

## Expand the Breadth and Depth of Your Investigation by Discovering the Hidden

Upon completion of this intense two-day course, students will have a complete understanding of the threat posed by the use of steganographic technologies in the current digital environment, and the tools to help mitigate that threat. The course will discuss the tools used by criminals exploiting children, terrorists and crime organizations. Students will learn how suspects create covert communication channels, and how disgruntled employees can easily transmit proprietary information outside the company. Students also learn how to conduct a complete steganography investigation. Stages from steganography suspicion to detection, analysis, cracking, and finally to possible recovery of the hidden information are presented both in lecture and lab environments.

### WetStone Trainings

WetStone's advanced Training Courses provide students with a unique opportunity to learn about using the most advanced digital investigation tools available. Trainings are developed and taught by experts in computer forensics, information security, and field investigation. Investigator trainings are offered at various locations throughout the U.S. and at several cyber security conferences. Students will also receive formal certification that you can use to enhance your professional background.



### Prerequisites

This hands on course is an advanced investigation training that is presented as part lecture and part lab. It is therefore highly suggested that students possess:

- ◇ A background in digital investigation techniques
- ◇ Familiarization with PC's and their operation
- ◇ Familiarization with Microsoft Windows®

### Software and Course Materials

All students are provided laptops for use during the training. This class includes 6 hours of lecture and 6 hours of hands on lab exercises. Course materials, lab exercises and all necessary software is pre-installed.

### Training Slides & Lab Exercises

Students receive full copies of the lecture, lab exercises and reference materials presented throughout the 2 day course.

### Software Package Options

There are options available for students to purchase the software packages used during the class at a discounted rate. The course package would include a copy of Stego Suite™, the most advanced software bundle available for the investigation, detection, analysis, and recovery of digital steganography and Gargoyle Investigator™ Forensic Pro™, which performs rapid searches for known "bad or hostile" programs and their associated files or remnants. For more details on software packages, please contact your sales representative.

MAXIMIZE YOUR TIME

STREAMLINE YOUR INVESTIGATION

UNCOVER HIDDEN EVIDENCE

DETECT COVERT COMMUNICATIONS

### Is Steganography Really a Threat?

In the last decade, the technology for digitally manipulating image, video and audio data has advanced tremendously, resulting in the ability to rapidly hide information in binary data files. Numerous web sites offer "stego" programs free for the downloading. The potential for industrial espionage, trade secret theft, cyber weapon exchange and criminal coordination are boundless.

WETSTONE TECHNOLOGIES, INC.  
17 MAIN STREET  
SUITE 237  
CORTLAND, NY 13045

VOICE: 607.756.6086

FAX: 607.756.6084

SALES@WETSTONETECH.COM

WETSTONETECH.COM

STEGANOGRAPHY INVESTIGATOR TRAINING  
COURSE FEE: \$1,495

SOFTWARE PACKAGES AVAILABLE UPON REQUEST!

IS YOUR DIGITAL INVESTIGATION COMPLETE ?

# Day 1

## Day 1

### Overview

#### Origins & Overview of Steganography

This module provides background information about steganography giving students a solid framework from which to base their digital steganography investigation.

- ◇ History of Use
- ◇ Covert Messaging
- ◇ Null Cipher Messages
- ◇ Steganography vs. Encryption
- ◇ Threats Posed by Steganography Use
- ◇ Steganography in the Media
- ◇ Availability & Production

#### Digital Carriers

This module focuses on digital carrier format, (both images and audio), and the reason they provide the perfect hiding place for data.

- ◇ Used to Exploit Human Weaknesses
- ◇ Digital Images
  - ◇ Palette
  - ◇ True Color
  - ◇ Compressed
  - ◇ Lossy, Lossless
  - ◇ Formats: BMP, JPG, GIF, PNG
- ◇ Digital Audio
  - ◇ Converters
  - ◇ Signal Processors
  - ◇ Wav files
  - ◇ MP3
  - ◇ Dangers

#### Steganography Embedding Tools

Steganography tools are readily available and increasing both in number and complexity. This module describes each method in depth and gives examples of each method.

- ◇ Steganography Methods
  - ◇ Data Appending
  - ◇ Formatting Modification
  - ◇ Word Substitution
  - ◇ Color Palette Substitution
  - ◇ 24 Bit LSB Encoding
  - ◇ DCT Modification
  - ◇ PNS Modification
  - ◇ Covert Channels
- ◇ Tools vs. Carrier Types

### The Practice

#### Tool Demonstration

- ◇ Gargoyle Investigator™
  - ◇ Evidence of Stego Programs
- ◇ Stego Watch™
  - ◇ Detection
- ◇ Stego Analyst™
  - ◇ Analysis
- ◇ Stego Break™
  - ◇ Breaking

#### Lab 1-Steganography In Action

This lab will show students how to utilize a variety of steganography tools and methods. Carrier, payload and covert messages are created and examined.

## Day 2

## Day 2

#### Lab 2-Digital Carrier Interrogation

Students visually examine multiple sets of images and audio files containing various forms of steganography. Using Stego Analyst™, students examine image characteristics including LSB values, true color rendering techniques, color palettes, DCT coefficient histograms and digital audio recording anomalies.

#### Lab 3-Steganography Program Search

This lab teaches students how to identify the suspected use of steganography programs. Using Gargoyle Investigator™ Forensic Pro to search the suspect system, students are able to quickly identify if steganography is present and will learn how interpret and narrow the results to focus the investigation toward files of high threat.

#### Lab 4-Steganography Discovery

This lab shows students how to utilize Stego Watch™ to perform both probabilistic and signature based scans. After running multiple steganography investigations with Stego Watch™, students use Stego Analyst™ to further validate and confirm their findings.

#### Lab 5-Steganography Cracking

In this lab, students run Stego Break™ to perform direct dictionary and brute force attacks against known steganography files. With the results from Stego Break™, students are able to extract and recover steganographic content.

### Certification

#### Steganography Investigator Certification

Students have the option to take the Steganography Certification written and practical examinations. In order to achieve the certification, students must pass both portions of the exam. After completion, students will receive a certified certificate that is timestamped and traceable by our secure time division providing students a formal certification for the class.

