

Information Technology Laboratory Newsletter

INSIDE THIS ISSUE

ITL Focuses on Forensic Analysis Technologies

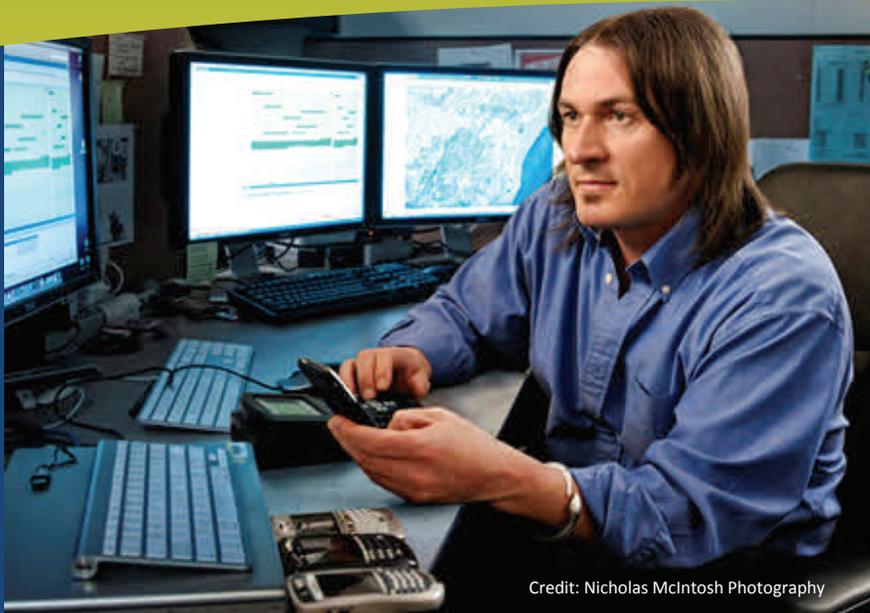
NIST Engineers Test Initial Flight of a Robotic Sensor Platform

ITL Contributes to the DARPA XDATA (Big Data) Summer Camp

Staff Recognition

Selected New Publications

Upcoming Technical Conferences



Credit: Nicholas McIntosh Photography

September-October 2014

Issue 131

Engineer Rick Ayers makes sure commercial forensics tools for cell phones conform to required specifications by testing them on a number of phone models.

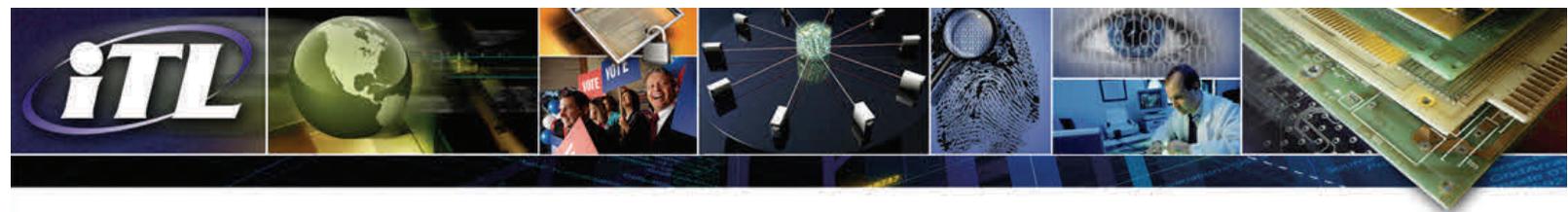
ITL Focuses on Forensic Analysis Technologies

Mobile devices in today's society often contain valuable information that can help investigators reconstruct events and solve crimes. Numerous research advances have occurred in both mobile devices and the tools used to analyze these devices. Investigators and analysts that rely on the outputs of the devices and tools require confidence that the data recovered is reliable and reproducible. Stakeholders in the mobile forensic science community continue to work together to maintain pace with the rapid change experienced in the industry. These stakeholders perform research to develop new analysis tools, use collaborative venues to develop procedural standards, and validate tools through testing programs to support investigators through the investigation and judicial process.

To explore the latest technology advances and applications in mobile device forensics, ITL's Computer Forensic Tool Testing (CFTT) program recently hosted a free one-day workshop and live webcast. Focusing on how technologies are used in casework, the workshop provided information that was tailored to increase the situational awareness of investigators and criminal justice stakeholders across the United States about the latest trends, analysis protocols, and issues encountered when applying analysis tools to mobile devices.

The workshop addressed a broad range of mobile forensic topics including mobile forensic tool testing at NIST; mobile forensics from A to Z; mobile forensic research needs from academic and practitioner perspectives; mobile device forensics – is it actually forensics; open-source, Blackberry, and Apple forensics; chip-off technology and JTAG analysis tools; and real-world application of mobile forensic analytical tools.

Toolmakers continually face the challenge of releasing software updates in a timely manner, providing forensic examiners and law enforcement with an acquisition solution for the current mobile devices. The ongoing mobile testing performed by ITL's CFTT program provides information necessary for toolmakers to improve tools and for interested parties to understand tools limitations and capabilities. Additionally, ITL recently released [NIST Special Publication 800-101 \(Revision 1\), Guidelines on Mobile Device Forensics](#), which discusses procedures for the validation, preservation, acquisition, examination, analysis, and reporting of digital information. For more information, see this [website](#).



NIST Engineers Test Initial Flight of a Robotic Sensor Platform

Engineers from ITL and NIST's Engineering Laboratory (EL) recently performed initial flight tests on a robotic aerial sensor platform on the NIST Gaithersburg campus. The tests are the first phase of a project aimed at developing unified methods for capability provisioning and information assurance between physical perception and cyber infrastructure.

Given the growing use of robotic sensor platforms and the advent of cloud-based curation and analysis of large data sets, NIST engineers are collaborating to demonstrate strategies and interfaces required to co-optimize robot perception, via sensor tuning and path planning, along with metrics used for data science and information assurance. As an application scenario, the team will focus on optimizing data collection and data organization tools used in an emergency response situation such as a multiple vehicle collision.

ITL Contributes to the DARPA XDATA (Big Data) Summer Camp

ITL contributed to the eight-week DARPA XDATA Summer Camp, the second such camp that brings together the current field of XDATA program performers in a hack-a-thon setting aimed to develop data analytics and big data visualization techniques for inclusion in the Defense Advanced Research Projects Agency (DARPA) [Open Catalog](#). XDATA is developing an open source software library for big data to help overcome the challenges of effectively scaling to modern data volume and characteristics. The program is developing the tools and techniques to process and analyze large sets of imperfect, incomplete data. Its programs and publications focus on the areas of analytics, visualization, and infrastructure to efficiently fuse, analyze, and disseminate these large volumes of data.

ITL's role in XDATA is to support the program's evaluation of analytic accuracy and system benchmarking. During the past three months, the NIST team developed three evaluation tracks and the corresponding software tools necessary to support the assessment of analytic accuracy; perform system benchmarking; and automatically generate a common report for inclusion in the software's documentation. Each evaluation track consisted of four tasks, the first three of which were designed to measure infrastructure or analytic software, and the fourth was designed to measure visualizations.

Occurring from June through mid-August, the XDATA Summer Camp had between 20 and 100 researchers gathered in the lab daily. Researchers from around the country presented daily updates on research and progress. Participation in the NIST-designed evaluations was voluntary and will continue for the next couple of months. ITL's participation in the XDATA program has helped NIST prepare for its own Data Science evaluation series that will build upon the tools and infrastructure created to support XDATA.

STAFF RECOGNITION

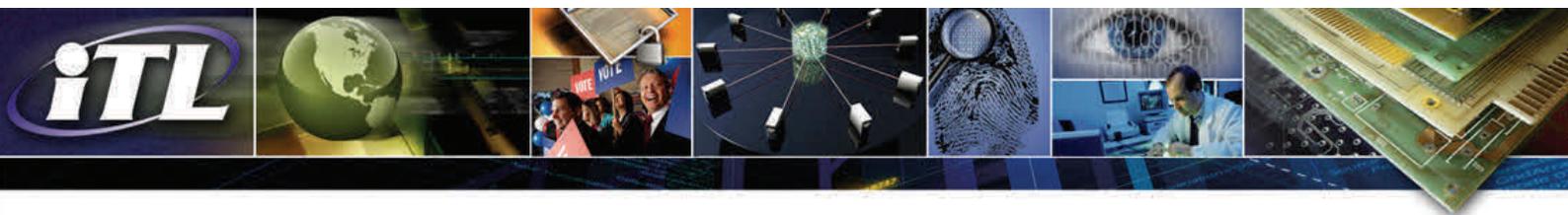
Jeffrey Fong, Applied and Computational Mathematics Division, received the 2014 Lifetime Achievement Award from the International Conference on Computational Engineering and Science (ICCES). Fong was cited for his "seminal contributions to reliability engineering and probabilistic mechanics." The ICCES Lifetime Achievement Award recognizes sustained and significant contributions in the form of research, teaching, and service to the community, in the technical areas of the ICCES series of conferences.

Chris Schanzle received an Outstanding Service award from Sigma Xi, the Scientific Research Society. Schanzle was recognized for his exceptional service in support of the ITL Applied and Computational Mathematics Division, the Statistical Engineering Division, and their collaborators throughout the NIST Laboratories.



This summer ITL hosted 28 students from 20 colleges and universities in the Summer Undergraduate Research Fellowship (SURF) program, which provides hands-on research experience in applied mathematics, statistics, software testing, computer security, information access, and networking.

Credit: Denease Anderson, NIST



Selected New Publications

[Approximate Matching: Definition and Terminology](#)

By Frank Breitinger, Barbara Guttman, Michael McCarrin, Vassil Roussev, and

Douglas White
NIST Special Publication 800-168
May 2014

This document provides a definition of and terminology for approximate matching, which is a promising technology designed to identify similarities between two digital artifacts. It is used to find objects that resemble each other or objects that are contained in another object. This can be very useful for filtering data for security monitoring, digital forensics, and other applications.

[NIST Smart Grid Interoperability Panel Priority Action Plan 2, Guidelines for Assessing Wireless Standards for Smart Grid Applications](#)

Participants of the Priority Action Plan 2 Working Group
David E. Cypher, Editor
NISTIR 7761 Rev. 1
July 2014

This report is a draft of key tools and methods to assist Smart Grid system designers in making informed decisions about existing and emerging wireless technologies. An initial set of quantified requirements have been brought together for advanced metering infrastructure (AMI) and initial distribution automation (DA) communications. These two areas present technological challenges due to their scope and scale. These systems will span widely diverse geographic areas and operating environments and population densities ranging from urban to rural.

[Policy Machine: Features, Architecture, and Specification](#)

By David Ferraiolo, Serban Gavrila, and Wayne Jansen
NISTIR 7987
May 2014

The ability to control access to sensitive data in accordance with policy is perhaps the most fundamental security requirement. Despite over four decades of security research, the limited ability for existing access control mechanisms to enforce a comprehensive range of policy persists. This report describes an access control framework, referred to as the Policy Machine (PM), which fundamentally changes the way policy is expressed and enforced. The report gives an overview of the PM and the range of policies that can be specified and enacted. The report also describes the architecture of the PM and the properties of the PM model in detail.

[Design and Testing of a Mobile Touchscreen Interface for Multi-Modal Biometric Capture](#)

By Kristen K. Greene, Ross Micheals, Kayee Kwong, and Gregory P. Fiumara
NISTIR 8003
May 2014

This report describes the design and usability testing of a touchscreen interface for multi-modal biometric capture, an application called WSABI, Web Services for the Acquisition of Biometric Information. The application code is publicly available online at <https://github.com/NIST-BWS/wsabi2>. The interface is a tablet-based reference application for the Web Services for Biometric Devices (WS-BD) protocol. Just as WS-BD specifies a method of communication between client and sensors (i.e., machine-to-machine communication), WSABI provides a consistent and modality-independent method of interaction between human operators and sensors (i.e., human-to-machine communication).

[Performance of Face Identification Algorithms](#)

By Patrick Grother and Mei Ngan
NISTIR 8009
May 2014

This report documents performance of one-to-many face identification algorithms and compares it with performance in 2010. Performance in this context refers to recognition accuracy and computational resource usage as measured by executing those algorithms on massive sequestered datasets. These datasets consist of reasonable-quality law enforcement mugshot images; poor-quality webcam images collected in similar detention operations; and moderate-quality visa application images. The mugshot and visa images are used to approximate performance obtainable using high-quality ISO standardized images collected in passport, visa, and driving license duplicate detection operations.

[A Measurement Metric for Forensic Latent Fingerprint Preprocessing](#)

By Haiying Guan, Andrew Dienstfrey, Mary Theofanos, and Brian Stanton
NISTIR 8017
July 2014

This report describes a proposal to extend Spectral Image Validation and Verification (SIVV) to serve as a metric for latent fingerprint image quality measurement. ITL researchers implemented and tested the new SIVV-based metric for latent fingerprint image quality and used it to measure the performance of the forensic latent fingerprint preprocessing step. Preliminary results show that the new metric can provide positive indications of both latent fingerprint image quality and the performance of the fingerprint preprocessing.



Upcoming Technical Conferences

[2nd Privacy Engineering Workshop](#)

Dates: September 15-16, 2014

Place: San Jose, California

Sponsors: NIST and the International Association of Privacy Professionals

As part of NIST's Privacy Engineering Initiative, this workshop will consider draft privacy engineering definitions and concepts. The results of the workshop will inform the development of the NIST report on privacy engineering. System design and privacy engineers as well as privacy subject matter experts should attend this interactive workshop.

NIST contact: [Suzanne Lightman](#)

[2014 Global Identity Summit](#)

Dates: September 16-18, 2014

Place: Tampa Convention Center, Tampa, Florida

Sponsors: NIST and National Security Agency

Presented by the Biometric Consortium and the Armed Forces Communications and Electronics Association, this conference promotes information exchanges on scientific and technical advancements, operational requirements, and future strategic directions of biometrics and identity management. It focuses on solutions for the corporate, defense, and homeland security communities.

NIST contact: [Fernando Podio](#)

[Safeguarding Health information: Building Assurance through HIPAA Security – 2014](#)

Dates: September 23-24, 2014

Place: Grand Hyatt Hotel, Washington, D.C.

Sponsors: NIST and the Department of Health and Human Services (HHS) Office of Civil Rights (OCR)

This 7th annual conference will explore the current health information technology (IT) security landscape and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The conference will address security management and technical assurance of electronic health information. Topics will include updates on the Omnibus HIPAA/HITECH Final Rule, breach management, strengthening cybersecurity in the healthcare sector, integrating security safeguards into health IT, managing risk, securing mobile devices, and more.

NIST contact: [Kevin Stine](#)

[6th Cybersecurity Framework Workshop](#)

Dates: October 29-30, 2014

Place: Florida Center for Cybersecurity, Tampa, Florida

Sponsor: NIST

The purpose of this workshop is to gather input to help NIST understand stakeholder awareness of, and initial experiences with, the Cybersecurity Framework and related activities to support its use. NIST plans to release a formal Request for Information (RFI) asking for further feedback in these areas. Responses to the RFI will inform the workshop agenda.

NIST contact: [Suzanne Lightman](#)

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.



The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST). As a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, our research program supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. ITL cybersecurity experts collaborate to develop cybersecurity standards, guidelines, and associated methods and techniques for federal agencies and industry. Our mathematicians and statisticians collaborate with measurement scientists across NIST to help ensure that NIST maintains and delivers the world's leading measurement capability. ITL computer scientists and other research staff provide technical expertise and development that underpins national priorities such as cloud computing, the Smart Grid, homeland security, information technology for improved healthcare, and electronic voting. We invite you to learn more about how ITL is enabling the future of the nation's measurement and standards infrastructure for information technology by visiting our website at <http://www.itl.nist.gov>.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
Email: elizabeth.lennon@nist.gov

TO SUBSCRIBE TO THE
ELECTRONIC EDITION OF
THE ITL NEWSLETTER, GO
TO
[ITL HOMEPAGE](#)

Credit: Katherine Green, NIST