

**DCCI
Test Report
Gargoyle
2007**



Test Report for Gargoyle V2.6


January 2007



Mark Hirsh
System Engineer

1/18/07

Date



Edmond Kong
Acting Director, DCCI

18 JAN 07

Date

TABLE OF CONTENTS

EXECUTIVE SUMMARY	III
1. SCOPE	1
1.1 Identification.....	1
1.2 Gargoyle 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 Complete Steganography Program Libraries.....	3
2.2.1 <i>Test Data</i>	3
2.3 Many Steganography Programs.....	4
2.3.1 <i>Test Data</i>	4
2.4 Remnants.....	5
2.4.1 <i>Test Data</i>	5
3. SUMMARY OF FINDINGS FOR GARGOYLE V2.6	6

EXECUTIVE SUMMARY

Gargoyle, a forensic tool that uses a number of internally developed hash sets to search for known contraband and hostile programs on a suspect system, is a product of Wetstone Technologies. Although Gargoyle is capable of searching for many types of hostile programs, the testing conducted by DCCI used only the Wetstone Technologies steganography hash set.

DCCI testing found that Gargoyle is an effective tool for the law enforcement and forensic communities. The expected results were obtained on all tests conducted. In a controlled test environment, Gargoyle 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

1. SCOPE

1.1 IDENTIFICATION

This report describes the tests and procedures that were used to evaluate Gargoyle, v2.6. Gargoyle, a forensic tool that searches a suspect system for known contraband and hostile programs, is a product of the Wetstone Technologies.

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

1.2 GARGOYLE FEATURES AND CAPABILITIES

Gargoyle searches for contraband and hostile programs using hash sets that have been populated by Wetstone Technologies. When running Gargoyle, the user has the ability to select the particular hash sets that are of interest. All testing conducted by DCCI used only the steganography hash set. No other hash sets were tested or validated.

The steganography program hash values contained in the Gargoyle steganography hash set are those that Wetstone Technologies personnel have identified as meaningful representations of particular steganography program libraries. When creating the steganography hash set, Wetstone 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 that 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.

1.3 TEST APPROACH

Gargoyle'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 Gargoyle 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 Gargoyle 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.

2. TEST DESCRIPTIONS

2.1 FALSE POSITIVES

The intent of this test was measure the extent to which Gargoyle generates false positives, that is, to determine the extent to which Gargoyle 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	GA-01
Test objective	Determine the extent to which Gargoyle 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, Gargoyle will identify no more than three steganography programs as residing on the hard drive and for each program identified, the degree of confidence will be less than 10%.
Test Results	Expected results were obtained.
Test Procedure	Gargoyle was run against the specially configured drive, with the steganography hash set selected. After completion a Gargoyle Investigative Report was produced and the "Programs Detected Summary" portion of the report was evaluated.
Measure	The number of steganography programs found was determined by counting the entries found in the "Programs Detected Summary" portion of the report. The degree of confidence was measured by evaluating the "# of Files" and "Confidence" fields within the "Programs Detected Summary."
Actual Results	No steganography programs were identified as being on the drive. In other words, no false positives were produced.
Anomalies	None.

2.2 COMPLETE STEGANOGRAPHY PROGRAM LIBRARIES

The intent of this test was to determine whether Gargoyle could correctly identify (with a high degree of confidence) suspect media as containing steganography programs when the media contained the entire steganography program libraries. This test used a Windows XP system hard drive configured with three complete steganography program libraries.

2.2.1 Test Data

Test case ID	GA-02
Test objective	Determine whether Gargoyle correctly identifies suspect media as containing steganography programs when the entire program libraries reside on the media.
Expected Results	When run against a specially configured Windows XP system hard drive, which contains the entire libraries of three steganography programs, Gargoyle will identify only these three steganography programs as residing on the hard drive and for each program identified, the degree of confidence will be greater than or equal 90%.
Test Results	Expected results were obtained.
Test Procedure	Gargoyle was run against the specially configured drive, with the steganography hash set selected. After completion a Gargoyle Investigative Report was produced and the "Programs Detected Summary" portion of the report was evaluated.
Measure	The number of steganography programs found was determined by counting the entries found in the "Programs Detected Summary" portion of the report. The degree of confidence was measured by evaluating the "# of Files" and "Confidence" fields within the "Programs Detected Summary."
Actual Results	Gargoyle correctly identified all three steganography program libraries as being on the hard drive and no other steganography programs were identified as being on the hard drive. The degree of confidence for all three program hits was 100%.
Anomalies	None.

2.3 MANY STEGANOGRAPHY PROGRAMS

The intent of this test was to determine whether Gargoyle 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.

2.3.1 Test Data

Test case ID	GA-03
Test objective	Determine whether Gargoyle 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, Gargoyle will correctly identify at least 90% of the steganography programs residing on the hard drive.
Test Results	Expected results were obtained.
Test Procedure	Gargoyle was run against the specially configured drive, with the steganography hash set selected. After completion a Gargoyle Investigative Report was produced and the "Programs Detected Summary" portion of the report was evaluated.
Measure	The number of steganography programs found was determined by counting the entries found in the "Programs Detected Summary" portion of the report.
Actual Results	Gargoyle correctly identified 100% of the 85 steganography programs as being on the hard drive and no other steganography programs were identified as being on the drive.
Anomalies	None.

Defense Cyber Crime Institute

2.4 REMNANTS

The intent of this test was to determine whether Gargoyle 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 for the media.

2.4.1 Test Data

Test case ID	GA-04
Test objective	Determine whether Gargoyle 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, Gargoyle 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	Gargoyle was run against the specially configured drive, with the steganography hash set selected. After completion a Gargoyle Investigative Report was produced and the "Programs Detected Summary" portion of the report was evaluated.
Measure	The steganography programs identified as being on the hard drive was determined by reviewing the entries found in the "Programs Detected Summary" portion of the report.
Actual Results	Gargoyle 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.

3. SUMMARY OF FINDINGS FOR GARGOYLE V2.6

DCCI testing found that Gargoyle, a program that uses a steganography hash set created by Wetstone Technologies to search suspect media for steganography program executables and other files contained within steganography program libraries, is an effective tool for the law enforcement and forensic communities. The expected results were obtained on all tests conducted.

In a controlled test environment, Gargoyle 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