CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Computer Forensics at NIST

How do I know my tools produce valid results?

The Computer Forensics Tools Verification project provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.

The testing methodology developed by NIST is functionality driven. The activities of forensic investigations are separated into discrete functions or categories, such as hard disk write protection, disk imaging, string searching, etc. A test methodology is then developed for each category. Currently we have developed a methodology for disk imaging tools and are developing a methodology for software hard disk write blocking tools. Deleted file recovery tools will be the next category for development of a test methodology.

www.cftt.nist.gov

How do I know the software is what it says?

The National Software Reference Library (NSRL) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information.

The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations.

www.nsrl.nist.gov

How can I do testing in my lab?

Reference data sets (CFReDS) provide to an investigator documented sets of simulated digital evidence for examination.

Investigators could use CFReDS in several ways including validating the software tools used in their investigations, equipment check out, training investigators, and proficiency testing of investigators as part of laboratory accreditation. The CFReDS site is a repository of images.

www.cfreds.nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

Homeland Security

NIJ

CERIAS

Discovery Park e-Enterprise Center