SARC Releases Expanded Steganography Hash Set

New Version of Steganography Application Fingerprint Database (SAFDB) Now Available

WASHINGTON, D.C. – Feb. 5 (SEND2PRESS NEWSWIRE) – Backbone Security, the industry leader in advanced digital steganalysis tools, announced the latest version of their market leading Steganography Application Fingerprint Database (SAFDB) at the opening of The Computer Forensics Show in the DC Convention Center.

Developed in Backbone's Steganography Analysis and Research Center (SARC), SAFDB Version 3.2 contains the fingerprints, or hash values, of every file artifact associated with 675 steganography applications.

SAFDB is the world's largest commercially available hash set exclusive to digital steganography and other information hiding applications and is widely used by Federal, state and local law enforcement; intelligence community; and private sector digital forensic examiners to detect the presence of a steganography application on seized digital media. The existence of an artifact of a steganography application is a strong indication the application was used to conceal digital evidence that may be of probative value in a criminal investigation.

Version 3.2 contains the hash values of each file artifact computed with the CRC-32, MD-5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 algorithms along with the artifact file name, file size, and other information about each file artifact.

A free extract of the database, with MD5 hashes only, is available to qualifying U.S. and international law enforcement, government, and intelligence agency digital forensic examiners.

The extract is available in formats that can be imported into EnCase, FTK, Hashkeeper, ILook, and ProDiscover. For information on registering for access to the free MD5 extract of SAFDB V3.0, please visit www.sarc-wv.com.

SAFDB is an integral part of the Steganography Analyzer Artifact Scanner, StegAlyzerAS. In addition to being the most comprehensive steganography artifact detection tool currently available on the market, StegAlyzerAS also offers the unique capability to detect Windows registry artifacts which may make it possible to determine a particular steganography application was used even if the user uninstalled the application and deleted the associated files and folders.

About the SARC
The SARC was established to create and maintain a national repository of steganography applications, fingerprints, and signatures that can be consulted during the forensic examination of seized media. In addition to

creating the world’s largest hash set exclusive to steganography applications, the SARC has become the industry leader in developing world-class forensic tools and techniques for detecting the presence or use of steganography applications and extracting the information hidden with those applications.

About Backbone Security
Backbone is a PCI Data Security Standard (DSS) Approved Scanning Vendor that conducts automated PCI DSS compliance assessments with their industry leading One-Stop Scanning Solution. Backbone also provides real-time intrusion monitoring, certification and accreditation, business continuity planning, and disaster recovery planning services.

Backbone Security, Veteran’s Square, 320 Adams Street, Suite 105, Fairmont, WV 26554. Voice: 304.366.9161, Fax: 304.366.9163. www.backbonesecurity.com or www.sarc-wv.com

News issued by: Backbone Security

Send2Press® Newswire

Original Image: https://www.send2press.com/wire/images/08-0101-Send2Press_72dpi.jpg

# # #

Original Story ID: (3655) :: 2008-02-0205-002

Original Keywords: Backbone Security, Steganography Analysis and Research Center, StegAlyzerAS, digital forensics, The Computer Forensics Show in the DC Convention Center, Steganography Application Fingerprint Database Backbone Security