

StegAlyzerAS

Steganography Analyzer Artifact Scanner

BENEFITS

- Search for artifacts of digital steganography applications
- Detect insiders using digital steganography to send sensitive or proprietary information outside of the enterprise network
- Enforce organizational policy prohibiting use of digital steganography or other data-hiding applications
- Search for Microsoft Windows registry artifacts, a feature exclusive to StegAlyzerAS
- Search for file artifacts using the largest steganography application hash set commercially available anywhere
- Verify file artifacts with any of seven different hashing algorithms



¹ <http://www.dc3.mil/dcci/catalog.htm>

² <http://www.cybersciencelab.com>

StegAlyzerAS is a digital forensic analysis tool designed to extend the scope of traditional digital forensic examinations by allowing the examiner to scan suspect media or forensic images of suspect media for known artifacts of over 800 steganography applications.

Artifacts may be identified by scanning the file system as well as the registry on a Microsoft Windows system. StegAlyzerAS allows for identification of files by using CRC-32, MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 hash values stored in the Steganography Application Fingerprint Database (SAFDB). SAFDB is the largest commercially available steganography hash set. Known registry keys are identified by using the Registry Artifact Key Database (RAKDB) distributed with StegAlyzerAS.

StegAlyzerAS was found to be effective for identifying file and registry artifacts by the Defense Cyber Crime Institute (DCCI)¹ and the CyberScience Laboratory (CSL)².

Product highlights in StegAlyzerAS:

- Case generation and management
- Mount and scan forensic images of storage media in EnCase, ISO, RAW (dd), SMART, SafeBack, Paraben Forensic Replicator, and Paraben Forensic Storage formats
- Automated scanning of an entire file system, individual directories, or individual files on suspect media for the presence of steganography application file artifacts
- Automated scanning of the Microsoft Windows Registry for the presence of registry artifacts associated with particular steganography applications
- File and registry artifact evidence viewers allow the examiner to view evidence according to the percentage of artifacts that were discovered for each steganography application detected
- Scan summary viewer allows the examiner to quickly view a statistical summary of any previous scan performed during a particular examination
- Extensive report generation in HTML format
- Automated logging of key events and information of potential evidentiary value
- Integrated help feature to explain specific features and functions

StegAlyzerAS licenses include all product updates for one year.

**BACK
BONE**
SECURITY

Backbone Security Steganography Analysis and Research Center

42 Mountain Park Drive
Fairmont, WV 26554
877-560-SARC or 304-333-SARC
Fax 304-366-9163

RR 5, Box 5282
Upper Cherry Valley Road
Saylorsburg, PA 18353
888-805-4331 or 570-234-0635

www.sarc-wv.com • www.backbonesecurity.com

