

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



Certified Steganography Examiner Training

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.aspx>

**BACK
BONE**
SECURITY

Backbone Security Steganography Analysis and Research Center

42 Mountain Park Drive
Fairmont, WV 26554
877-560-SARC or 304-333-SARC
Fax 304-366-9163

RR 5, Box 5282
Upper Cherry Valley Road
Saylorsburg, PA 18353
888-805-4331 or 570-234-0635

www.sarc-wv.com • www.backbonesecurity.com

© 2004 - 2010 Backbone Security.Com, Inc. All rights reserved.
StegAlyzer and Certified Steganography Examiner are registered trademarks of Backbone Security.Com, Inc.

