

Computer Forensics Standards:

National Software Reference Library Computer Forensics Tool Testing Computer Forensics Reference Data Sets PDA Forensics Research

Barbara Guttman
bguttman@nist.gov
September 21, 2007

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

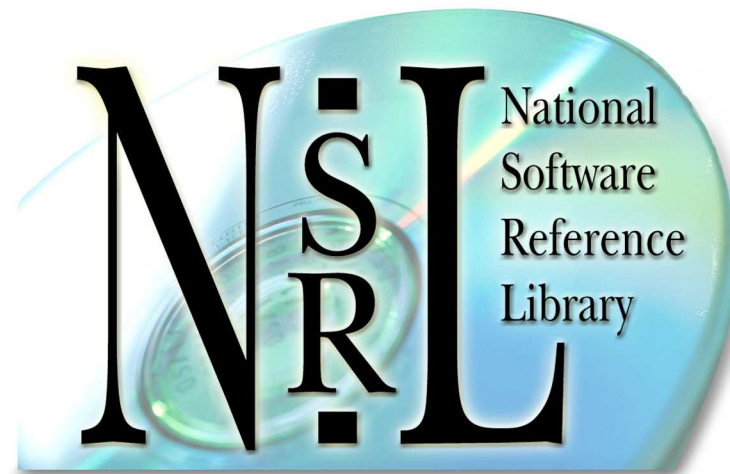
Computer Forensics in NIST

- **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**

Goals of CF at NIST

- **Provide international standard reference data that tool makers and investigators can use in investigations (NSRL)**
- **Establish computer forensic tool testing methodology (CFTT)**
- **Provide test material for proficiency testing and lab-based tool testing (CFReDs)**
- **Research emerging PDA forensics**

NSRL Project



What is the NSRL?

The National Software Reference Library is:

- **A physical collection of over 8,000 software packages**
- **A database of 34 million file “fingerprints” and additional information to uniquely identify each file**
- **A Reference Data Set (RDS) extracted from the database onto CD, used by law enforcement, investigators and researchers**

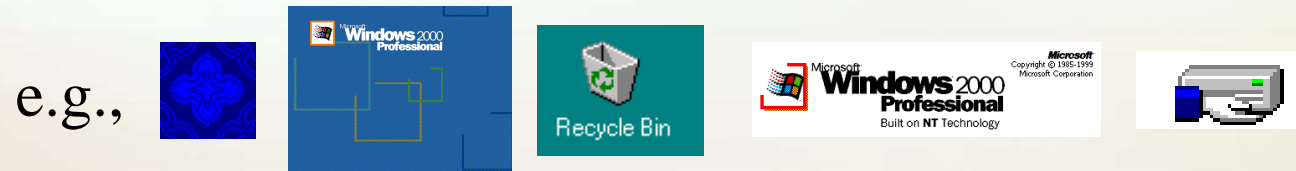
Use of the RDS

- **Eliminate known files from the examination process using automated means**
- **Discover expected file name with unknown contents**
- **Identify origins of files**
- **Look for malicious files, e.g., hacker tools**
- **Provide rigorously verified data for forensic investigations**
- **Used by many forensics tools (ILook, EnCase, FTK)**

RDS Field Use Example

You are looking for images on a computer which is running Windows 2000.

Windows 2000 operating system software contains 5933 images which are known gifs, icons, jpeg files



By using the RDS and an analysis program the investigator would not have to look at these files to complete his investigation.

Are Hashes “broken”?

- **Both MD-5 and SHA-1 have been shown to have weaknesses**
- **The weaknesses do not affect the use of hashes for forensic analysis**
 - **Hash attacks are not “pre-image” attacks**

Computer Forensics Tool Testing (CFTT)



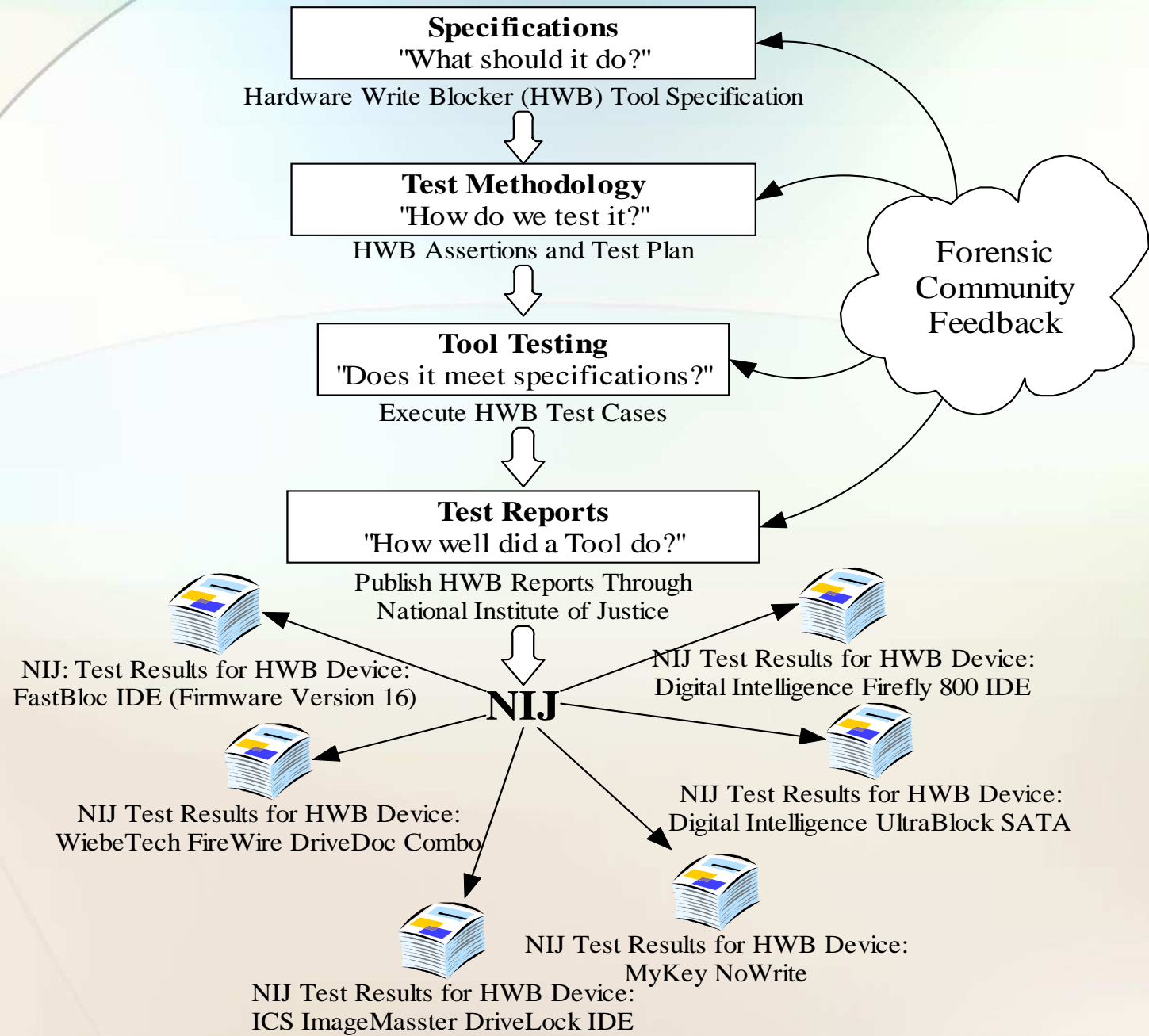
A Problem for Investigators

Do 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**

Project Tasks

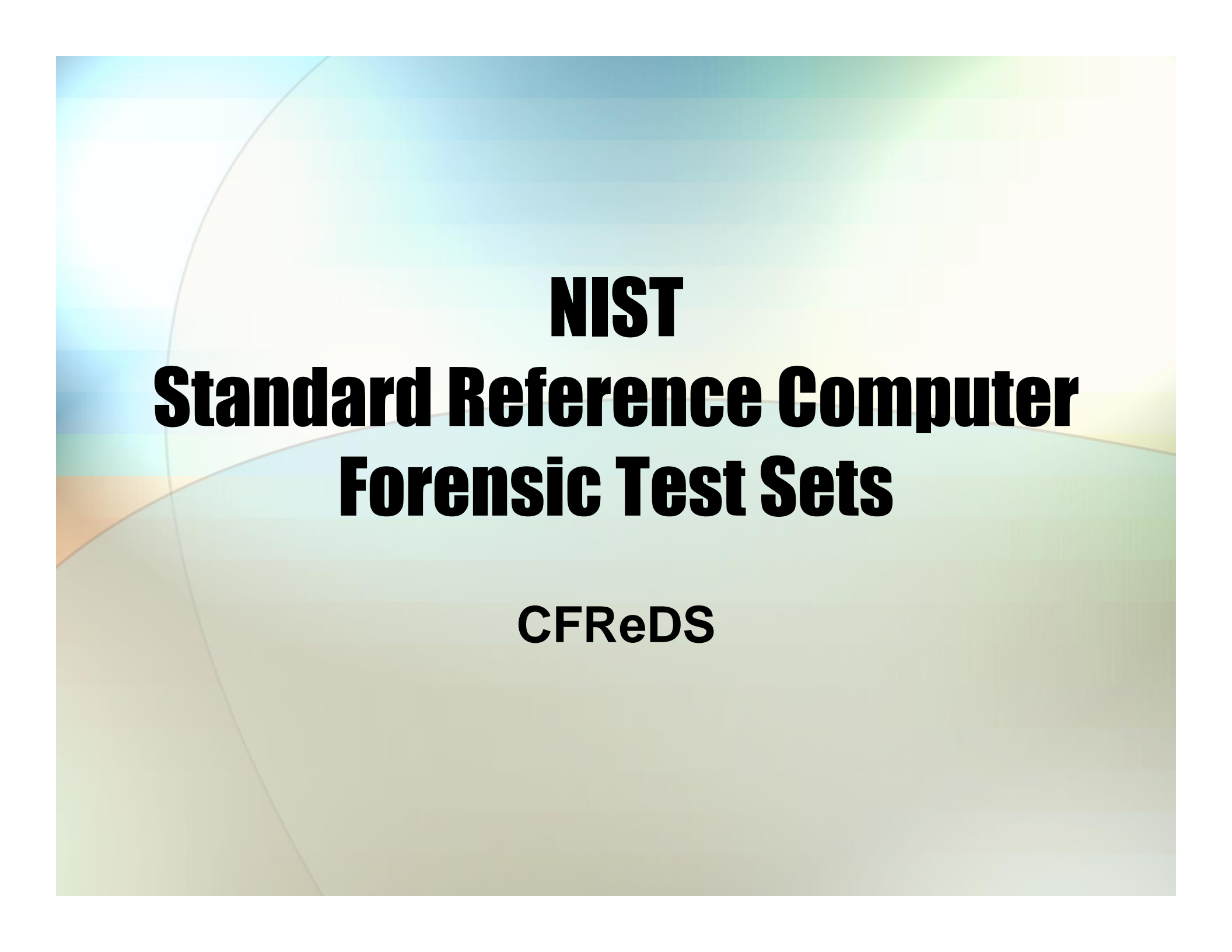
- **Identify forensics functions**
- **Develop specification for each category**
- **Peer review of specification**
- **Test methodology for each function**
- **Report results**



Benefits of CFTT

Benefits of a forensic tool testing program

- **Users can make informed choices**
 - **Odd sector problem**
- **Reduce challenges to admissibility of digital evidence**
 - **Moussaoui case**
- **Tool creators make better tools**
 - **Safeback 2.18**
 - **EnCase documentation**

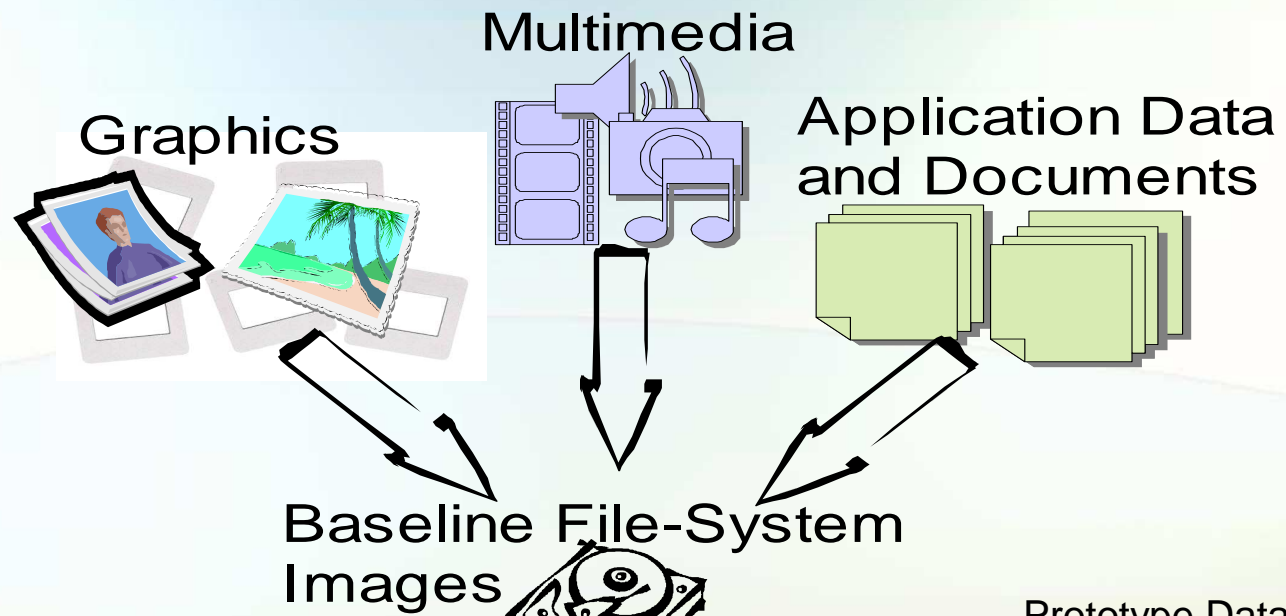


NIST
Standard Reference Computer
Forensic Test Sets

CFReDS

Uses of CFReDS

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



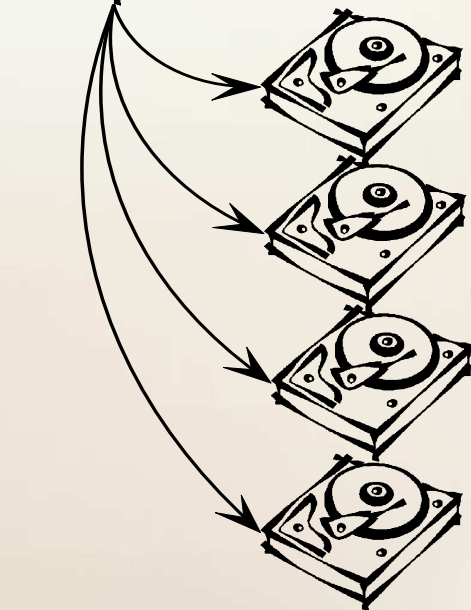
Prototype Data Sets

Russian Team Room
(Big-endian, UTF-8)

Hacking Case

Mac Image (Multiple
File-Systems)

Rhino Hunt



PDA Forensics

- **NIST also performs research on PDA forensics including mobile phones**
- **Provide overview information and guidelines**