Electronic Evidence

Law enforcement personnel must properly preserve digital evidence to make it suitable for presentation in court. Techniques may vary depending upon the technology, but officers have several considerations. They must have a secure storage location; sufficient back-up copies, as lost evidence can place prosecutions in jeopardy; and proof that the data has not been altered—that it is authentic.[2] Officers must ensure the long-term integrity of evidence. Further, investigators need to recognize that the chain of custody is just as important with digital evidence as it is with physical types, and they should have a written log to document any occasions in which the media goes in or out of storage or changes hands. As one fairly simple means of preservation, personnel can transfer digital information onto a read-only, nonrewritable CD-ROM. Investigators should make two copies and ensure that they put on each disk the operator's name and signature, as well as the date and case number, and then treat each CD-ROM as they would any other item of

> ***"Law enforcement personnel must properly preserve digital evidence to make it suitable for presentation in court."***

Inspector Cameron is the commanding officer of the Suffolk County, New York, Police Department's Special Patrol Bureau in Ronkonkoma.

evidence, establishing a chain of custody and securely storing the media.[3]

Concerning detectors or sensors with a removable media card, at the scene of the investigation, officers can seal the card in an envelope with the operator's name and signature, the date, and the case number written on the outside. A secondary process involves uploading the data onto a secure server while employing a method, such as the hashing function, to ensure the data's integrity. Investigators then can store the card in a secure location.[4]

Personnel using electronic equipment must ensure the accuracy of the date and time displayed on the unit. In many instruments, the date and time will default to an earlier period if the batteries become depleted. Then, restoration of power can result in readings that appear out of sequence. Some detectors will not afford the operator the ability to reset the date and time without a computer interface cable. An improper reading from one instrument could result in members of the jury questioning the readings from others, and they may perceive incompetence or a lack of care on the part of the operator.

Due to the inherent time lag between arrest and prosecution, officers should recognize that data files stored for a particular item of equipment may need proprietary software to retrieve and read the display. Prior to a courtroom prosecution, the detector or sensor used to gather the evidence could be replaced with a more current model or one from a different manufacturer. Personnel must retain copies of the proper software unless they have saved the data files in a universal format or exported the results in hard copy format and maintained those results as evidence. If they do not maintain the proprietary software, investigators may not be able to open the archived data files. As a general rule, personnel should store digital evidence in its original, as well as nonproprietary, format to ensure accessibility.[5]

Most law enforcement officers know that they should use a clean sheet of paper, new notebook, or fresh roll of film to document each crime scene to prevent details from other cases commingling with the one at hand. This rule also applies to digital evidence, such as that produced by a sensor. Despite the reusability of some units of storage media, merely erasing them is insufficient; they must be forensically prepared, or wiped. Investigators must not only remove any vestige of the previous contents but also ensure that only known data

Digital bomb x-ray image of a suspicious package that appears to contain a hand grenade.

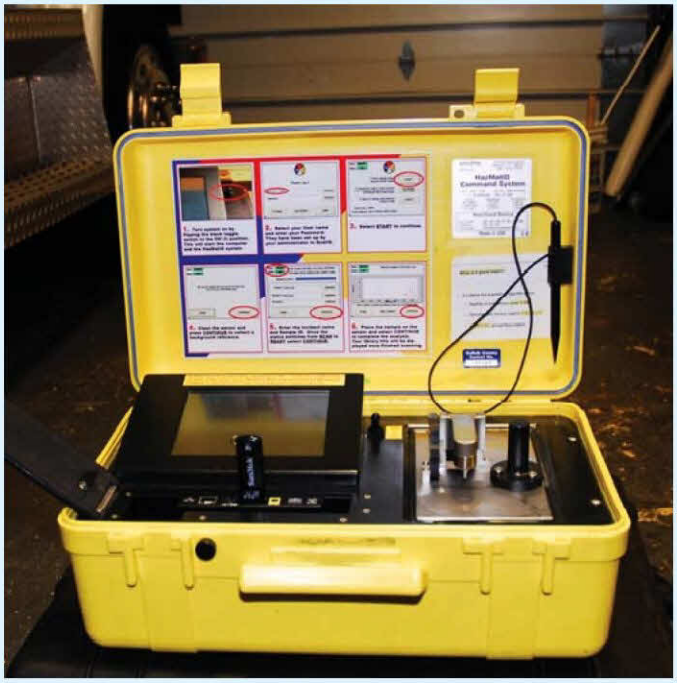
is written to each sector of the media. Personnel usually accomplish this with software that will overwrite a known character, such as 0 or 1, to the entire device and eliminate all of the previous data.[6] Agencies should be prepared with a mitigation strategy for detectors and sensors that store data internally if they intend to use the readings as digital evidence. If available, a similar device employing removable storage media may be easier to sterilize and would allow the original removable storage media to be archived, if necessary, without the loss of the entire instrument. Alternatively, a digital photograph could be taken of the relevant readings from the device's screen to document the events, and those digital photographs could be preserved.

Operators also should be aware that the names of the computer files exported by sensors often contain potentially important *metadata*, such as the sensor's unique identification number and the date and time of the file creation. Accordingly, personnel should not change file names in any way. Further, if a reading is taken and an error is made, the created data file should not be deleted. Rather, this error should be documented and later explained during the operator's testimony. Deleting files may create a gap in the sequential numbering system and could lead to the appearance that someone intentionally discarded the evidence.

Radioisotope identification device (RIID) connected to a laptop. This unit can identify various radioactive isotopes. The spectra files can be downloaded onto a laptop computer that has the proper transfer software installed using either a serial cable or a USB cable.

A bomb squad almost always will accompany radiological incident responders to rule out any threat of explosives. Many of these squads have made the transition from conventional film X-ray equipment to digital bomb X-ray devices. The results obtained from digital X-rays generally allow better analysis than conventional film counterparts, and, like digital photographs, personnel can electronically archive them for later presentation in court. Often, the digital X-ray is the only record of what a device looked like prior to the rendering of safe operations.

If the digital X-rays reside solely on the computer associated with the digital X-ray system, investigators would find it very difficult, if not impossible, to introduce them as evidence at a later date. Saving these images in a manner consistent with other digital photographs would mitigate this problem. Jurors generally will be familiar with electronic devices and may question the credibility of



HazMat ID system with a USB drive inserted into it. This system can identify thousands of different substances, and the results can be downloaded onto a USB drive.

an officer who could have, but did not, back up his testimony about a meter or sensor reading simply by downloading an electronic file. The lack of this digital evidence may not result in the loss of a conviction, but it could make obtaining one more difficult.

Documenting Terrorist Activity

A wide range of digital evidence can support a terrorism prosecution. For example, a thwarted attack using a radiological dispersal device could create a vast amount of evidence potentially lost without proper procedures and planning. In this case, the initial detection may have resulted from an officer's small belt-worn personal radiation detector. Investigators carrying these devices may not realize that an internal data-logging feature has stored the critical radiation readings, and their agencies might not expect them to know how to download this material as it often requires a computer interface.

While these detectors are relatively small, many of them log detections and save this data internally until the device becomes full, at which time the evidence can be overwritten. Data also can become lost if the batteries die. Thus, officers must have proper forethought and ensure that they save data quickly. Otherwise, this initial detection information could be forfeited, and the only record of it would be through the device operator's oral testimony without any further support.

The next step in the thwarted attack might be the use of an RIID to identify the type of radioactive material and its potential for harm. Certain radioactive isotopes work better than others in creating effective dispersal devices. Accordingly, the accurate identification of the isotope is critical in determining the danger posed. In this regard, RIIDs capture data and provide a preliminary assessment.

For a higher degree of assessment, during a process known as "reach back," officers can use this type of device to electronically transmit data within an e-mail to a *spectroscopist* who can "read" the digital signature created by the energy generated from the material and then analyze this data and verify the internal assessment from the RIID. This process creates a tremendous amount of potential digital evidence that personnel might overlook or delete unless they recognize it in advance.

The data file from the RIID, the e-mail message used to

transmit it, and any photographs sent all represent potential sources of digital evidence. Some agencies use an electronic template form to provide the incident background information during the reach back process, thereby creating more potential evidence.

Due to the critical nature of an incident, many departments use special operations commands to operate the identification devices. Because these personnel primarily focus on assessing a situation to resolve it without causing harm, agencies need to ensure they are trained to recognize that their assessment process is creating important digital evidence.

Calibrating and Testing Equipment

Creating usable electronic evidence also requires agencies to properly maintain and calibrate the instruments generating it, much like they service their speed-detection and alcohol-testing instruments. Of course, personnel need proper training to do this.

Departments also must retain records of calibration and repair for potential presentation to the court. While this process may seem complicated, agencies now consider it a matter of routine.

Additionally, officers who use these sensors and detectors must have knowledge of any set-up testing required before use. Personnel who have used radar guns for speed enforcement are well familiar with tuning-fork and internal-calibration checks that they must complete and document before deploying the device to issue tickets.

Similarly, many of the sensors and detectors used by hazardous materials teams and bomb squads require investigators to perform testing procedures before use. Agencies need to ensure that personnel not only perform the tests but record the results in the same way they do with enforcement equipment, recognizing the potential for usage data, such as material detection, to become crucial evidence needed in court. Departments should retain any documentation from the manufacturer, such as operator manuals, as controlled documents. Personnel also should test all equipment before use to ensure correct operation.

> ***Creating usable electronic evidence also requires agencies to properly maintain and calibrate the instruments generating it....***

Conclusion

Law enforcement agencies must establish procedures for handling digital evidence created through the advanced technology now commonplace in the profession. Taking the time to recognize and develop procedures for devices that create electronic files, establish standard operating procedures to properly save this downloaded data, and institute procedures that explain any deviations from established standards will aid the prosecution, instill confidence in jurors, and highlight the professionalism of law enforcement officers and their agencies. ✦

Endnotes

[1] Scientific Working Group on Imaging Technology (SWGIT); *http://www.theiai.org/guidelines/swgit/guidelines/section_15_v1-0.pdf.*

[2] Scientific Working Group on Imaging Technology (SWGIT); *http://www.theiai.org/guidelines/swgit/guidelines/section_1_v3-2.pdf.*

[3] Scientific Working Group on Imaging Technology (SWGIT); *http://www.theiai.org/guidelines/swgit/guidelines/section_13_v1-0.pdf.*

[4] Ibid.

[5] Scientific Working Group on Imaging Technology (SWGIT); *http://www.theiai.org/guidelines/swgit/guidelines/section_15_v1-0.pdf.*

[6] J. Philip Craiger, "Computer Forensics Procedures and Methods", *http://ncfs.ucf.edu/craiger.forensics.methods.procedures.final.pdf* (accessed September 2, 2010).