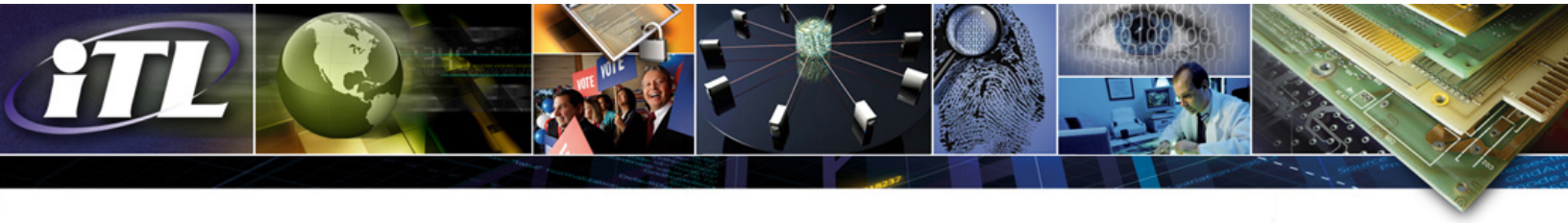


ITL BULLETIN FOR JUNE 2014

ITL FORENSIC SCIENCE PROGRAM

Barbara Guttman, Software and Systems Division
Martin Herman, Office of the ITL Director
Michaela Iorga, Larry Feldman, and Kim Quill, Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Digital forensics is the process used to acquire, preserve, analyze, and report on evidence using scientific methods that are demonstrably reliable, accurate, and repeatable such that they may be used in judicial proceedings. Through the application of computer science, mathematics, and statistics, the ITL Forensic Science program advances the measurements and standards infrastructure for forensic science. ITL works with national and international stakeholders, other government agencies, and state and local governments to develop standards, measurement methods, tests, validation studies, and technologies to:

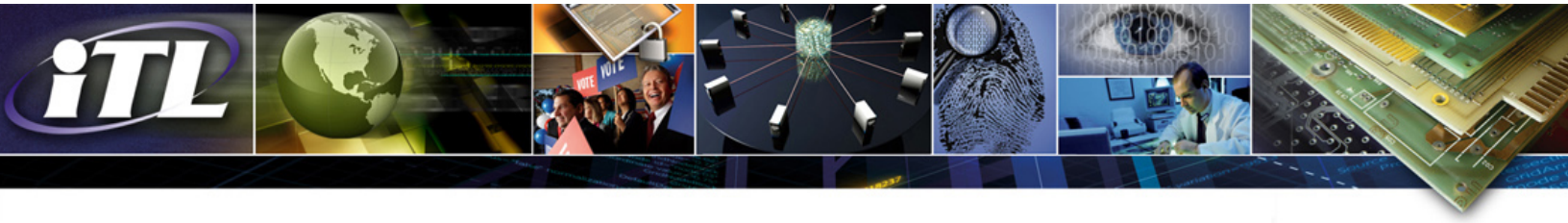
- Better understand and improve the accuracy and reliability of forensic science;
- Provide scientifically validated bases for forensic methods and standards;
- Establish measures of uncertainty for forensic analyses;
- Develop automated computing methods for forensic analyses and research; and
- Enhance the usability and interoperability of forensic systems.

The ITL Forensic Science Program currently supports several forensics research areas including human identity, multimedia forensics, ballistics, and digital forensics. Specific programs in these areas include the evaluation of latent fingerprint technologies (ELFT), face recognition, speaker recognition, image- and audio-based biometrics, and digital and multimedia evidence. The ITL Forensic Science Program's pursuits in digital forensics include the National Software Reference Library (NSRL), the Computer Forensic Reference Data Sets (CFReDS), Computer Forensics Tool Testing (CFTT), and Cloud Forensics.

The National Software Reference Library

The National Software Reference Library (NSRL) seeks to promote efficient and effective use of computer technology in the investigation of crimes involving computers. It serves as a resource for metadata that describes computer files from various, sometimes deprecated and obsolete, sources.

Without efficient methods, investigation of computer files requires a tremendous amount of effort. The NSRL provides an automated method for eliminating known files with verified metadata from an investigation, leaving unknown files and files with suspicious metadata to be reviewed. The NSRL creates short data profiles called "hashes," digital fingerprints (often called file signatures) that uniquely identify a file on a computer as an unaltered copy of a specific program or other piece of software in the library's



index. These hashes help to determine which files are important as evidence on computers that have been seized as part of criminal investigations. The NSRL contains both benign and malicious software and is intended as a filter of "known" file signatures, not "known good" signatures.

The NSRL consists of four components:

A large collection of software packages. Software is donated by software manufacturers and other organizations or purchased. These packages (including physical media and purely electronic) include both new and older versions of operating systems, database management systems, utilities, graphics images, component libraries, etc. The electronic library is on an isolated NIST network.

A database. The NSRL database contains detailed information about the files that make up the packages listed above.

The Reference Data Set (RDS). This data set contains signatures and identifying metadata, but not the software files. The metadata includes manufacturer name, operating system information, product information, application type, cryptographic information, and file storage information.

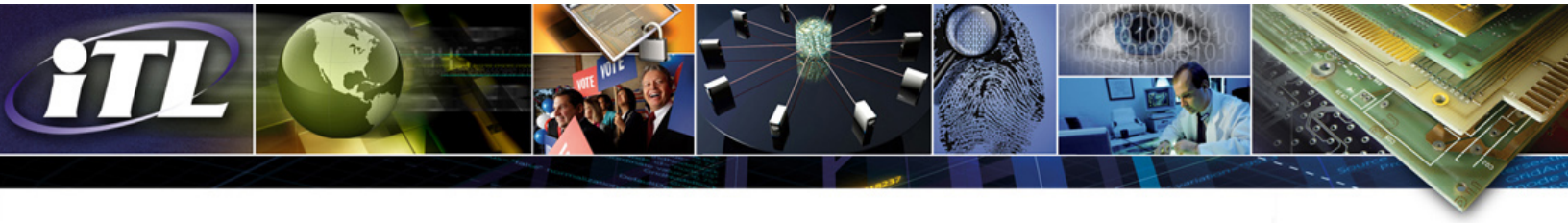
A research environment. This environment facilitates the collaboration of NIST with researchers to access NSRL's collection of software packages.

The first release of the RDS as NIST Special Database #28 was in October 2001. It is distributed quarterly to subscribers. ISO images are available via free download one month after subscriber media has been mailed. As of 2013, the RDS has grown to include over 100 million file signatures.

Computer forensics examiners, federal, state, and local law enforcement, government agencies, and industry organizations that perform investigations on computer technology use the NSRL to obtain digital evidence much more quickly and efficiently. The NSRL has also been used by researchers to quickly and automatically reduce the amount of data involved in experiments, where known files need to be identified. Digital librarians also apply the RDS to collections to distinguish computer system applications from user data. For example, ITL collaborates with the Stanford University Libraries on the preservation of early microcomputing software.

Computer Forensics Tool Testing Project

As stated above, ensuring the validity and reliability of computer forensics tools is important to the integrity of the U.S. criminal justice system. Many different automated tools are used routinely by law enforcement organizations to assist in the investigation of crimes involving computers. ITL's Computer Forensics Tool Testing (CFTT) project works to provide a measure of assurance that these forensics tools produce accurate results. The project establishes a methodology for testing computer forensics software tools by the development of tool specifications, test procedures, test criteria, test sets, and test hardware. With this information, investigators can make informed decisions about using a tool given its capabilities and limitations, and toolmakers can improve tools based on information obtained from test results. The CFTT project also provides international standard reference data.



The project has developed a computer forensics testing framework containing specifications and testing requirements for several categories of tools (e.g., disk imaging products, write blockers, deleted file recovery, etc.). ITL performs research to determine core characteristics for each category. These characteristics are then decomposed into a set of testable requirements. Assertions are derived from these requirements. Test cases to evaluate these assertions are compiled into a tool category specification document, which is posted for peer review by members of the computer forensics community and for public comment.

Currently, the CFTT project has produced a methodology for disk imaging, forensic media preparation, write blocking, deleted file recovery, mobile device forensics, file carving, and string searching.

Cloud Computing Forensics

Cloud computing offers a cost-effective, efficient approach to meeting the computing needs of government, industry, and private users. However, significant forensic science challenges arise with respect to cloud computing ecosystems' technical operations and control dynamics. The NIST Cloud Computing Forensic Science Working Group (NCC-FSWG) was established in November 2012 to investigate needs and solutions in cloud forensics involving technology, measurements, and standards. The group works toward this goal by identifying, aggregating, prioritizing, and analyzing cloud forensic science challenges, aiming to promote research in measurements, standards, and technology that address those forensic science challenges. The NCC-FSWG has an open membership, with participants that include academics, representatives from federal agencies, cloud providers, cloud forensic practitioners, and international users.

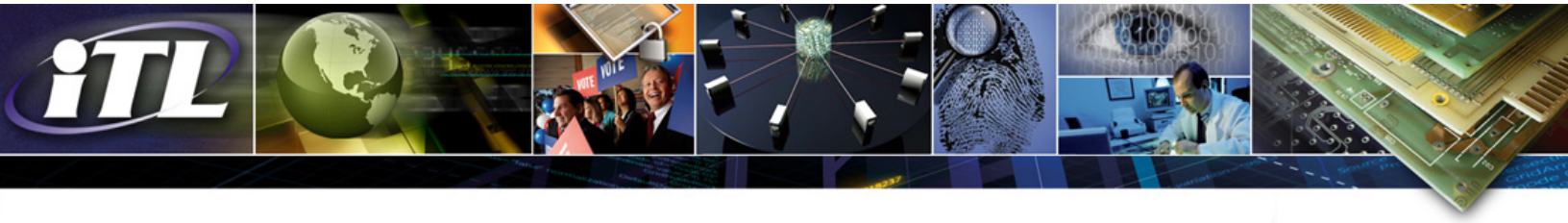
Additionally, the NCC-FSWG provides a forum for information sharing and discussions regarding identified cloud forensic science concerns and challenges. As a result of the latest research performed, the team identified approximately 65 challenges consisting of technical, legal, and organizational concerns. The list of challenges is not comprehensive but rather a snapshot of the technical, legal, or organizational tasks impeded by cloud computing. The list is expected to evolve as solutions are researched and developed for those challenges.

The identified challenges are analyzed and prioritized based on importance and impact. Prioritized challenges that cannot be handled with current technology and methodologies will be further investigated to determine gaps in technology, standards, and measurements. The program will then create roadmap plans to address these gaps.

To participate in the NCC-FSWG, individuals need to subscribe to the mailing list. Additional information can be found on the TWiki.

Future Work

Mobile Forensics: Mobile devices are ubiquitous in today's society. The technologies behind these devices vary greatly across platforms, and are constantly undergoing significant changes to both



hardware and software. It is often difficult to determine the most effective method for extracting information from mobile devices during an investigation. The goal of mobile forensics is the practice of applying sound methodologies to acquire data contained within the internal memory of a mobile device and its associated media. ITL has just released a new version of NIST Special Publication 800-101 Rev. 1, *Guidelines on Mobile Device Forensics*. The goal of this document is to help organizations evolve appropriate procedures for dealing with mobile devices and to prepare forensic specialists to conduct forensically sound examinations involving mobile devices.

Workshop and Webcast: ITL will host the NIST Mobile Forensics Workshop and Webcast on June 18, 2014. This is a free one-day workshop and live webcast with the goal of educating attendees on the latest developments in the forensic analysis of mobile devices, and how technologies are used in casework.

Cloud Forensics NIST Interagency Report (NISTIR): The NCC-FSWG will soon release NISTIR 8006, *NIST Cloud Computing Forensic Science Challenges,* for public review and comment. The document will present the cloud forensic challenges described above along with associated literature. It will also provide a preliminary analysis of these challenges.

Additional Resources

NIST Cloud Computing Forensic Science website

Cloud Computing Forensic Science Working Group TWiki (NCC-FSWG)

See ITL's information security programs, projects, and research. All security publications (standards, special publications, guidelines, interagency reports, and related papers) are available from the Computer Security Resource Center.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov