StegAlyzerFS

Steganography Analyzer Field Scanner

StegAlyzerFS is a steganalysis tool designed to perform rapid field triage on suspect media on computers to detect the use of steganography to conceal information. Often it is necessary to quickly identify potential evidence of concealed information while at the scene. If the information was hidden with a steganography application, currently deployed computer forensic triage tools will not detect it.

A suspect computer can be booted from the StegAlyzerFS device and results can be obtained in a matter of minutes. StegAlyzerFS detects any of the files associated with over 1,225 applications in the Steganography Application Fingerprint Database (SAFDB). SAFDB is the largest commercially available steganography hash set. In addition, StegAlyzerFS detects over 55 uniquely identifiable byte patterns, or known signatures, left inside files when particular steganography applications are used to embed hidden information within them.

Product highlights in StegAlyzerFS:

- Software executes from single USB device
- Requires no installation or configuration
- Does not change target storage media, preserving its forensic integrity
- Automated scanning of entire devices
- Detect file artifacts associated with over 1,225 steganography applications
- Detect signatures associated with over 55 steganography applications
- Scan popular file systems such as ext2, ext3, ReiserFS, XFS, FAT, FAT32, NTFS, ISO and others supported by Linux kernel 2.6.32
- Automated decompression/extraction of the following archive and compressed file types: zip, iso, tar, gz, gz2, bz, bz2, rar, cab, pax, cpio, xar, lha, ar, mtree
- Extensive report generation in HTML format
- Automated logging of key events and information of potential evidentiary value

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

BENEFITS

- Perform rapid triage of suspect computer systems for the presence and use of steganography
- Simple deployment on a USB device
- Does not change target storage media, preserving its forensic integrity
- Detect files associated with over 1,225 steganography applications
- Detect signatures of over 55 steganography applications
- Deploy at crime scenes where time-critical evidence may be present such as missing persons, child exploitation, and threats of imminent danger
- Deploy at border checkpoints to prevent entry and exit of sensitive information such as terrorism, espionage, and trafficking

StegAlyzer FS

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

© 2004 - 2014 Backbone Security.com, Inc. All rights reserved.
StegAlyzer, Certified Steganography Examiner, and the SARC logo are registered trademarks of Backbone Security.com, Inc.