National Software Reference Library (NSRL) Exercise

BitCuratorEdu

Last Updated: January 18, 2022

About This Exercise

Author
Cal Lee

Description
This hands-on exercise is meant to introduce students to the National Software Reference Library and the NSRL Lookup command line tool. These slides are excerpted from Cal Lee's SAA "Advanced Digital Forensics" class.

Learning object type
Lesson plan/materials

Learning objectives
This learning object might be used in a lesson to satisfy the following learning objectives:

- Practice using tools in the BitCurator Environment.

National Software Reference Library (NSRL)

- The NSRL (http://www.nsrl.nist.gov) includes a library of hashes of files associated with a large number of software tools developed over the past few decades. See the product list at: http://www.nsrl.nist.gov/RDS/rds_2.41/ProdList.txt. There are various third-party tools that can be used to access the NSRL.

- There's a web interface available at: Visit: http://www.hashsets.com/home/ (Navigate to Hash Set Engines > National Software Reference Library > SEARCH BY NAME / MD5). But it often generates invalid results, so the following instructions are based on running a command-line tool instead.

Using NSRL Hash Sets to Investigate System Files

- Find a directory from your computer that contains system files.
  - For Windows, a good place to look is in Computer > Local Disk (C:) > Program Files. For example, you could select Program Files > 7-Zip.
  - On a Mac, look in /Applications/ and select a specific folder
- Move the contents of the directory to a new folder called system-files on your host computer's desktop.
- Navigate to your shared folders [Desktop > Shared Folders and Media] in the BitCurator environment and copy the folder system-files to the desktop of the BitCurator environment
- Use md5deep to create a set of md5 hashes of the files in the system-files folder, then pipe the output into nsrllookup to generate lists of known and unknown hashes:
  - *md5deep –r ~/Desktop/system-files | nsrllookup –s nsrllookup.com -K known-hashes.txt -Uunknown-hashes.txt*
- What is the above command doing?
- Look at the contents of the two files:
  - type known-hashes.txt
  - type unknown-hashes.txt

For your Reference: Running NSRL Lookup in Windows

- Visit: http://rjhansen.github.io/nsrllookup/ and download the Windows binary (64-bit).
- Open the .zip file and extract the executable to your desktop.
- Visit: https://github.com/jessek/hashdeep/releases and download **md5deep-4.4.zip**
- Open the .zip file and extract md5deep64.exe to your desktop.
- Open a command prompt window (in the start box, type "cmd"). Navigate to your desktop (cd Desktop).
- Type: nsrllookup –help
- Same commands as in previous slide but *use quotation marks around the file path in the command.*

Most resources from the BitCuratorEdu project are intentionally left with basic formatting and without project branding. We encourage educators, practitioners, and students to adapt these materials as much as needed and share them widely.

The BitCuratorEdu project is a three-year effort funded by the Institute of Museum and Library Services (IMLS) to study and advance the adoption of digital forensics tools and methods in libraries and archives through professional education efforts. This project is a partnership between Educopia Institute and the School of Information and Library Science at the University of North Carolina at Chapel Hill, along with the Council of State Archivists (CoSA) and several Masters-level programs in library and information science.