National Software Reference Library: Applications in Digital Forensics

Douglas White

National Institute of Standards and Technology
U.S. Department of Commerce

Disclaimer / Disclosure

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.

This research was funded by the National Institute of Standards and Technology Office of Law Enforcement Standards, the Department of Justice National Institute of Justice, the Federal Bureau of Investigation and the National Archives and Records Administration.

NSRL Introduction

Started in 2001 as unbiased source of software metadata.

Software collection contains both physical and digital-only sources.

Used at outset primarily by law enforcement organizations.

Produces short data profiles that uniquely identify a file.

Helps determine which files are important as evidence.

The NSRL aims to be useful to diverse researchers by expanding its holdings and measuring aspects of them in new ways.

National Software Reference Library

16,000+ Applications
2,300+ Manufacturers
750+ Operating Systems
23,000,000+ Unique Files
180,000,000+ File Records
Many Registry entries

Shrinkwrapped & “Clickwrapped” products

Mobile device apps, iOS & Android
Scope: free, popular apps

National Software Reference Library

Applications are categorized, e.g. “Encryption”, “Word Processing”, “Steganography”

Applications are **NOT** categorized as “known good”

Application title, version, vendor, operating system(s)

File path, name, extension, size

Subset of metadata is published quarterly

Schedule: first week of March, June, September and December

National Software Reference Library

RDS – SHA1, MD5, CRC32
Separately: SHA256, SHA512
SHA3: awaiting FIPS release
Block hashes
Approximate matching : Draft SP 800-168
  http://csrc.nist.gov/publications/PubsDrafts.html
Bulk_extractor

Corpus of unique files
Collection of media (disk) images

Installation in virtual machines
Memory
Registry
Network

National Software Reference Library

Taxonomy of applications, OSes

Automated identification: SWIDTags

Interoperability with National Vulnerability Database

CYBOX, DFXML

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.

Contacts

Barbara Guttman, Software and Systems Division
guttman@nist.gov

Douglas White, NSRL
dwhite@nist.gov -or- nsrl@nist.gov

www.nsrl.nist.gov

Susan Ballou, Office of Law Enforcement Standards
Rep. For State/Local Law Enforcement
susan.ballou@nist.gov