

StegAlyzerSS

BENEFITS

- Scan files to discover hidden information to use as evidence of criminal activity that would have otherwise gone unnoticed
- Discover evidence of covert communications
- Protect your organization's intellectual property and other sensitive or proprietary information
- Determine if trusted insiders are using covert techniques to send sensitive and proprietary information outside of your enterprise network
- 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/catalog.htm>
² <http://www.cybersciencelab.com>

Steganography Analyzer Signature Scanner

StegAlyzerSS 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 over 50 uniquely identifiable hexadecimal 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 other techniques for detecting whether information may have been appended to or 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:

- 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 determine if information has been hidden within the file
- 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.

**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

© 2004 - 2010 Backbone Security.Com, Inc. All rights reserved.
StegAlyzer and Certified Steganography Examiner are registered trademarks of Backbone Security.Com, Inc.

