Computer & Mobile Forensics Standards

Barbara Guttman
bguttman@nist.gov

October 1, 2009

United States Department of Commerce
National Institute of Standards and Technology

What is a Standard?

- Test and Measurement Standard
  - e.g., gram, meter and how you measure it
- Product, Process, and Management standards (aka Documentary or Normative standards)
  - establish the *fitness of a product for a particular use*
  - set specifications for the *function and operation of a device or system*
  - process or management standards, e.g., ISO 9000

Kinds of Standards

- Formal standards (~400 US-based)
  - ANSI-accredited
  - ISO
  - Treaty organizations
- Open Consortia
- Closed Consortia
- Government Agencies
- Some people in the basement
- Proprietary “standards”

Types of CF Standards

- CF Tool Functionality
- Rules for acquisition (collection), preservation, and examination (analysis), and transfer
- Best practices for above
- Training standards
- Test standards

Current Computer Forensics Standards

- IOCE (International Organization on Computer Evidence)
- American Society of Crime Laboratory Directors/ Laboratory Accreditation Board (ASCLD/LAB)
- ASTM
  - E2678 Standard; Guide for Education and Training in Computer Forensics
- ISO SC 27 CS1
- AES (Audio Engineering Society)
  - Authentication of analog tape
- SWGDE & SWGIT
  - Several guidance and best practices documents
- NIST
  - CFTT, NSRL, CFReDS
- NIJ Standards Technical Working Group

SWGDE/SWGIT

SWGIT

1. Guidelines for Field Applications of Imaging Technologies in the Criminal Justice System (Under revision)
2. Recommendations and Guidelines for Using Closed-Circuit Television Security Systems in Commercial Institutions
3. Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System (Updated 1-9-2006)
4. Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System
5. Best Practices for Forensic Video Analysis (released 1-16-2009) NEW
6. General Guidelines for Capturing Latent Impressions Using a Digital Camera (Under revision)
7. General Guidelines for Photographing Tire Impressions (Under revision)
8. General Guidelines for Photographing Footwear Impressions (Under revision)
9. Best Practices for Documenting Image Enhancement
10. Best Practices for Forensic Image Analysis
11. Best Practices for Maintaining the Integrity of Digital Images and Digital Video (released 6-4-2007)
12. Best Practices for Image Authentication (released 6-4-2007)
13. Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System (released 6-4-2007)
14. Best Practices for Forensic Photographic Comparison (released 1-16-09)

Collaboration between SWGIT and SWGDE

- Recommended Guidelines for Developing Standard Operating Procedures
- Guidelines and Recommendations for Training in Digital & Multimedia Evidence
- Proficiency Test Program Guidelines

SWGDE/SWGIT

SWGDE

- **Best Practices for Mobile Phone Examinations**
- **SWGDE Validation Guidelines**
- **SWDGE Standards and Controls Position Paper**
- **SWGDE Live Capture**
- **Peer to Peer Technology**
- **Special Considerations when Dealing with Cellular Telephones**
- **Embedded Technology**
- **Best Practices for Computer Forensics**
- **Data Archiving**
- **Data Integrity**

Why are Standards Good?

- Promote market efficiency and expansion
- Foster trade
- Encourage competition and lower barriers to market entry
- Diffuse new technologies.
- Protect consumers against unsafe or substandard products.
- Enable interoperability among products.

Why are CF Standards Good?

IOCE Goals for standards for CF evidence:

- **Consistency with all legal systems;**
- **Allowance for the use of a common language;**
- **Durability;**
- **Ability to cross international boundaries;**
- **Ability to instill confidence in the integrity of evidence;**
- **Applicability to all forensic evidence; and**
- **Applicability at every level, including that of individual, agency, and country.**

Why are Standards Bad?

When standards work poorly, they can:

- Raise transaction costs and barriers to trade/significant burden for smaller operations
- Constrain innovation and entrench inferior technologies
- And hinder the development of interoperable systems

Standards Success Issues

- There should be a market incentive

A Standard is Like a Product

- Most recent successful standards started small
- The realities of standards development should be understood up front

Issues for Standards
Market Incentive

- Who will build them?
- Who will use them?
- Will they enable someone to make/save money?

Issues for Standards

- What kind of standards should be developed?
- What are the goals that the standards are to achieve?
- Will the standards allow for future innovation?
- Can the standards be developed in a timely manner?

Issues for Standards Development Realities

- **Who has the expertise to write them?**

- **Who has the motivation to write them?**

- **And who will update/maintain the standards?**

Standard Infrastructure

"The nice thing about standards is that there are so many to choose from.”

NIJ Standards Technology Working Group

NIJ Standards for Law Enforcement and Corrections Equipment

Purpose:

- Establish minimum design and performance requirements for equipment and define tests methods to measure performance

Benefits:

- Provides the end user with performance information on key equipment characteristics
- Allows comparison of products based on common testing and minimum requirements
- Provides a level of confidence in a product’s fitness for use

Important Notes about NIJ Standards

- NIJ standards are voluntary
- Manufacturers are motivated to develop products conforming to NIJ standards based on grant funding and law enforcement procurement requirements
  - No regulatory authority to compel conformity to standards
- Grant funding requirements and the need for confidence in performance motivate purchasers to buy products that have been tested to and meet NIJ standards

Examples of NIJ Standards

- **Ballistic Resistance of Personal Body Armor – Revised July 2008**
- **Walk-through and Hand-held Metal Detectors – Revisions; publication goal by mid-2009**
- **Bomb Suit – New; publication goal by mid-2009**
- **Ballistic Helmets – Under revision**
- **CBRN Protective Ensemble Standard – New; nearly complete**
- **Holsters Standard – New; process has begun**
- **Handcuffs Standard – Revision; process has begun**
- **Electronic Monitoring – New; process begins mid-2009**

NIJ Standards:
3 Related Documents

1. **Standard** - Defines minimum design and performance requirements and test methods to assess performance

2. **Conformity Assessment Requirements** – Details the requirements for demonstrating that products conforms to the standard

3. **Selection and Application Guide** - Provides information to assist law enforcement and corrections agency decision-makers, procurement officials, and end users; *directly tied to 1 and 2*

Computer Forensics Standards at NIST

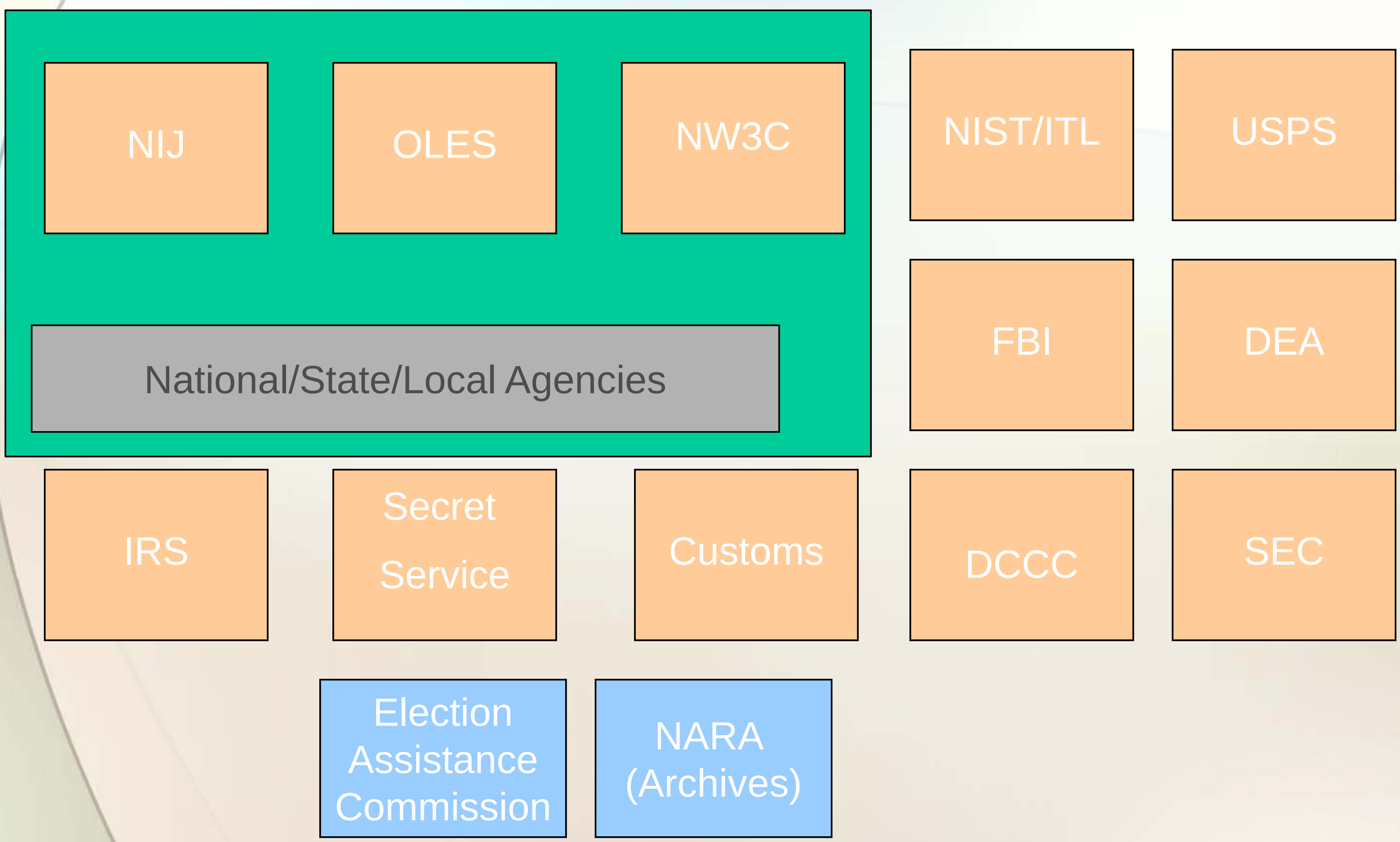
Goals of Computer Forensics Projects

- Support use of automated processes into the computer forensics investigations
- Provide stable foundation built on scientific rigor to support the introduction of evidence and expert testimony in court

Current Computer Forensics Work

- Provide international standard reference data to support investigations and research (NSRL)
- Establish computer and mobile device forensic tool testing methodology (CFTT)
- Provide test material for proficiency testing and lab-based tool testing (CFReDs)

Major Partners



NIJ

OLES

NW3C

National/State/Local Agencies

NIST/ITL

USPS

FBI

DEA

IRS

Secret Service

Customs

DCCC

SEC

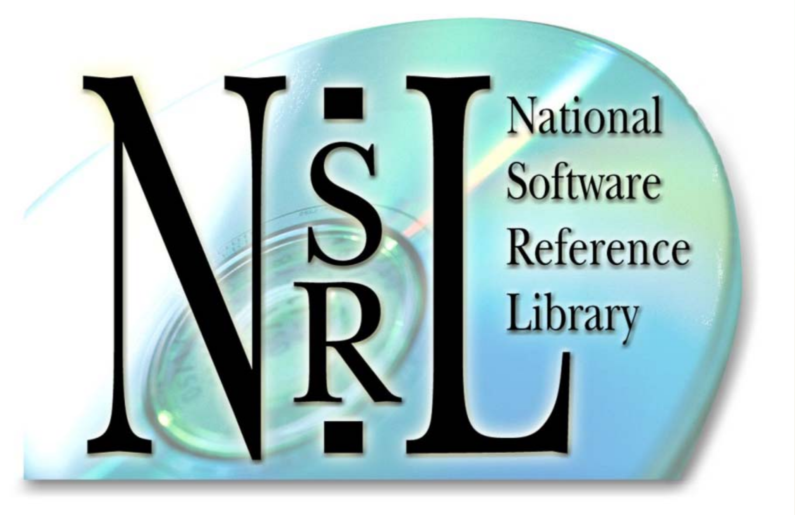
Election Assistance Commission

NARA (Archives)

Why NIST is involved

- Mission: Assist federal, state & local agencies
- NIST is a neutral organization – not law enforcement or vendor
- NIST provides an open, rigorous process

NSRL Project



What is the NSRL?

The National Software Reference Library is:

- A physical collection of over 11,000 software packages
- A database of over 50 million file “fingerprints” and information that uniquely identifies each file – 16 million unique
- A Reference Data Set (RDS) extracted from the database, used by law enforcement, computer security and researchers

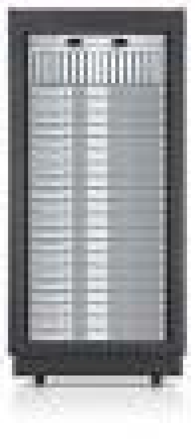
Use of the RDS

- **Eliminate known files from the examination process using automated means**
- **Identify software files for system integrity management**
- **Discover expected file name with unknown contents**
- **Look for malicious files, e.g., hacker tools**
- **Provide rigorously verified data for forensic investigations**
- **Used by all major forensics tools and investigators**

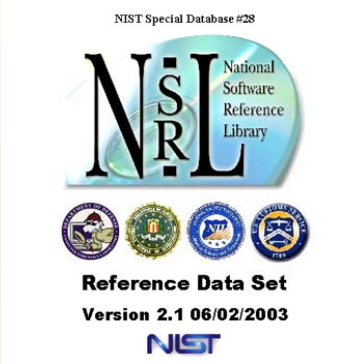
NSRL Process

Collect software

Secure library



Compute file profiles



NIST Special Database #28

NSRL National Software Reference Library

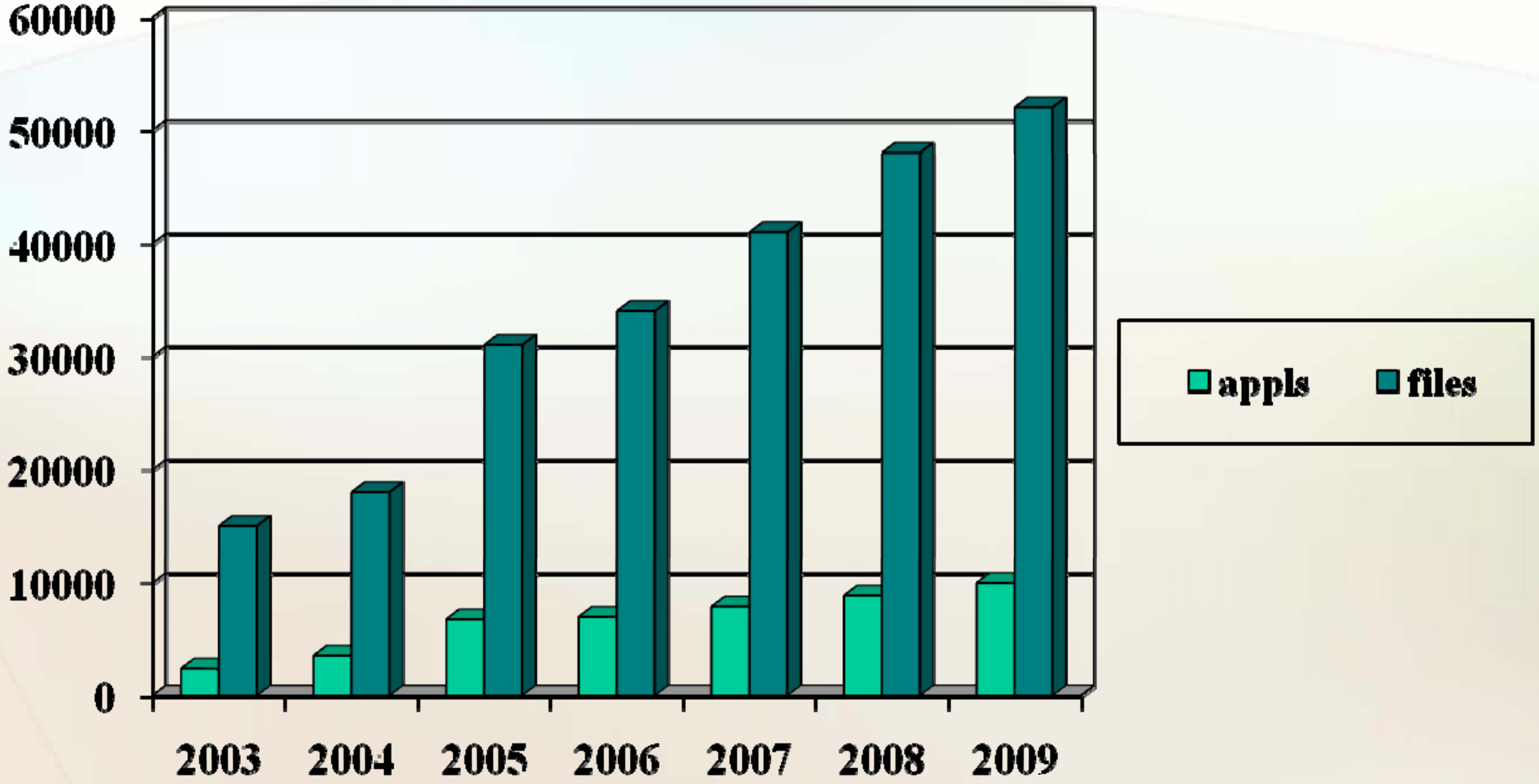
Reference Data Set

Version 2.1 06/02/2003

NIST

Reference Data Set (RDS)

NSRL Growth
(files in thousands)



NSRL Future Plans

- Continue to build and publish the RDS
- New Products & Services:
  - Better support for system integrity management
    - Link to NVD
  - Better support for memory analysis
    - WIRED
  - Better support for rapid data acquisition
    - Block hashing
  - Better support for new research ideas
    - Use of research facility

Computer Forensics Tool Testing (CFTT)

A Problem for Investigators

Do computer and mobile forensic tools work as they should?

- Software tools must be …
  - Tested: accurate, reliable & repeatable
  - Peer reviewed
  - Generally accepted
- … by whom?
- Results of a forensic analysis must be admissible in court

Benefits of CFTT

Benefits of a forensic tool testing program

- Users can make informed choices
- Reduce challenges to admissibility of digital evidence
- Tool creators make better tools

Benefits (cont.)

Testimonial: “Guidance Software wants to thank NIST for their efforts on this study. Objective third parting testing and standards are critical to the advancement of any industry and forensics is no exception. As the leading provider of validated forensics products Guidance Software is in debt to NIST for their work and the positive effect it has had on the advancement of forensics and incident response.”

Ken Basore, VP Research & Development, Guidance Software

Project Tasks

- Identify forensics functions
- Develop specification for each category
- Peer review of specification
- Test methodology for each function
- Report results

Active Areas

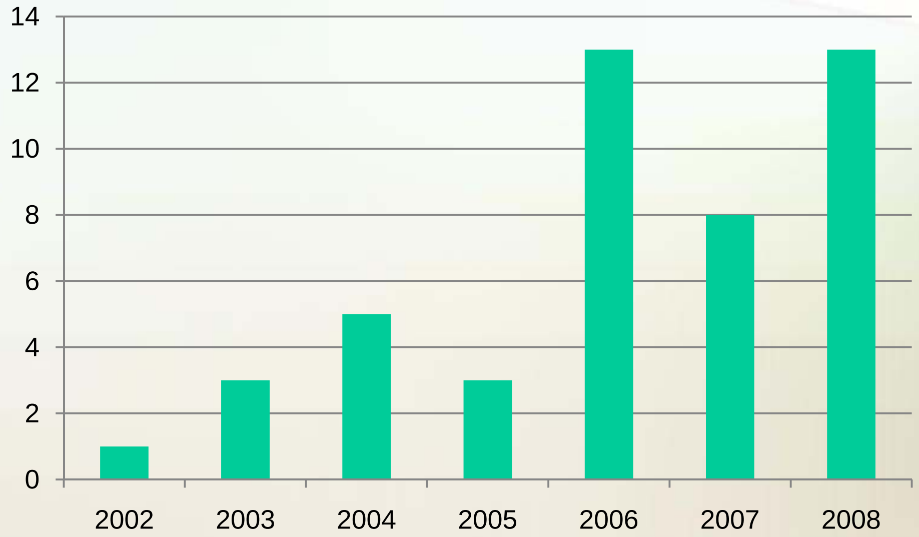
- Disk Imaging
- Hard Disk Write Blocking
- Deleted File Recovery
- Forensic Disk Re-Use
- String Searching
- Mobile Devices
  - GSM
  - Non-GSM
  - Smart Phone

CFTT Reports (since Aug 2002)

Tool Type	Published	Testing/Drafting
Disk imaging	11	5
Software Blocker	9	0
Hardware Blocker	21	2
Mobile Devices	4	6
Drive erase/wipe	0	5

Reports Published on E-Crime Website

- 2002 – one report
- 2003 – 3 reports
- 2004 – 5 reports
- 2005 – 3 reports
- 2006 – 13 reports
- 2007 – 8 reports
- 2008 – 13 reports
- 2009 ~ 15 reports



NIST
Standard Reference Computer Forensic Test Sets

CFReDS

CFReDS

- The CFReDS project provides documented sets of simulated digital evidence.
- Uses for Data Sets
  - Calibration of Forensic Tools
  - Proficiency Testing
  - Tool Testing
  - Training

CFTT Future Plans

- More specifications and test reports
  - Smart Phones
  - Deleted File Recovery
  - String Searching
  - Continue with imaging, blocking & erasing
- More CFReDS images
  - Cell phones
  - Hard drives with proprietary software

Contacts

Jim Lyle
www.cftt.nist.gov
cftt@nist.gov

Doug White
www.nsrl.nist.gov
nsrl@nist.gov

Barbara Guttman
bguttman@nist.gov

Sue Ballou, Office of Law Enforcement Standards
susan.ballou@nist.gov