StegAlyzerAS

Steganography Analyzer Artifact Scanner

StegAlyzerAS is a steganalysis tool designed to extend the scope of traditional computer forensic examinations by allowing the examiner to scan suspect media or forensic images of suspect media for known artifacts of over 1,150 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). RAKDB is the only commercially available steganography registry key database.

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:

- Versions available for both 32-bit and 64-bit forensic workstations
- 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 from date of purchase. Volume license, government, and educational discounts are available.