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 1,150 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 1,150 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.
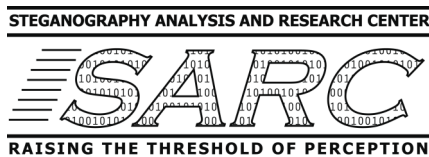

Certified Steganography Examiner Training

Certified Steganography Examiner Training

BENEFITS

- Understand the threat from use of digital steganography to conceal evidence of criminal activity

- Learn techniques used to hide information in carrier files

- Learn how to expand digital forensic examinations to include steganalysis

- Learn how to search for file and registry artifacts

- Learn how to search for known signatures of steganography applications

- Learn how to extract hidden information with "point-click-and-extract" interface

- Earn your Certified Steganography Examiner certification

SARC CERTIFIED STEGANOGRAPHY EXAMINER

Upon completion of this comprehensive two day course, students will have the tools and experience needed to detect the presence and use of digital steganography applications as part of their digital forensic examinations. Students will gain an understanding of the threat posed by the use of steganography in today's interconnected digital world. Students will become familiar with various techniques and methods used for embedding hidden information within carrier files. Students will also gain hands-on experience using a variety of steganography tools while learning how the tools manipulate carrier files.

Students will learn about the Analytical Approach to Steganalysis: an approach developed by the Steganography Analysis and Research Center (SARC) as a result of extensive research of steganography applications and the techniques they employ to embed hidden information within carrier files. The premise of the Analytical Approach is to first determine if a particular steganography application existed on storage media at one point in time. Next, potential carrier file types are identified and examined for known signatures of steganography applications. Once steganography signatures are detected, extraction of the hidden information is possible.

Students will conduct a complete steganography examination from initial suspicion and analysis to detection and recovery of hidden information. The Steganography Analyzer Artifact Scanner (StegAlyzerAS) will be used to scan suspect media for the presence of steganography application artifacts. Students will also learn how to scan for artifacts in the Microsoft Windows Registry, a feature exclusive to StegAlyzerAS. The Steganography Analyzer Signature Scanner (StegAlyzerSS) will be used to identify files containing signatures of steganography applications. Students will learn how to use Automated Extraction Algorithms to extract hidden information from carrier files with a simple "point-click-and-extract" interface, a feature exclusive to StegAlyzerSS.

Steganography Examiner Training consists of six hours of lecture, six hours of practical laboratory exercises, and a two hour written and practical examination. Each student will have access to their own notebook computer containing all tools and laboratory exercises needed for the course. All students will receive a reference CD containing copies of the steganography tools used to hide information as well as all training materials and laboratory exercises. All students who pass the written and practical examination will receive a Certified Steganography Examiner certificate.

If software is purchased with training, the student will also receive fully licensed copies of StegAlyzerAS and StegAlyzerSS. These licenses include all product updates for one year after the class.

On-site and closed-session training are available upon request.

To locate an upcoming training class please visit: http://www.sarc-wv.com/training

---

STEGANOGRAPHY ANALYSIS AND RESEARCH CENTER

SARC

RAISING THE THRESHOLD OF PERCEPTION

Steganography Analysis and Research Center
Backbone Security

42 Mountain Park Drive	811 Ann Street
Fairmont, WV 26554	Stroudsburg, PA 18360
877-560-SARC	888-805-4331
Fax 304-366-9163	Fax 570-234-0636
www.sarc-wv.com	**www.backbonesecurity.com**

BACK BONE SECURITY

Steganography Detection Policy for Fidelis XPS

BENEFITS

- Upgrade the functionality of your existing Fidelis XPS system to detect 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 file artifacts using the largest steganography application hash set commercially available anywhere

Backbone Security is a Fidelis Technology Partner

FIDELIS
SECURITY SYSTEMS

Technology
Partner
Program

Steganography Detection Policy for Fidelis XPS

The Steganography Detection Policy for Fidelis XPS integrates into Fidelis Security Systems' flagship session-level network security solution, Fidelis XPS. The policies are capable of detecting and analyzing digital steganography applications downloaded by insiders on enterprise networks. Built from the world's largest commercially available hash set exclusive to digital steganography applications, the policies can be used to determine whether files traversing the network can be associated with a particular digital steganography or other data-hiding application. The policies contain the fingerprints, or hash values, of each file artifact associated with over 1,150 digital steganography applications.

Product highlights in Steganography Detection Policies for Fidelis XPS:

- Policies are pre-formatted for easy import into Fidelis XPS CommandPost management console for subsequent deployment to Fidelis XPS sensors
- Scan network traffic at the session-level for the presence of steganography applications file artifacts

The Steganography Detection Policy for Fidelis XPS is available on a monthly or annual subscription basis with a minimum term of one year. Subscription level is based on the number of end users connected to the Enterprise network monitored by Fidelis XPS sensors. The subscription includes all policy updates at no additional charge during the subscription period.

STEGANOGRAPHY ANALYSIS AND RESEARCH CENTER

SARC

RAISING THE THRESHOLD OF PERCEPTION

Steganography Analysis and Research Center
Backbone Security

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