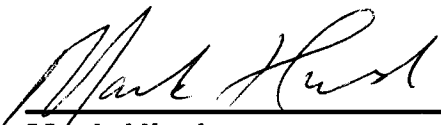


Test Report for

StegAlyzerAS™ V3




December 2007



Mark Hirsh
System Engineer

1/8/08
Date



Edmond Kong, DAFC
Director DCCI

10 JAN 08
Date

Defense Cyber Crime Institute

TABLE OF CONTENTS

EXECUTIVE SUMMARY	III
1. SCOPE	1
1.1 Identification.....	1
1.2 StegAlyzerAS Features and Capabilities.....	1
1.3 Test Approach.....	1
2. TEST DESCRIPTIONS	2
2.1 False Positives.....	2
2.1.1 <i>Test Data</i>	2
2.2 Many Steganography Programs.....	3
2.2.1 <i>Test Data</i>	3
2.3 Remnants.....	4
2.3.1 <i>Test Data</i>	4
2.4 Registry Analysis With Steganography Programs Installed.....	5
2.4.1 <i>Test Data</i>	5
2.5 Registry Analysis Without Installing the Steganography Programs.....	6
2.5.1 <i>Test Data</i>	6
3. SUMMARY OF FINDINGS FOR STEGALYZERAS V3	7
4. VENDOR COMMENTS	8

Defense Cyber Crime Institute

EXECUTIVE SUMMARY

This report describes the tests and procedures used to evaluate StegAlyzerAS™ v3 (Release Candidate 4), a product of the Backbone Security Steganography Analysis and Research Center. StegalyzerAS™ is designed to search suspect media for steganography programs using two approaches: 1) hashing all files on the suspect media and comparing the resulting hashes to hash sets that Backbone Security personnel have identified as meaningful representations of particular steganography program libraries, and 2) scanning the Windows XP registry for indications that known steganography programs have been installed on and/or run from suspect media.

DCCI testing found both the hash set and registry analysis features of StegAlyzerAS are effective for law enforcement and forensic use.

In a controlled test environment, the StegAlyzerAS hash analysis was able to:

- Identify the hash values of a significant number of the files, modules, and applications found in the distribution libraries of a considerable number of steganography programs
- Minimize false hits by ignoring modules and applications that are typically found in steganography program libraries, but are also very common to software development efforts that do not involve the creation of steganography programs
- Identify, with a high degree of accuracy, steganography programs that are currently on or have at one time been on suspect media even though only a small fraction of the library may currently reside on the media

With respect to the Windows XP registry artifact analysis feature, in a controlled test environment StegAlyzerAS was able to recognize situations in which specific steganography programs had been installed on and run from suspect media, for a reasonable number of steganography programs, without producing any false or misleading indicators.

(Note: StegAlyzer, including any suffixes thereto, is a registered trademark of Backbone Security.Com, Inc.)

Defense Cyber Crime Institute

1. SCOPE

1.1 IDENTIFICATION

This report describes the tests and procedures that were used to evaluate StegAlyzerAS, v3 (Release Candidate 4). StegAlyzerAS, a forensic tool that searches a suspect system for known steganography programs, is a product of the Backbone Security Steganography Analysis and Research Center.

The Defense Cyber Crime Institute (DCCI) developed this test report. The intent of the testing was to determine whether StegAlyzerAS provides the law enforcement and forensic communities with an effective means of detecting the existence of steganography programs on suspect media.

1.2 STEGALYZERAS FEATURES AND CAPABILITIES

StegAlyzerAS searches suspect media for steganography programs using two approaches: 1) hashing all files on the suspect media and comparing the resulting hashes to hash sets that Backbone Security personnel have identified as meaningful representations of particular steganography program libraries, and 2) scanning the Windows XP registry for indications that known steganography programs have been installed on and/or run from suspect media. When creating the steganography hash set, Backbone Security personnel have attempted to remove common modules and applications that do not actually provide firm indicators that a particular steganography program resides on suspect media. Although the common modules and applications may be used by steganography program developers, they do not actually provide evidence particular steganography programs currently reside on (or have at one time resided on) suspect media, because the modules and applications are common to a wide range of software development efforts. Similarly, the registry scan is designed to minimize false indicators by ignoring registry entries that resemble steganography program entries but cannot be associated with any particular program with a high degree of certainty.

1.3 TEST APPROACH

StegAlyzerAS's ability to identify suspicious files was evaluated using specially configured hard drives. The hard drive configurations allowed DCCI to determine the extent to which StegAlyzerAS provided false or misleading indicators as well as the extent to which the program was actually able to provide accurate indicators. The test process was designed to not only determine whether StegAlyzerAS is able to identify and provide effective alerts in situations where suspect media contained reasonably complete libraries of steganography programs, but also to determine the program's ability to provide effective alerts in situations where only a small number of highly suspicious files, related to particular steganography programs, were found on suspect media.

Defense Cyber Crime Institute

2. TEST DESCRIPTIONS

2.1 FALSE POSITIVES

The intent of this test was to measure the extent to which StegAlyzerAS generates false positives; that is, to determine the extent to which StegAlyzerAS identifies suspect media as possibly containing steganography programs when in fact no steganography programs have ever been installed on the media. This test used a Windows XP system hard drive configured with many applications that are used to support forensic investigations, many common software development libraries (which are known to have been used by steganography program developers), and publicly available compression tools that are known to have been incorporated into certain steganography programs.

2.1.1 Test Data

Test case ID	AS-01
Test objective	Determine the extent to which StegAlyzerAS incorrectly identifies suspect media as possibly containing steganography programs.
Expected Results	When run against a specially configured Windows XP system hard drive, which contains many forensic investigative tools, many software development libraries that are known to have been used by steganography programs developers, and publicly available compression tools that are known to have been incorporated into certain steganography programs, StegAlyzerAS will identify no more than three steganography programs as residing on the hard drive and for each program identified, no more than three artifacts will be identified.
Test Results	Expected results were obtained.
Test Procedure	StegAlyzerAS was run against the specially configured drive, with both the steganography hash set and the option to scan the Windows Registry selected. After completion the StegAlyzerAS logs were evaluated.
Measure	The number of steganography programs found was determined by counting the entries found in the Case Log that were identified as "Unique File Artifact" and those identified as "Registry Artifact."
Actual Results	No Unique File Artifacts and no Registry Artifacts were identified.
Anomalies	None.

Defense Cyber Crime Institute

2.2 MANY STEGANOGRAPHY PROGRAMS

The intent of this test was to determine whether StegAlyzerAS could correctly identify at least 90% of the steganography programs contained in the DCCI steganography program library data set. This test used a Windows XP system hard drive configured with 85 steganography program libraries.

2.2.1 Test Data

Test case ID	AS-02
Test objective	Determine whether StegAlyzerAS is able to correctly identify at least 90% of the steganography programs contained in the DCCI stego library.
Expected Results	When run against a specially configured Windows XP system hard drive, which contains 85 steganography program libraries, StegAlyzerAS will correctly identify at least 90% of the steganography programs residing on the hard drive.
Test Results	Expected results were obtained.
Test Procedure	StegAlyzerAS was run against the specially configured drive, with the option to scan the registry turned off. After completion the StegAlyzerAS logs were evaluated.
Measure	The number of steganography programs found was determined by counting the entries found in the Case Log that were identified as Unique File Artifact.
Actual Results	StegAlyzerAS identified all 85 steganography program libraries as residing on the hard drive.
Anomalies	None.

Defense Cyber Crime Institute

2.3 REMNANTS

The intent of this test was to determine whether StegAlyzerAS could correctly determine that a steganography program had at one time been resident on the suspect media, even though all but a few elements of the program library had been removed from the media.

2.3.1 Test Data

Test case ID	AS-03
Test objective	Determine whether StegAlyzerAS is able to determine that a particular steganography program has at one time been resident on suspect media even though only remnants of the steganography program library are currently resident on the drive.
Expected Results	When run against a specially configured Windows XP system hard drive, which contains remnants from two steganography program libraries, StegAlyzerAS will provide an alert that implies that the two steganography programs in question appear to have at one time been resident on the drive, and no other programs will be identified as ever having been on the drive.
Test Results	Expected results were obtained.
Test Procedure	StegAlyzerAS was run against the specially configured drive, with the option to scan the registry turned off. After completion the StegAlyzerAS logs were evaluated.
Measure	The number of steganography programs found was determined by counting the Unique File Artifact entries that referenced a unique steganography program.
Actual Results	StegAlyzerAS identified files from the two steganography program libraries as being resident on the hard drive and no other steganography programs were identified as ever having been resident on the drive.
Anomalies	None.

Defense Cyber Crime Institute

2.4 REGISTRY ANALYSIS WITH STEGANOGRAPHY PROGRAMS INSTALLED

The intent of this test was to determine whether StegAlyzerAS is able to examine the Windows XP registry and correctly state that one or more steganography programs have been run from a suspect drive, without producing any false positives. In this test all steganography programs that were known to have been run had at one time actually been installed on and run from the Windows XP operating system drive.

2.4.1 Test Data

Test case ID	AS-04
Test objective	Determine whether StegAlyzerAS is able to examine the Windows XP registry on a hard drive and correctly state that a particular steganography program has been run if the steganography program was at one time installed on and run from the hard drive itself.
Expected Results	When run against a specially configured Windows XP system hard drive, which was known to have had thirteen steganography programs installed on and run from the drive, StegAlyzerAS will be able to examine the system registry and identify at least one of the programs that had been run. Additionally, it will not identify any programs as being run from the drive which were never actually installed on or run from the drive.
Test Results	Expected results were obtained.
Test Procedure	StegAlyzerAS was run against the specially configured drive, with the option to scan the registry selected. After completion the Registry Artifact entries shown in the Scan Summary Log were examined.
Measure	The steganography programs identified as being run from the hard drive were determined by counting the Registry Artifact entries that referenced a unique steganography program.
Actual Results	StegAlyzerAS correctly identified eight of the thirteen steganography programs as having been run from the hard drive and no other steganography programs were identified as ever having been resident on the drive.
Anomalies	None.

Defense Cyber Crime Institute

2.5 REGISTRY ANALYSIS WITHOUT INSTALLING THE STEGANOGRAPHY PROGRAMS

The intent of this test was to determine whether StegAlyzerAS is able to examine the Windows XP registry and correctly state that one or more steganography programs have been run from a suspect drive even though the programs have never been installed on the drive. In this test the steganography programs that were known to have been run were run from a thumb drive inserted into a USB port.

2.5.1 Test Data

Test case ID	AS-05
Test objective	Determine whether StegAlyzerAS is able examine the Windows XP registry on a hard drive and correctly state that a particular steganography program has been run if the steganography program was never installed on the hard drive and was not run from the hard drive itself.
Expected Results	When run against a specially configured Windows XP system hard drive, which was known to have had two of the steganography programs that were correctly identified in test AS-04 run from a thumb drive inserted into a USB port, StegAlyzerAS will be able to examine the system registry and identify at least one of the programs that was run. Additionally, it will not identify any programs as being run from the drive which were never actually run from the drive.
Test Results	Expected results were not obtained.
Test Procedure	StegAlyzerAS was run against the specially configured drive, with the option to scan the drive registry selected. After completion the Registry Artifact entries shown in the Scan Summary Log were examined.
Measure	The steganography programs identified as being run from the hard drive were determined by counting the Registry Artifact line items that referenced a unique steganography program.
Actual Results	No Registry Artifact line items were produced.
Anomalies	None.

3. SUMMARY OF FINDINGS FOR STEGALYZERAS V3

DCCI testing found that both the hash set and registry analysis features of StegAlyzerAS are effective for law enforcement and forensic use.

In a controlled test environment, the StegAlyzerAS hash analysis was able to:

- Identify the hash values of a significant number of the files, modules, and applications that are found in the distribution libraries of a considerable number of steganography programs
- Minimize false hits by ignoring modules and applications that are typically found in steganography program libraries, but are also very common to software development efforts that do not involve the creation of steganography programs
- Identify, with a high degree of accuracy, steganography programs that are currently on or have at one time been on suspect media even though only a small fraction of the library may currently reside on the media

With respect to the Windows XP registry artifact analysis feature, in a controlled test environment StegAlyzerAS was able to recognize situations in which specific steganography programs had been installed on and run from suspect media, for a reasonable number of steganography programs, without producing any false or misleading indicators.

4. VENDOR COMMENTS

Regarding test AS-05, Registry Analysis Without Installing the Steganography Programs, the expected results were not obtained because the capability to detect steganography programs run from a USB thumb drive has not yet been added to StegAlyzerAS. This feature will be included in a future release.