

Expand the Breadth and Depth of Your Investigation by Revealing Hostile Cyber Weapons

Upon completion of this intense two-day course, students will have a complete understanding of the threat posed by the use of **malicious software** or malware in the current digital environment, and the tools to help mitigate that threat. The course will discuss the tools used by criminals, terrorists and crime organizations. Students will learn how suspects create, deploy and utilize malware for political, social and economic gain. Over a dozen categories of malware are discussed, demonstrated and put into use during our detailed lab exercises.

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 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 4 hours of lecture and 10 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 package used during the class at a discounted rate. The course package would include a copy of Gargoyle Investigator™ Forensic Pro™, which performs rapid searches for known "bad or hostile" programs and their associated files or remnants. For more details on the software package, please contact your sales representative.

MAXIMIZE YOUR TIME

STREAMLINE YOUR INVESTIGATION

COUNTER THE TROJAN DEFENSE

INSTANTLY PROFILE SUSPECT'S MALWARE TENDENCIES

What is Malware?

Along with viruses and worms, one of the biggest threats to computers on the Internet today is malware. Malware, short for **malicious software**, is any program designed to wreak havoc, hide potentially incriminating information, and/or disrupt or damage computer systems. Examples of malware include Trojans, key loggers, denial of service tools, virus toolkits, encryption and steganography tools and more.

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

VOICE: 607.756.6086
FAX: 607.756.6084
SALES@WETSTONETECH.COM

MALWARE INVESTIGATOR BOOTCAMP
COURSE FEE: \$1,495

SOFTWARE PACKAGES AVAILABLE UPON REQUEST!

IS YOUR DIGITAL INVESTIGATION COMPLETE ?

Overview

Origins & Overview of Malware

This module provides background information about how to detect malware programs, conduct hash searches and create datasets for digital investigations.

- ◇ Categories
- ◇ Threat
- ◇ Construction
- ◇ Deployment Methods

This module goes into detailed discussion, examination and decomposition of the following categories with specific examples of each:

- ◇ Botnets
- ◇ Rootkits
- ◇ Worms
- ◇ Trojans
- ◇ Keyloggers
- ◇ Denial of Service
- ◇ Steganography
- ◇ Encryption
- ◇ Fraud
- ◇ Anti-Forensics
- ◇ Password Cracking

The Practice

Lab 1-Network Surveillance

This lab demonstrates the tools and techniques necessary for monitoring and infiltrating a wireless network. Using various pieces of network surveillance software, students learn how to gather vital information about a wireless network, capture network traffic attack, 64-bit WEP encryption, and authenticate into a secured network.

Lab 2-Trojan Horses and Password Crackers

This lab provides students with in-depth hands-on experience with Trojan horse, password cracker, and credit card fraud applications. Students will gain knowledge on conducting stealth, back-door attacks on remote machines, acquiring and breaking password protected corporate documents, and generating and validating authentic fraudulent credit card data.

Day 2

Day 2

Lab 3- Steganography and Anti-Forensics

Students are introduced to the dangers of data hiding. Students will utilize a variety of steganography tools and methods to hide various pieces of data. In addition, students will learn methods and techniques used to alter file properties.

Lab 4-Keyloggers

Students gain the necessary knowledge to successfully install and configure a keylogging application. Students have the opportunity to conduct a real-world keylogging attack on the instructor as he or she navigates the Internet. Advanced keylogging techniques such as remote logging and website viewing are also covered.

Lab 5-Botnets, Rootkits and Denial of Service

This lab introduces three of the most dangerous categories of malicious software present today, botnets, rootkits, and denial of service applications. Students utilize botnet software to create a network of zombie computers, hide the presence of this software with a rootkit, and finally conduct a distributed denial of service attack on an actual website in order to render it useless.

Lab 6- Gargoye Investigator Hard Drive

Students conduct a malicious software search on a physical hard drive. Using Gargoye, students conduct a malware investigations from start to finish.

Lab 7- Gargoye Investigator EnCase® Hash File

In this lab, students learn how to use the Gargoye EnScript to successfully generate and export a hash file from EnCase. Using Gargoye, this hash file is then imported and scanned for the presence of malicious software.

Lab 8- Gargoye Investigator FTK® Hash File

Students walk away with the knowledge necessary to integrate Gargoye into a Forensic Toolkit investigation. Students learn how to create an evidence database within Forensic Toolkit, convert this database to a hash file, and successfully import the hash file into Gargoye.

Lab 9- Gargoye Investigator Mobile Investigation

Students conduct a simulated mobile, onsite investigation of a suspicious machine, customize the way Gargoye displays its results, and learn how to interpret the dataset risks Gargoye provides.

Lab 10- Gargoye Investigator Drive Image

Students use Gargoye Investigator Forensic Pro to mount and investigate a logical drive image. Prior to conducting a malware scan of the logical drive image, students learn how to configure Gargoye Investigator to provide email notification of the completed scan.

Lab 11- Gargoye Investigator Dataset Creator

Students create custom datasets using Gargoye's Dataset Creator. Students gain hands-on knowledge creating both contraband and malware datasets. Upon completion of the custom datasets, students utilize the newly created datasets to detect malicious applications.

Certification

Malware Investigator Certification

Students have the option to take the Malware 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.

