In the first of two short reports on recent developments in forensic software, we looked at the National Software Reference Library (NSRL) project described in the ITL BULLETIN from the National Institute of Standards and Technology (NIST) Information Technology Laboratory. In this report, we look at the Computer Forensics Tool Testing (CFTT) project.

* * *

Tools that are supposed to achieve a particular analytical purpose – e.g., intrusion detection software, firewalls, and antivirus products – need to be tested to see how well they work. Testing requires standards, and that’s what CFTT is designed for.

NIST has defined a framework for testing computer forensics tools which allows product developers and users to

* classify functions and requirements;

* specify details of these functional characteristics and user requirements; and

* define tests for measuring how well specific tools meet those standards.

Currently, project efforts are focused on disk imaging software. Disk imaging tools are critically important in preserving the chain of custody over evidence; with suitable affidavits, these bit-for-bit copies of hard disk drives are burned onto CD-ROMs so that the courts can have impeccable copies of the original data with no grounds for questioning their accuracy. Other projects for the future include password crackers (which help investigators access password-protected systems and files) and image-analysis tools (useful in locating information hidden by _steganography_ inside pictorial files).

The development process is highly interactive, with subject area experts involved at every step. Interim results are posted to the CFTT Website (http://www.cftt.nist.gov) for discussion and suggestions. The current disk imaging specification (version 3.1.1) was posted for comment to <http://www.cftt.nist.gov/teststat.html> on 13 July 2001. Eventually, specific forensic product test results will be published by the National Institute of Justice.

* * *

This kind of work illustrates the value of public-private partnerships in high technology. The NIST initiatives might be very difficult for any individual company to launch, and industry consortia can be cumbersome, in part because of competitive pressures and fears of being seen as a cartel in violation of anti-trust regulations. In addition, these NIST projects are breaking new
ground in an increasingly important area of computing: forensic analysis. As computer crime and abuse increases in our ever-more computerized society, law enforcement personnel and private investigators need to be able to track down and, if appropriate, prosecute malefactors.

Best wishes to the NIST team and their collaborators for continued progress!

* * *
For more information about computer forensics, visit

High Technology Criminal Investigation Association (HTCIA) <http://htcia.org/>

<more>

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.