Computer & Mobile Forensics Standards

Barbara Guttman
bguttman@nist.gov

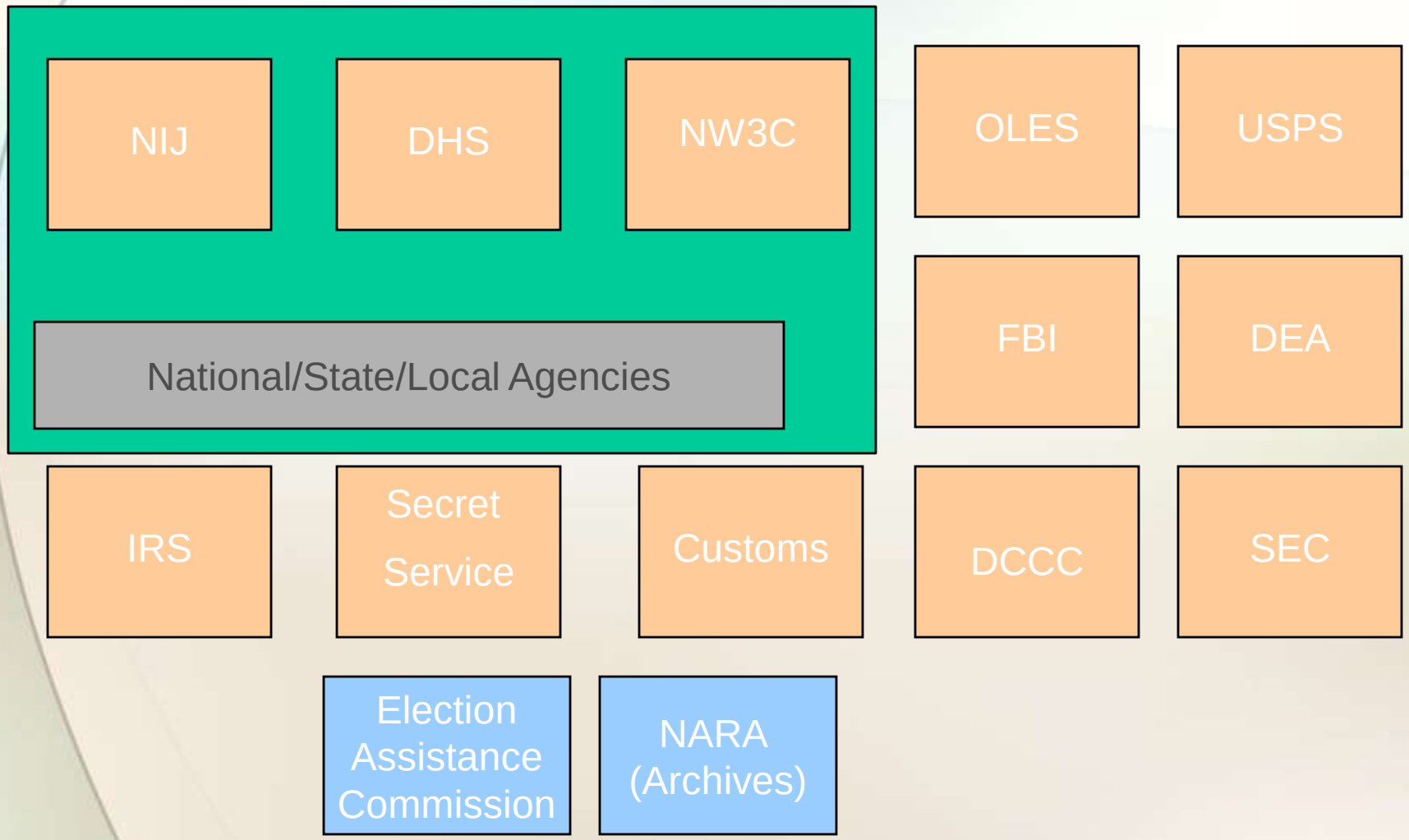
May 14, 2010

NIST United States Department of Commerce
National Institute of Standards and Technology

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)**

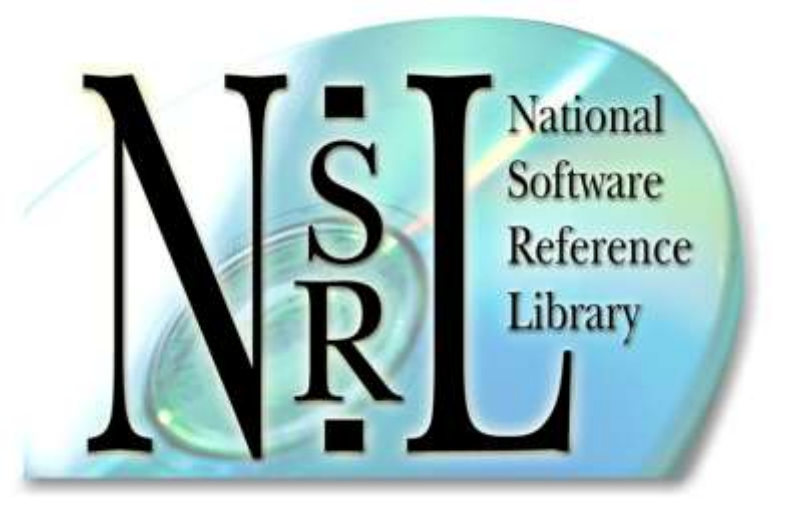
Major Partners



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 12,000 software packages**
- **A database of 60 million file “fingerprints” and information that uniquely identifies each file – 17 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

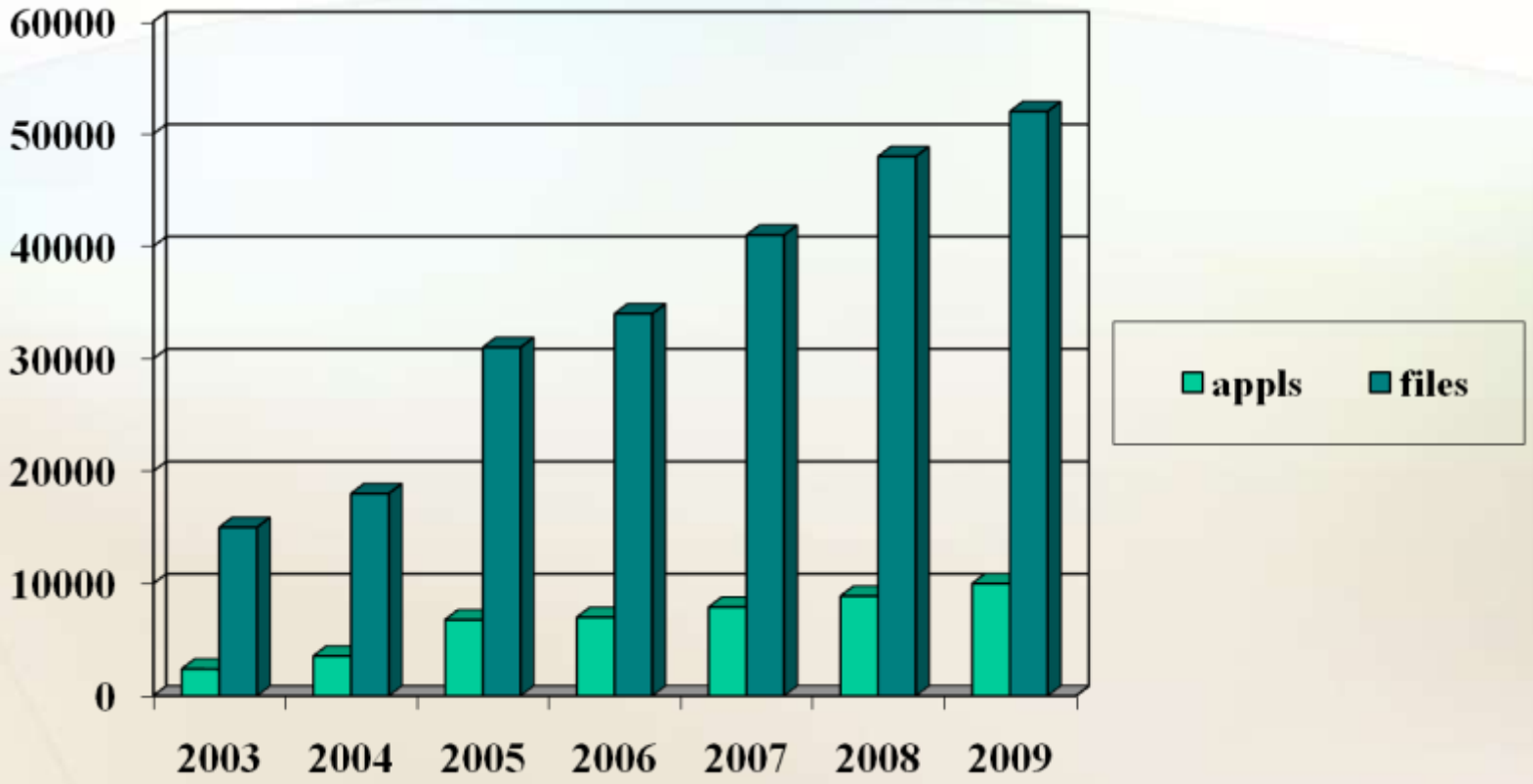
Collect software

Secure library

Compute file profiles

Reference Data Set (RDS)

NSRL Growth
(files in thousands)



Beyond Files Hashes

- Block hashes can find pieces of files
- Fuzzy hashes can find similar files
- Software leaves other traces on a system. E.g., Windows Registry & In Memory
- New methods of software identification will be created
- NSRL publishes/can publish these as well

NSRL & Digital Archiving

- We used many of these techniques to analyze records for NARA.
- Source: redacted GHW Bush records
  - 2.3 GB
  - 51,146 files
- Identified 11,118 unique files
- 8,077 were in the NSRL
- Used fuzzy hashes to find 5,303 pairs of similar files

NSRL and Archiving

- NSRL can be used to identify millions of software files and all the software packages that contain the file.
- Can identify software “pedigree” on a computer – software updates
- Separate and identify software files from user-created files

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 (including help with e-discovery)**
- **Tool creators make better tools**

Active Areas

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

String Searching

- Working with NARA
- Clarify in searching is in records (current files) or between records (deleted files)
- Can search in multiple languages/character sets

Imaging

- Create forensically sound image
- Hard Drives
- RAIDs
- CDs
- Cell phones (1/2 of world's population has a cell phone)

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