

Expand the Breadth and Depth of Your Digital Investigation by Going “Live”

Students will learn techniques for acquiring digital evidence from a running target host in an overt or covert manner. This includes running process state, open handles, process/port associations, system logs, installed devices, physical and logical drives, network statistics and configuration, user accounts, logged in users. Class participants will also learn how to acquire volatile memory and/or registry snapshot of the target host. This would include recently used applications and documents, recently visited web sites, chat logs and e-mails. The physical RAM capture may contain vital password and account information, remnants of visited web sites, recent messages, phone numbers, e-mail addresses and chat identities.

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, networks and their operation
- ◇ Familiarization with Microsoft Windows®

Software and Course Materials

All students are provided laptops for use during the training. This class includes 8 hours of lecture and 8 hours of hands on lab exercises. All course materials, lab exercises and 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 LiveWire Investigator™, which applies digital forensics technology to the investigation of live, running computer systems and LiveDiscover™, a network mapping tool. For more details on software packages, please contact your sales representative.

IS YOUR
DIGITAL INVESTIGATION
COMPLETE ?

Why “Live” Investigation?

Live digital investigation of a suspect system is the next generation technique for Forensic Examiners, Private Investigators, federal, state and local Law Enforcement Investigators, prosecutors and corporate IT security personnel. LiveWire Investigator™ and it's associated suite of products provides extensive and comprehensive information regarding evidence contained on 'live-running' networks, computers, servers and network enabled devices .

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

VOICE: 607.756.6086
FAX: 607.756.6084
SALES@WETSTONETECH.COM
WETSTONETECH.COM

LIVEWIRE INVESTIGATOR TRAINING
COURSE FEE: \$1,495

SOFTWARE PACKAGES AVAILABLE UPON REQUEST!

Overview**Why Investigate Live Running Systems?**

Obtain evidence lost during postmortem investigations:

- ◇ Volatile Memory
- ◇ System State
- ◇ Current User Activity
- ◇ File System Status
- ◇ Active Network State & Connections
- ◇ Comprehensive Enterprise Investigation

Live Investigation — What is it?

- ◇ Real-time IP based acquisition, analysis & examination
- ◇ Quickly Evaluate Events & Situations
- ◇ Perform Detailed Analysis
- ◇ Provide Quality Information

Relevant Standards

- ◇ ISO 1770
- ◇ NIST Special Publication: 800-61
- ◇ Gramm-Leach-Bliley Act
- ◇ Sarbanes Oxley
- ◇ HIPAA

Live Evidence Collection

- ◇ Physical vs. Digital Investigations
- ◇ Forensic Evidence Collection & Preservation
- ◇ Digital Hashes
- ◇ LiveWire Inquiry
 - ◇ General System Information (OS, memory, etc.)
 - ◇ System Event Log
 - ◇ Security Event Log
 - ◇ Remote Registry Examination
 - ◇ Startup/Login Items in Registry & Profile Directories
 - ◇ Application Event Log
 - ◇ Ethernet & Network Protocol Statistics
 - ◇ Time/Date
 - ◇ Environmental Variable Definitions
 - ◇ Running Process Information
 - ◇ Process Thread Information
 - ◇ Registered Services & Drivers
 - ◇ Open Handles & DLLs
 - ◇ Process/Port Associations
 - ◇ Logged In Users
 - ◇ User Account Lists & Groups
 - ◇ SMB Connection List
 - ◇ Open Network Shares
 - ◇ IP Interface Configuration & Routing Table
 - ◇ Ethernet ARP Table
 - ◇ Local NMB Network
 - ◇ All Network Connections/Listeners
 - ◇ NETBIOS Local Name Table
 - ◇ Disk & File Search

Live Cyber Weapons Search

- ◇ Assessing Hostile Software Usage
 - ◇ The Threat
 - ◇ Investigative Response

Importance of Secure Time for Live Investigation

- ◇ Digital Evidence Time Stamping

The Practice**Demonstration of Live Investigation Techniques**

- ◇ LiveDiscover™
 - ◇ Mapping the Enterprise
- ◇ LiveWire Investigator™
 - ◇ Live Search & Seizure
- ◇ Gargoyle Investigator™
 - ◇ Live Cyber Weapon Identification

Lab 1 - Live Network Discovery

Introduction to LiveDiscover™ teaching students to quickly discover the machines in a network as well as potential vulnerabilities in the network infrastructure.

Lab 2 - LiveWire Inquiry

This lab introduces the concept of on demand investigation, utilizing the covert transient utility present in LiveWire. View event logs, running processes, open ports, logged in users and an array of other volatile information acquired during an initial acquisition.

Lab 3 - LiveWire State Acquisition

Would you like to peek into memory and walk a suspect's registry? Students are able to perform detailed analysis of running memory whether looking for user names, passwords, or detailed content of open files. Also examine a registry over the wire and take note of the installed software or recently opened files.

Lab 4 - LiveWire Acquire Disk Data

Students learn to walk a file system and search the contents of a remote hard drive. Learn how to craft searches and utilize LiveWire to perform rapid investigative triage.

Lab 5 - Violation of Corporate Policy

Perform an internal corporate audit against a unsuspecting machine. Examine every aspect of this machine to see if there are benign processes or incriminating evidence in memory.

Lab 6 - Suspected Child Abduction

In a time sensitive missing child case, students are asked to recall their skills to investigate the machine of the missing child and try to recover any evidence that can be used to their benefit.

Certification**Live Investigator Certification**

Students have the option to take the LiveWire 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.

