Tools

Developed In-house:

bulk_extractor [1]

- A forensic analysis tool for extracting personally identifiable information and other useful information from digital media.

hashdb (hash database) [2]

- A lightweight database for storing and rapidly searching billions of hashes.

dirim (Directory Imager) [3]

- A suite of metadata analysis tools.

pathtrans

- A tools for natural language translation of file paths.

Sponsored by DEEP Lab:

sdhash (Similarity Digest Hash) [4]

- A tool for identifying binary similarity between arbitrary files, developed by Vassil Roussev at the University of New Orleans

sdtext (Similarity Digest Text) [5]

- A tool for identifying similarity between text documents, developed by Clay Shields at Georgetown University

sceadan (Systematic Classification Engine for Advanced Data Analysis) [6]

- A tool for performing file type classification, developed by Nicole Beebe at the University of Texas San Antonio

Transitioned to other agencies:

Smirk

Autopsy Modules:

- hashdb blacklist scanner