MICROFORENSICS®
DIGITAL FORENSICS SOFTWARE SOLUTIONS

Importing the NIST Hash Set

Introduction

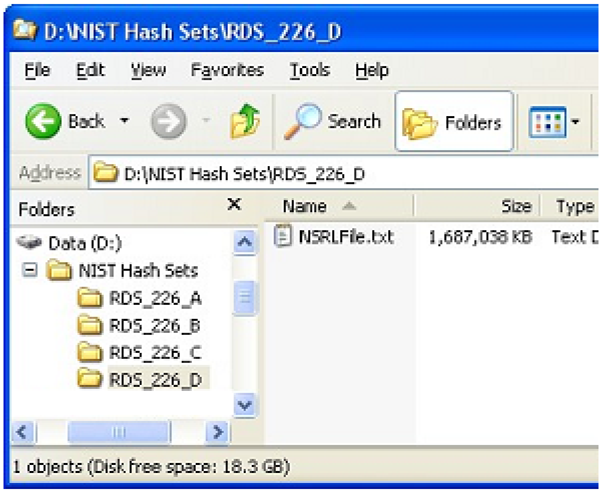
One powerful feature of both Titan Collector and Titan CLI that can reduce the size of data collected, extracted or reviewed is the ability to avoid collecting or extracting standard operating system or application files by utilizing the NIST (NSRL) hash set. Developed and maintained by the National Institute of Standards and Technology, the NIST hash set is a massive hash database developed to identify standard system and software application files. For more information on NIST files, visit the National Institute of Standards and Technology website: http://www.nsrl.nist.gov/

Importing the NIST Hash Set

The first step is to obtain a copy of the NIST hash set, which can be done in multiple ways. The easiest way is to download a converted version of the NIST hash set that is already in a format that Titan Collector/CLI can understand and use. A converted version of the NIST hash set is available on the MicroForensics web site; simply download it and extract the contents of the zip file into the Hash/NIST folder within the Titan Collector installation directory.

A second way is to download the raw NIST hash set from the NIST website and import each NSRL library into Titan Collector. This can be useful if a user would like to use a different version of the NIST hash set than the one provided by MicroForensics, or if a user finds it more defensible to download, verify, and import the NIST hash set personally. It should be noted that Titan CLI cannot use or import the raw NIST database; The NIST database must be converted with Titan Collector. Therefore, even if a user plans to use Titan CLI exclusively, he or she will need to use Titan Collector to import the NIST hash set, and then configure Titan CLI to use the compiled NIST database. The procedure to import the raw NIST hash set is outlined below.

First go to the National Institute of Standards and Technology's website's downloads page, http://www.nsrl.nist.gov/Downloads.htm. On that page are links to four ISO files, labeled "disc 1" through "disc 4". Download and save each of these files; the files will be named RDS_226_A.iso through RDS_226_D.iso, where 226 is the version of the hash set. It is possible to verify that they have been downloaded correctly by comparing the ISOs' signatures to the values found on the NIST website. After the files have been downloaded, the user must extract the files within the ISOs. This can be done in a variety of ways, including burning the ISOs to four CDs and copying the files, mounting the ISOs in a virtual drive and copying the data, or extracting the necessary data using a program like IsoBuster or 7-Zip.



D:\NIST Hash Sets\RDS_226_D

Address: D:\NIST Hash Sets\RDS_226_D

Data (D:)
NIST Hash Sets
RDS_226_A
RDS_226_B
RDS_226_C
RDS_226_D

Name	Size	Type
NSRLFile.txt	1,687,038 KB	Text D

1 objects (Disk free space: 18.3 GB)

Figure 1: Four directories containing extracted NSRLFiles

Inside each ISO are three text files, and one zip file with the same name as the ISO. Open this zip file; inside it are six more text files. The text file that is of interest is named NRSLFile.txt; it is by far the largest of the text files. On a local hard drive, create a folder called “NIST Hash Sets”; within this folder create four directories, one for the NRSLFile.txt from each ISO. Extract NRSLFile.txt from RDS_226_A.iso, and save it in the first directory. Each ISO has a different NRSLFile.txt; repeat this process for each ISO, until all four NRSLFile.txt files have been extracted and saved into their respective folders.

Next Titan Collector will be used to combine these four separate NSRLFile.txt files into the NIST hash database. Open Titan Collector, and then go to Tools > Import NIST Hash Sets. A dialog box will appear; navigate to the “NIST Hash Sets” directory, and open the first NRSLFile.txt. A box titled “Load NIST Hash Progress” with a progress bar will pop up; it may take several minutes for Titan Collector to load the hashes. Once the first file has completed loading, repeat this process with the other three NRSLFiles. Once all four have been loaded, the NIST hash database is ready to be used by either Titan Collector or Titan CLI.

The four NRSLFiles contain many duplicate hashes; as part of the loading process Titan Collector de-duplicates them, creating a database of unique values.   Because of this, if the same NRSLFile is added multiple times, Titan Collector’s NIST database will not grow in size, because all the newly imported hashes will be marked as duplicates. Similarly, if an older NIST hash set is imported after a newer one (say v2.21 is imported when v2.26 has already been loaded), Titan’s NIST database will not grow, as the newer version contains all of the older version’s hashes.