Steganography Investigator Training is an intense two-day course designed to provide students with 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 steganography 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.

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 downloading and it often does not require any type of identification. It is no longer correct to assume that those suspects using steganography are advanced. As it become easier and easier to obtain tools to create such messages, we are finding a broader base of users. The potential for industrial espionage, trade secret theft, cyber weapon exchange, and criminal coordination are boundless.

Who Should Attend?
- Criminal Investigators
- Local, state and federal law enforcement
- Private investigators
- IT security professionals
- Security auditors

Skills Learned
Upon completion of the course, students will have gained knowledge in the fundamentals of the steganography investigation process.

- Identification of steganography programs
- Image analysis and characteristics
- Steganography embedding tools
- Evidence extraction
- Identify digital carrier files

Our trainers take you inside the minds of today’s criminals. Students completing the class will be able to execute a full investigation in the respective discipline. Participants’ proficiency in the above skills will be tested with certification exams.

Course Materials
- Cyber safe lab environment
- Full copy of lecture and lab exercises
- Reference materials
- Written and practical exams

WetStone’s advanced training courses provide students with a unique opportunity to learn about using the most advanced digital investigation tools available. We differ from other vendors focusing our training on the expertise of the subject matter, not a vendor specific product. We feel that with the proper knowledge and specific techniques learned from the experts, each student walks away capable of completing a full investigation using the tools in the respective field. Trainings are developed and taught by experts and we carry out several classes in conjunction with major cyber security conferences each year. Visit us online to find a class near you!

sales@wetstonetech.com · www.wetstonetech.com
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 and 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.
- 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

Tool Demonstration
- Stego Hunter™-Stego program identifier
- Stego Watch™-State-of-the-art detection tool
- Stego Analyst™-Image and audio analysis
- Stego Break™-Extract hidden messages

Lab 1-Steganography In Action
Objective:
This lab will show students how to utilize a variety of steganography tools and methods. Carrier, payload and covert messages are created and examined.

Expected Outcome:
- Create and examine carrier payloads and covert messages
- Become familiar with programs such as Stools, JP Hide & Seek and Camouflage

Lab 2-Digital Carrier Interrogation
Objective:
Students visually examine multiple sets of images and audio files containing various forms of steganography.

Expected Outcome:
- 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
Objective:
Students learn how to identify the suspected use of steganography programs and how to rapidly detect programs currently installed and even remnants left behind.

Expected Outcome:
- Utilize Stego Hunter™ to quickly identify if steganography is present

Lab 4-Steganography Discovery
Objective:
Utilize Stego Watch™ to perform both probabilistic and signature based scans

Expected Outcome:
- Quickly scan and detect carrier files
- Open Stego Analyst™ to further validate and confirm findings.

Lab 5-Steganography Cracking
Objective:
Students utilize Stego Break™ to perform direct dictionary and brute force attacks against known steganography files.

Expected Outcome:
- Students are able to extract and recover steganographic content
- Reveal hidden covert messages

Steganography Investigator Certification
Our certification approach is unique as it certifies the student on the specific tools used in class AND the techniques of the investigation process broadening the student’s expertise in the respective subject matter.

In order to achieve certification, students must pass both the written and practical exams. Students will be notified of passing grades within two weeks of the completion of the class and a certificate, will then be mailed to you directly.