StegAlyzerSS

Steganography Analyzer Signature Scanner

StegAlyzerSS 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 over 55 uniquely identifiable byte patterns, or known signatures, left inside files when particular steganography applications are used to embed hidden information within them. Automated extraction algorithms unique to StegAlyzerSS can be used to recover hidden information.

StegAlyzerSS extends the signature scanning capability by also allowing the examiner to use more traditional blind detection techniques for detecting whether information may be hidden within potential carrier files.

StegAlyzerSS was found to be effective for identifying files that contain hidden steganographic data by the Defense Cyber Crime Institute (DCCI)[1] and the CyberScience Laboratory (CSL)[2].

Product highlights in StegAlyzerSS:

- 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 signatures
- Identify files that have information appended beyond a file’s end-of-file marker with the Append Analysis feature and analyze the files in a hex editor view to determine the nature of the hidden information
- Identify files that have information embedded using Least Significant Bit (LSB) image encoding with the LSB Analysis feature and extract and rearrange the LSBs for analysis in a hex editor view to detect hidden information
- Exclusive Automated Extraction Algorithm functionality for selected steganography applications gives examiners a “point-click-and-extract” interface to easily extract hidden information from suspect files
- Extensive report generation in HTML format
- Automated logging of key events and information of potential evidentiary value
- Export session activity and evidence logs in comma separated value (.csv) format
- Integrated help feature to explain specific features and functions

StegAlyzerSS licenses include all product updates for one year from date of purchase. Volume license, government, and educational discounts are available.

BENEFITS

- Search for signatures associated with over 55 steganography applications
- Scan files to discover hidden information to use as evidence of criminal activity that would have otherwise gone unnoticed
- Discover evidence of covert communications
- Determine if trusted insiders are using covert techniques to steal sensitive and proprietary information
- Enforce organizational policy prohibiting use of digital steganography or other data-hiding applications
- Automated Extraction Algorithms allow examiners to “point-click-and-extract” hidden information, a feature exclusive to StegAlyzerSS

[1] http://www.dc3.mil/dcci
[2] http://www.cyberscciencelab.com

Steganography Analysis and Research Center
Backbone Security

STEGANOGRAPHY ANALYSIS AND RESEARCH CENTER
SARC
RAISING THE THRESHOLD OF PERCEPTION

42 Mountain Park Drive
Fairmont, WV 26554
877-560-SARC
Fax 304-366-9163
www.sarc-wv.com

811 Ann Street
Stroudsburg, PA 18360
888-805-4331
Fax 570-234-0636
www.backbonesecurity.com

BACK
BONE
SECURITY