ICDF2C / SADFE

Digital Forensics & Cyber Crime

An Overview of Digital Forensics at

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Agenda

NIST's Broad Role In Forensics Science

Information Technology Laboratory (ITL)

Software & Systems Division

Digital Forensics Advances & Resources

nist.gov/forensics

Disclaimer

Trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

NIST Mission & Role

Unique Mission within the Federal Government - 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.

Deep research expertise underpins technological innovation – e.g ., new materials, advanced communications, **forensic science**, etc.

Non-regulatory status enables an important role as a convener that **facilitates collaboration** between agencies of the Federal Government, industry, private organizations, and state and local governments.

Organization of Scientific Area Committees

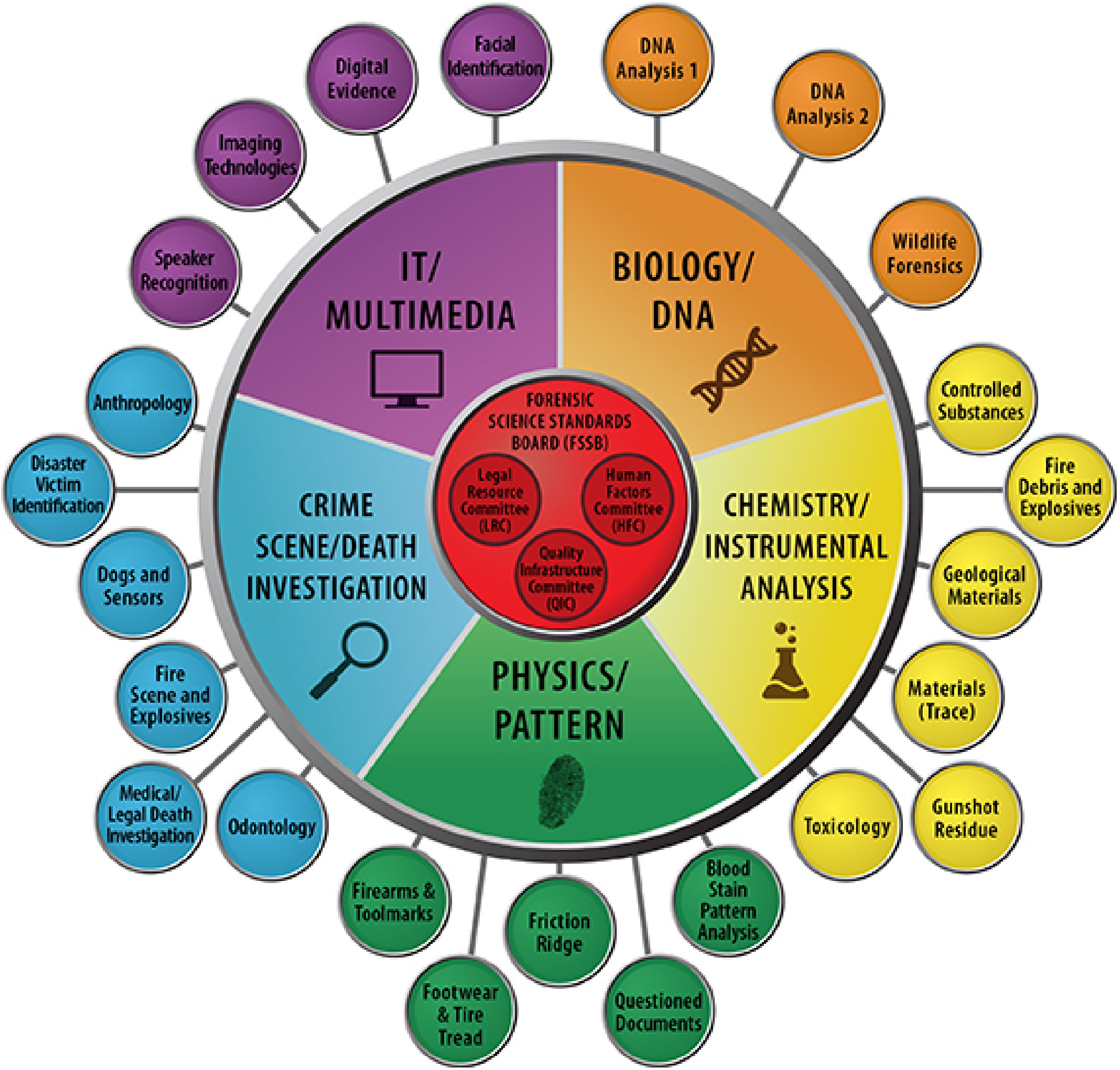
An initiative by NIST and the Department of Justice to strengthen forensic science in the United States.

Objective: To create a sustainable uniform organizational infrastructure that produces consensus documentary **standards and guidelines to improve quality and consistency** of work in the forensic science community.

NIST anticipates needing nearly 600 people in the OSAC organization:

Forensic Science Standards Board members (17)
3 resource committees (about 35 people)
5 scientific area committees (about 75 people)
23 subcommittees (about 460 people)

http://www.nist.gov/forensics/osac



FORENSIC SCIENCE STANDARDS BOARD (FSSB)

Legal Resource Committee (LRC)

Human Factors Committee (HFC)

Quality Infrastructure Committee (QIC)

IT/ MULTIMEDIA

- Speaker Recognition
- Imaging Technologies
- Digital Evidence
- Facial Identification

BIOLOGY/ DNA

- DNA Analysis 1
- DNA Analysis 2
- Wildlife Forensics

CHEMISTRY/ INSTRUMENTAL ANALYSIS

- Controlled Substances
- Fire Debris and Explosives
- Geological Materials
- Materials (Trace)
- Gunshot Residue
- Toxicology

PHYSICS/ PATTERN

- Blood Stain Pattern Analysis
- Questioned Documents
- Friction Ridge
- Footwear & Tire Tread
- Firearms & Toolmarks

CRIME SCENE/DEATH INVESTIGATION

- Odontology
- Medical/ Legal Death Investigation
- Fire Scene and Explosives
- Dogs and Sensors
- Disaster Victim Identification
- Anthropology

Forensic Science Standards Board

The FSSB supports the organization by:

overseeing operations of all resource committees, scientific area committees and subcommittees;

approving standards for listing on the OSAC Registry of Approved Standards; and

facilitating communication within OSAC and between OSAC and the forensic science community.

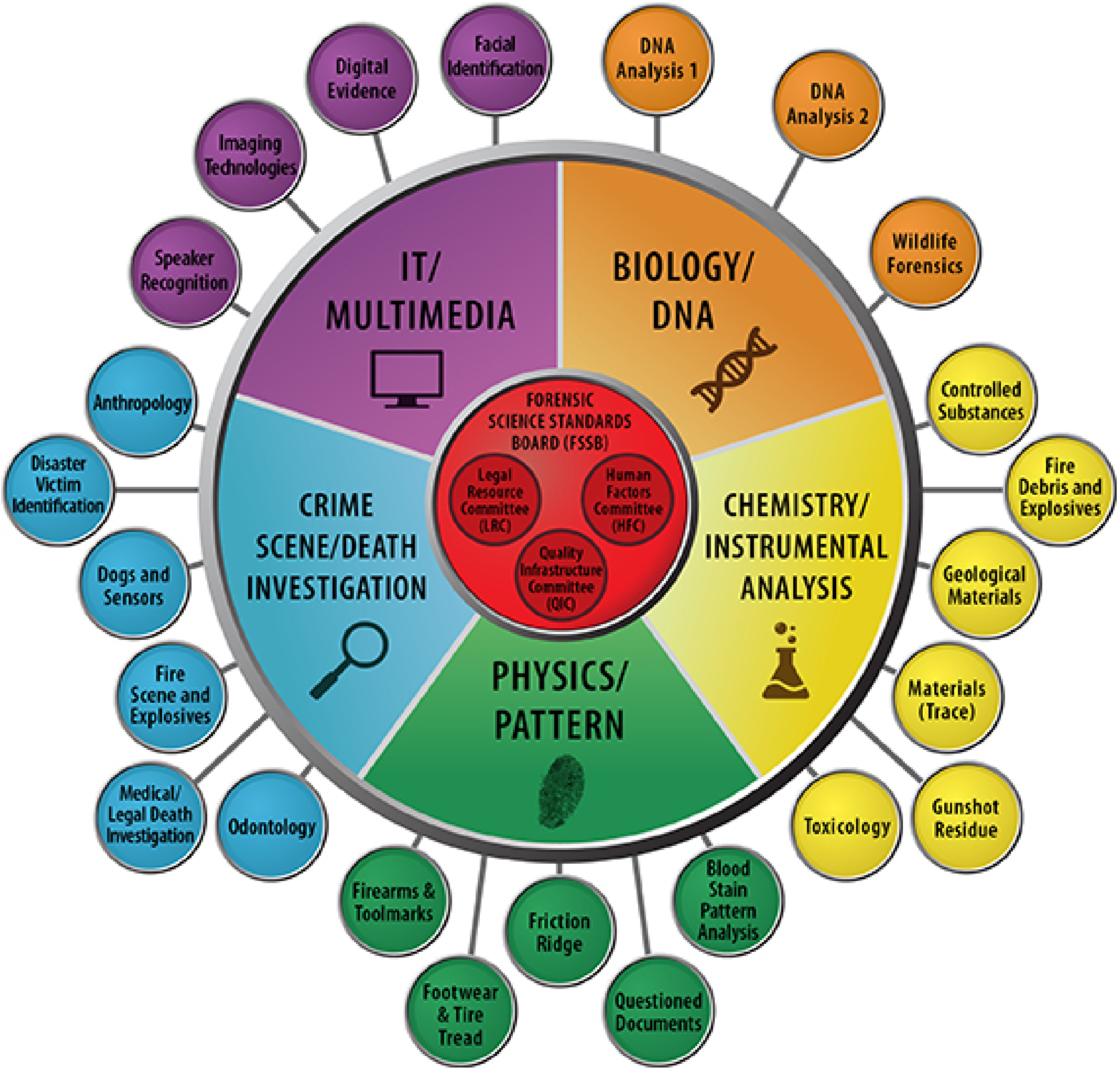
June 26, 2014: NIST Named Members to First FSSB.

5 Research representatives

6 Professional association representatives

5 Scientific Area Committee (SAC) chairs:

NIST Ex Officio member: Mark Stolorow, Director of OSAC Affairs



FORENSIC SCIENCE STANDARDS BOARD (FSSB)

Legal Resource Committee (LRC)

Human Factors Committee (HFC)

Quality Infrastructure Committee (QIC)

IT/ MULTIMEDIA
- Speaker Recognition
- Imaging Technologies
- Digital Evidence
- Facial Identification

BIOLOGY/ DNA
- DNA Analysis 1
- DNA Analysis 2
- Wildlife Forensics

CHEMISTRY/ INSTRUMENTAL ANALYSIS
- Controlled Substances
- Fire Debris and Explosives
- Geological Materials
- Materials (Trace)
- Gunshot Residue
- Toxicology

PHYSICS/ PATTERN
- Blood Stain Pattern Analysis
- Questioned Documents
- Friction Ridge
- Footwear & Tire Tread
- Firearms & Toolmarks

CRIME SCENE/DEATH INVESTIGATION
- Odontology
- Medical/ Legal Death Investigation
- Fire Scene and Explosives
- Dogs and Sensors
- Disaster Victim Identification
- Anthropology

Digital Evidence Subcommittee

Forensic science practitioners, academic researchers and others with expertise in digital evidence will hold up to 20 voting positions on the new Digital Evidence Subcommittee.

OSAC Vision: in 5-10 Years…

Forensic Science practitioners embrace change

OSAC Forensic Registries of Standards and Guidelines become implemented in the practice of forensic science across all forensic disciplines

Prosecutors, defense attorneys and judges use the Registries of Standards and Guidelines in direct and cross examinations of expert witnesses

Judges and Juries routinely hear witnesses testify about how their analysis met current standards and scientific validity and openly describe the limitations of the tests in general and their interpretations in the specific case

Significant forensic science research is well organized and well funded with influence from OSAC to define research priorities

Standards enforcement by accrediting bodies becomes the rule

Forensic Science Center of Excellence

NIST announced a competition to create a Forensic Science Center of Excellence dedicated to collaborative, interdisciplinary research.

Mission: to establish a firm scientific foundation for the analytic techniques used in two important branches of forensic science, pattern evidence and digital evidence.

Forensic Science Center of Excellence

Forensic investigations involve the collection of evidence, measurements of the evidence, analysis of those measurements and the determination of conclusions of known validity.

One important goal is to develop so-called “probabilistic methods”—**techniques that produce a quantifiable assessment** of the likelihood that a given method produced a correct result.

The planned center will work on **scientific advances in probabilistic methods and information technology tools**, as well as the necessary infrastructure to educate and train forensic science practitioners in using the new methods. The center will promote interactions between NIST, academia and various stakeholders in the forensic science community.

NIST – Office of Special Programs

The Office of Special Programs of NIST fosters communication and collaboration between NIST and external communities focused on critical national needs.

NIST has conducted and supported forensic science research for many decades. In fact, the FBI consulted with NIST (then National Bureau of Standards) experts when it established its laboratory in 1932.

NIST – Office of Special Programs

OSP focus areas include:

- AFIS Interoperability
- CBRNE
- Counterterrorism
- Forensics

A sample of the many forensics research topics:

- audio analysis
- biometrics
- computer forensics
- crime scene
- digital evidence
- engineering forensics
- image analysis
- questioned documents
- video analysis

NIST – OSP - OLES

The Law Enforcement Standards Office (OLES) helps criminal justice, public safety, emergency responder, and homeland security agencies make informed procurement, deployment, training and operating decisions by developing performance standards, measurement tools, operating procedures and equipment guidelines.

Information Technology Laboratory

NIST - ITL

The Information Technology Laboratory (ITL) has the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through **research and development in information technology, mathematics, and statistics**.

ITL researchers have developed detailed **protocols and operational standards** that mitigate anticipated discrepancies in their operation, and established **assessment criteria and test data sets** for validation of industrial products.

ITL formulates **metrics, tests, and tools** for a wide range of subjects such as information complexity and comprehension, high confidence software, mobile and wireless computing, as well as, issues of information quality, integrity, and usability.

ITL continues to develop **cybersecurity** standards, guidelines, and associated methods and techniques.

ITL seeks to excel in Information Measurement Science to enable international social, economic, and political advancement by **collaborating and partnering** with industry, academia, and other NIST laboratories to advance science and engineering.

ITL - NCCoE

The National Cybersecurity Center of Excellence (NCCoE) was established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County.

The center provides businesses with **real-world cybersecurity solutions**, based on commercially available technologies.

Goals:

Provide practical cybersecurity - Help people secure their data and digital infrastructure by equipping them with practical ways to implement cost-effective, repeatable and scalable cybersecurity solutions.

Increase rate of adoption - Enable companies to rapidly adopt commercially available cybersecurity technologies by reducing their total cost of ownership.

Accelerate effective innovation - Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment.

ITL - NVD

The National Vulnerability Database (NVD) is the U.S. government repository of standards based **vulnerability management data** represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

NVD is a comprehensive cyber security vulnerability database that **integrates publicly available U.S. government vulnerability resources** and provides references to industry resources.

The NVD statistics engine provides reporting capabilities that allow the tracking of vulnerability trends over time. This trending service allows users to **assess changes in vulnerability discovery rates** within specific products or within specific types of vulnerabilities.

ITL – NCP

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide **detailed low level guidance on setting the security configuration** of operating systems and applications.

NCP is migrating its repository of checklists to conform to SCAP, which will enable standards based security tools to automatically perform configuration checking using NCP checklists.

ITL – Mobile Security & Forensics

Scientists devise and implement, as proof-of-concept prototypes, various types of security mechanisms and frameworks.

Also studied is the **proper retrieval and analysis of data recovered** during a forensic examination, when conducted as part of an incident or criminal investigation.

NIST has focused on developing **reference materials, guidelines and procedures** for use in tool assessment and in improving the accuracy of results produced from mobile forensic tools.

NIST released a distribution of an **application and reference data set for populating identity modules**. The reference test data and application was developed to provide a greater amount of coverage than normally done by manual means. The initial results attained by processing commonly-used forensic tools against the populated test data indicate that a variety of inaccuracies exist in present-day forensic tools, which can be uncovered through this approach.

Software & Systems Division

SSD - SAMATE

The SAMATE (Software Assurance Metrics And Tool Evaluation) project is dedicated to improving software assurance by developing methods to enable software tool evaluations, measuring the effectiveness of tools and techniques, and identifying gaps in tools and methods.

The scope of the SAMATE project is broad: ranging from operating systems to firewalls, SCADA to web applications, source code security analyzers to correct-by-construction methods.

One of the SAMATE goals is to establish a methodology for evaluating software assurance tools by developing tool specifications, test plans, and test sets. The results provide information for tool developers to improve tools, for users to make informed choices about acquiring and using software tools, and for interested parties to understand tool capabilities.

Published specifications and test plans include NIST Special Publication 500-268 v1.1, NIST SP 500-269 and NIST SP 500-270.

SSD – Software Performance

The Software Performance project seeks to strengthen the scientific foundations of software performance measurement.

Its goals are:

Application: Replace unreliable common practices with rigorously-studied methods grounded in design of experiments.

Research: Solve measurement challenges created by the evolution and increased complexity of commodity hardware.

Transfer: Feed improved methods back into the community of practice.

One notable accomplishment is the Test Driver for Android, Version 1.0. The driver automates the repeated launching of Android test apps for experimental data collection.

SSD – CFTT

The goal of the Computer Forensic Tool Testing (CFTT) project is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware.

The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities.

The testing methodology developed by NIST is functionality driven. The activities of forensic investigations are separated into discrete functions or categories. A test methodology is then developed for each category.

Disk Imaging
Write block (Software)
Deleted File Recovery
Forensic File Carving
Forensic Media Preparation
Write block (Hardware)
Mobile Devices
String Search

SSD – CFTT

The Computer Forensics Tool Catalog provides an easily searchable online catalog of forensics tools enabling practitioners to find tools that meet their specific technical needs. The catalog provides the ability to search by technical parameters based on specific computer forensics functions.

Federated Testing is an expansion of CFTT to provide the digital forensics community with shared test materials for tool validation. The platform is a live Ubuntu CD featuring several components: Website, Reference information, Test plan, Final report, Command line test support tools, Test case setup and analyze results.

www.nsrl.cftt.gov

SSD - CFReDS

NIST develops Computer Forensic Reference Data Sets (CFReDS) for digital evidence.

These reference data sets 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, establishing that lab equipment is functioning properly, training investigators, and proficiency testing of investigators as part of laboratory accreditation.

SSD - NSRL

The National Software Reference Library (NSRL) was created as an offshoot of the FBI Automated Computer Examination System (ACES) program.

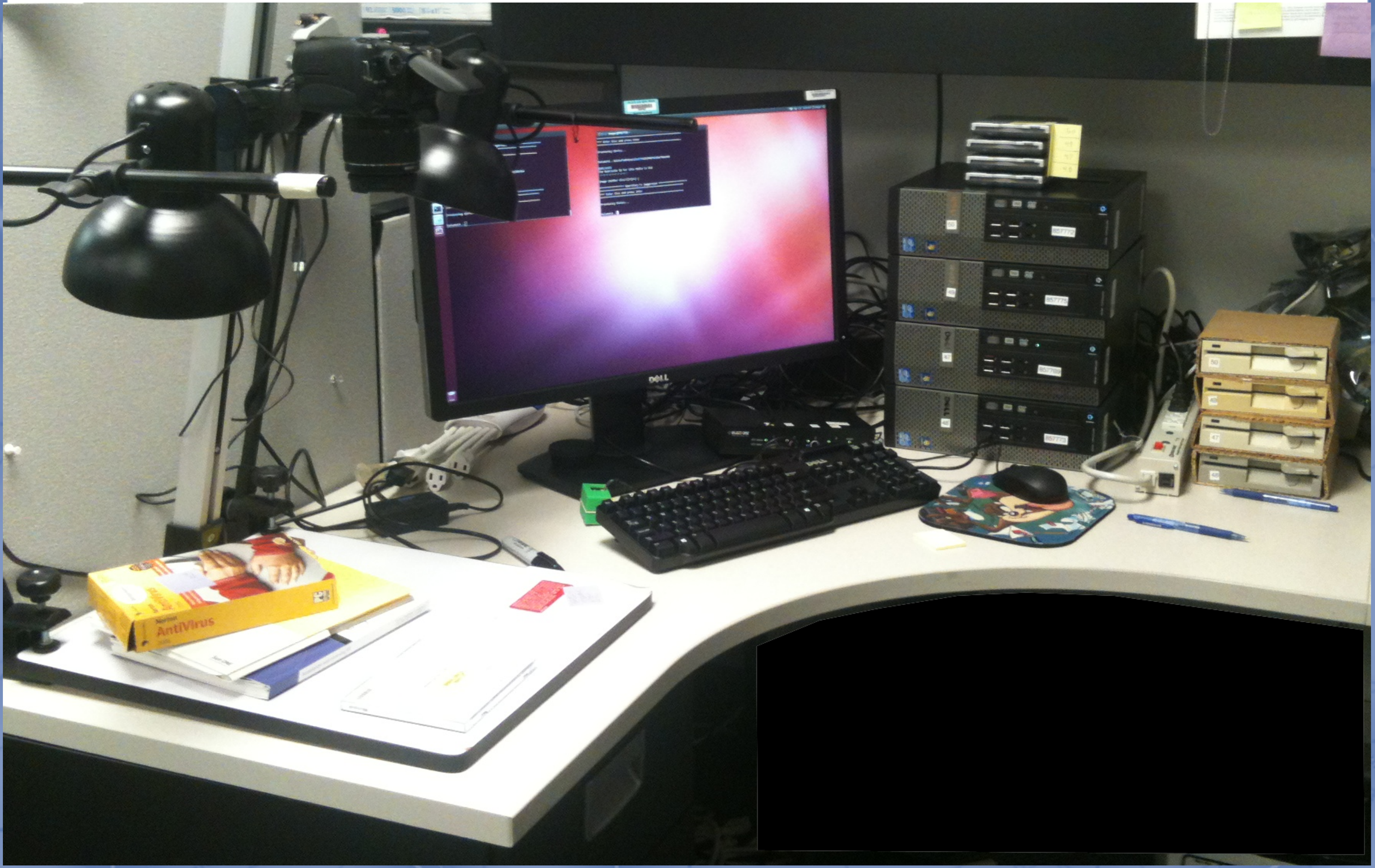
The NSRL is designed to **collect software** from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information.

The RDS can be used by law enforcement, government, and industry organizations to **automatically review computers or file systems** that have been seized as part of criminal investigations by matching file profiles in the RDS.

The RDS is a collection of digital signatures of known, traceable software applications. There are application hash values in the hash set which may be considered malicious. There are no hash values of illicit data, i.e. child abuse images.

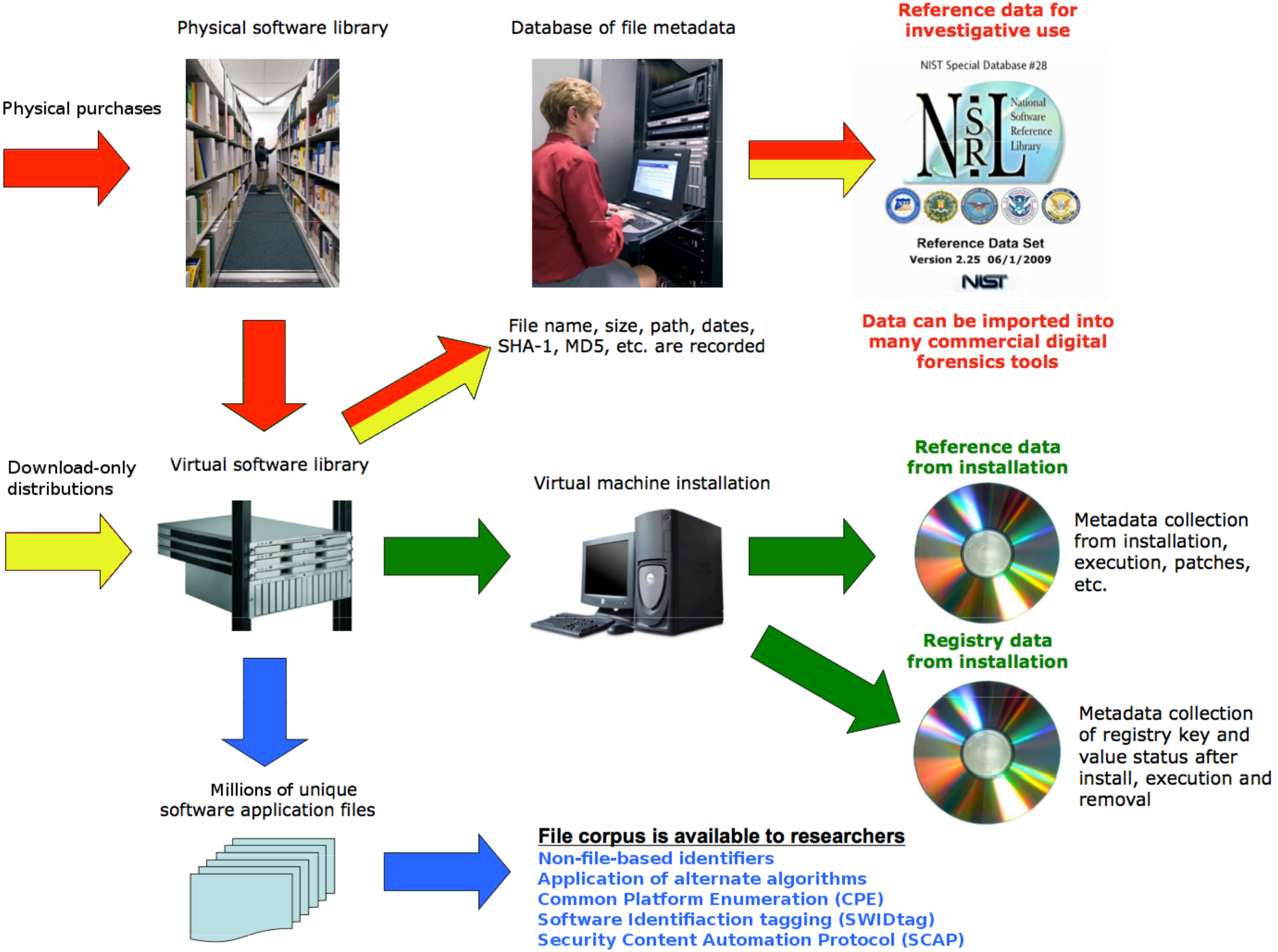
National Software Reference Library

Media Acquisition and Photography



[redacted]

National Software Reference Library



NIST Special Database #28
National Software Reference Library
NSRL
Reference Data Set
Version 2.25 06/1/2009
NIST

Physical purchases

Physical software library

Database of file metadata

Reference data for investigative use

Data can be imported into many commercial digital forensics tools

File name, size, path, dates, SHA-1, MD5, etc. are recorded

Download-only distributions

Virtual software library

Virtual machine installation

Reference data from installation

Metadata collection from installation, execution, patches, etc.

Registry data from installation

Metadata collection of registry key and value status after install, execution and removal

Millions of unique software application files

File corpus is available to researchers

- Non-file-based identifiers
- Application of alternate algorithms
- Common Platform Enumeration (CPE)
- Software Identifiaction tagging (SWIDtag)
- Security Content Automation Protocol (SCAP)

ISO 19770

Software ID (SWID) tags allow a publisher to define an authoritative name for a software product along with the various other artifacts.

SWID tags can facilitate:

More **accurate and consistent communications** with partners, customers and 3rd party tool providers;

Ability to automatically incorporate the data required by the US Federal Government to **work within the SCAP** infrastructure;

Integration of inventory findings with other tools that may not have direct integration;

Publisher data **validated through digital signature**, allowing for more authoritative and non-modifiable data;

Having a consistent way to represent software titles for **security, logistics and compliance**.

Approximate Matching

Traditional hash sets enable the exact comparison of files with the advantages that they are reasonably quick to compute and quick to compare. Hashes cannot assess how different the two files are in the case where they are not identical.

Of interest are those situations in which files A and B represent different versions of a file or where file A is partly or wholly contained within file B.

Approximate matching provides a means to assess/quantify the relationship between two files beyond same/not same.

The NSRL intends to be a central resource for approximate matching adoption in the forensic community.

NIST Special Publication 800-168

Diskprints

The NSRL catalogs effects of modifying known systems using known software under controlled conditions and recording the effects using virtual machine (VM) installations.

Each VM instance represents a slice of time in the software's life cycle on the system.

The set of all slices for a package in tandem with various metadata which apply to the entire package life cycle is referred to as the application's diskprint.

Each slice in a diskprint comprises a set of measurements which include: installed file metadata; Windows(R) registry data; RAM contents; network packet captures; descriptions of the slice and the stage of the software life cycle.

DFXML

Digital Forensics XML (DFXML) is an XML language used to automate digital forensics processing. DFXML contains information about both the results of forensic processing and the tools used to perform the processing (provenance).

Tools that produce DFXML : fiwalk, frag_find, photorec, bulk_extractor, afxml, ewfinfo, md5deep, sha1deep, hashdeep

Tools that consume DFXML : frag_find, iblkfind.py, identify_filenames.py, idifference.py, imap.py, imicrosoft_redact.py, iverify.py, Gumshoe

Tools that transform DFXML : sanitize_xml.py

SUL Cabrinety Collection

The Stephen M. Cabrinety Collection in the History of Microcomputing at Stanford University, is one of the world’s largest pristine software collections.

The Cabrinety Collection includes titles from virtually all of the major microcomputer platforms, including home computer and video game consoles.

SUL Cabrinety Collection

Contains 6,300 pieces of computer software.

Focuses on games for Atari, Commodore, Amiga, Sega, Nintendo, and Apple systems.

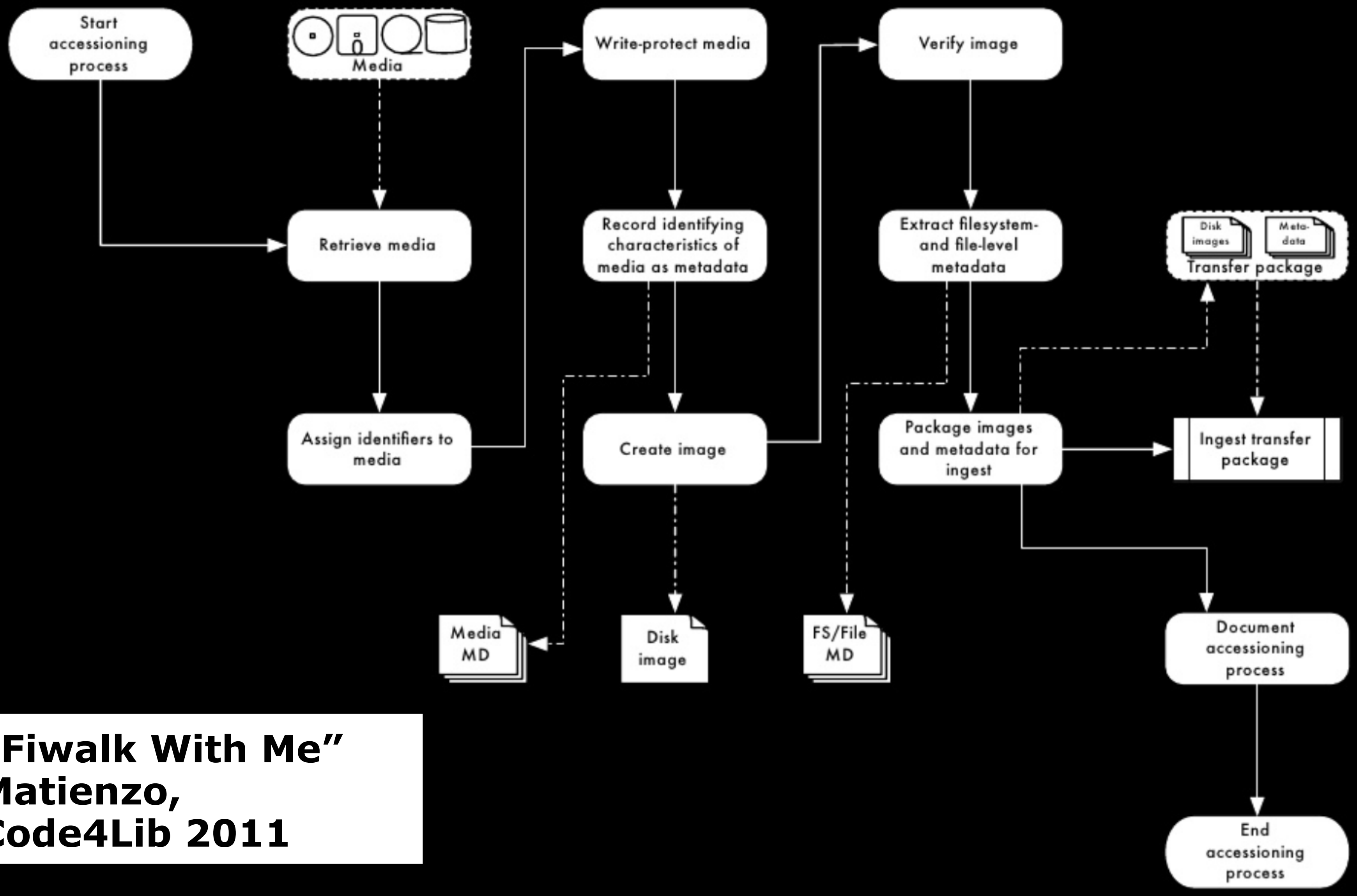
27 different operating systems represented.

Several formats : 8 in., 5¼ in., and 3 ½ in. computer disks, cassettes, cartridges, CD-ROMs.

Crossing Disciplines

Digital Humanities Archives
vs.
Digital Forensics Evidence

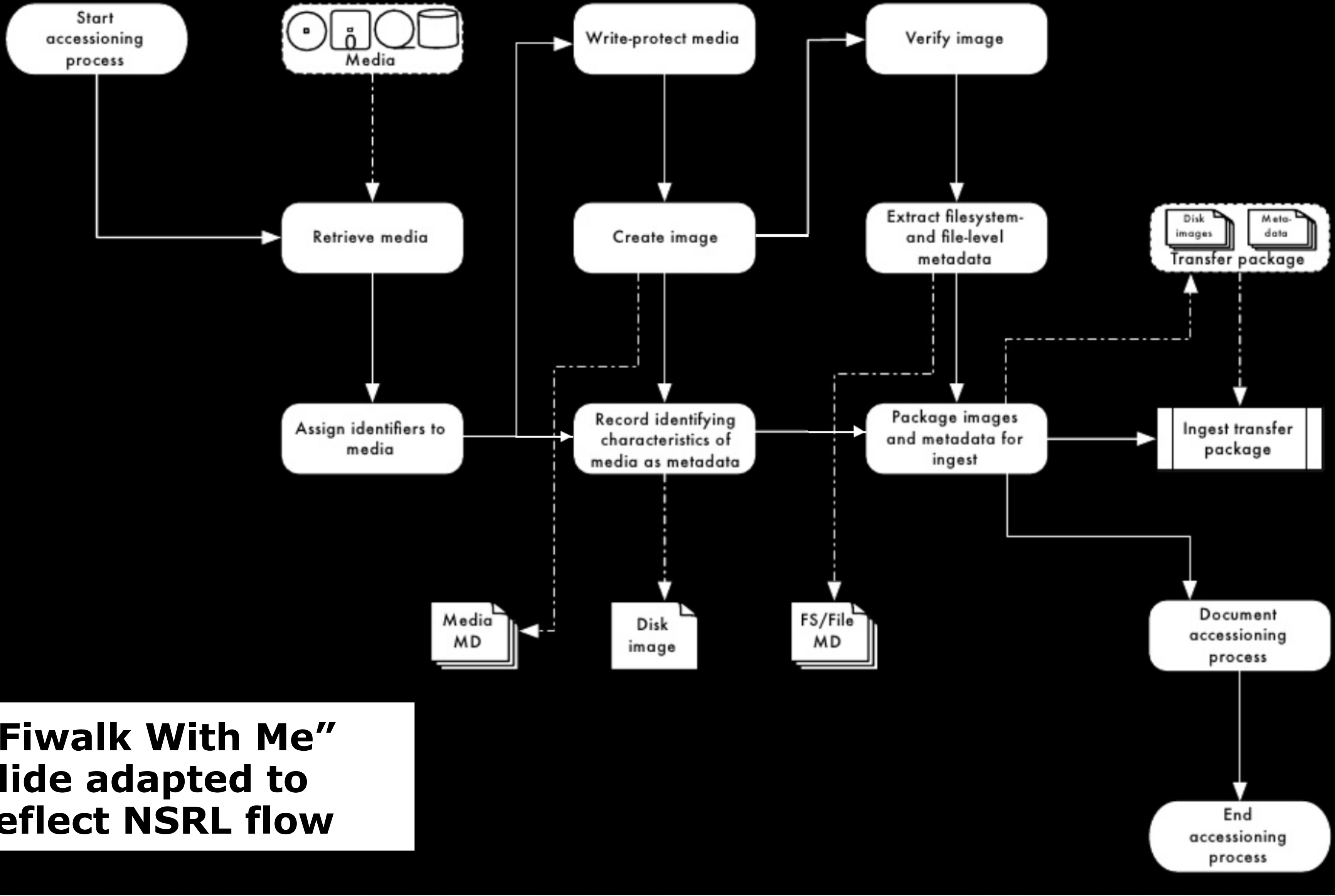
Accessioning Workflow



Start accessioning process
Media
Write-protect media
Verify image
Retrieve media
Record identifying characteristics of media as metadata
Extract filesystem- and file-level metadata
Disk images
Meta-data
Transfer package
Assign identifiers to media
Create image
Package images and metadata for ingest
Ingest transfer package
Media MD
Disk image
FS/File MD
Document accessioning process
End accessioning process

"Fiwalk With Me"
Matienzo,
Code4Lib 2011

Accessioning Workflow



Start accessioning process

Media

Retrieve media

Assign identifiers to media

Write-protect media

Create image

Record identifying characteristics of media as metadata

Media MD

Disk image

Verify image

Extract filesystem- and file-level metadata

FS/File MD

Package images and metadata for ingest

Disk images

Meta-data

Transfer package

Ingest transfer package

Document accessioning process

End accessioning process

“Fiwalk With Me” slide adapted to reflect NSRL flow

Crossing Disciplines

Digital Humanities

Microbiology

Astronomy

Bioinformatics

Unforseen Applications

Used as a resource by the Food & Drug Administration to follow the trail of a potentially fatal substance.

Used as a resource to investigate digital evidence relating to Malaysia Airlines 370.

Zooming Back Out

Descriptions of digital forensics objects

Can be interchanged between tools

Which can be tested and validated

Using common methodologies

And consistently generated test sets

To produce quantifiable assessments

Returning to the OSAC Vision

OSAC Forensic Registries of Standards and Guidelines become implemented in the practice of forensic science across all forensic disciplines

Prosecutors, defense attorneys and judges use the Registries of Standards and Guidelines in direct and cross examinations of expert witnesses

Judges and Juries routinely hear witnesses testify about how their analysis met current standards and scientific validity and openly describe the limitations of the tests in general and their interpretations in the specific case

Significant forensic science research is well organized and well funded with influence from OSAC to define research priorities

Standards enforcement by accrediting bodies becomes the rule

NIST.gov/iaao

The International and Academic Affairs Office (IAAO) supports NIST’s international and academic programs.

IAAO provides advice on international science and technology engagement; serves as liaison with the international science and technology community; manages NIST bilateral and multilateral cooperation; serves as the focal point for foreign visitors and associates, and oversees NIST's cooperation with academia.

ICDF2C / SADFE

Digital Forensics & Cyber Crime

An Overview of Digital Forensics at

NIST

National Institute of Standards and Technology

U.S. Department of Commerce