

# Introduction to Computer Forensics

**Course Duration:** 2 Days  
**CPE Hours:** 16 Hours  
**Level:** Beginner/Group-Live  
**Prerequisites:** None  
**Advanced Preparation:** None

This course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be demonstrated during this course, including software, hardware and specialized techniques. The need for businesses to become more efficient and integrated with one another, as well as the home user, has given way to a new type of criminal, the *cyber-criminal*. It is no longer a matter of, "Will your organization be compromised/hacked?" but rather, "When?" Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber-criminal, then this is the course for you.

## Who Should Attend:

This course is targeted towards auditors, system administrators, IT personnel, and all other security professionals requiring the knowledge and skills to track down and prosecute the perpetrator. This class is designed to increase the knowledge of participants of all levels.

## Seminar Outline:

### **I Introduction**

- Computer crime in the news

### **II Understanding Computer Forensics**

- What is computer forensics?
- Terminology
- How it applies to you
- Information warfare
- Hackers, crackers and cyber-terrorists
- Networking basics
  - Communications
  - Devices
- Identifying your vulnerabilities

### **III Tracking the Culprit**

- Need for thorough documentation
- What do you have to work with?
  - Written policies
  - Technical policies
  - Permissions
  - Billing statements
- System, application and device logs
- Monitoring suspects
  - Employer rights
  - Employee rights
  - Internet tracking
  - Email tracking
- Identifying a culprit's tracks and signature
- Creating a profile

### **IV Tools of the Trade**

- Software monitoring tools
  - O/S first
  - Key loggers
  - System trackers
- Software recovery tools
  - Data integrity
  - Recovery/search
  - Data wiping
- Software imaging tools
- Hardware monitoring tools
  - Cameras
  - Key loggers
  - Recording devices
- Password crackers
- Sniffers
- Encryption
- Intrusion detection tools

### **V Preserving Evidence**

- Securing the crime scene
- Backing up original data
  - Disk imaging
- Securing your data
  - Public/Private Key
  - Tokens
  - Permissions
  - Seals
- Validation/Authentication
  - Kerberos
  - Digital Certificates
  - Biometrics

### **VI Evidence Analysis**

- The many forms of digital evidence
- General guidelines for analyzing evidence
- What to look for
- Data classification
- Data reconstruction
- Need for cooperation of agencies and departments

### **VII Computer Forensics and the Law**

- Investigative procedures
  - Required search and seizure procedures
  - Your company's ethics
- Reconstructing the crime
- Computer fraud and abuse act
- Electronic communications and privacy act
- Case studies and cyber-crimes
- Presentation of evidence

### **VIII Checklists and Resources**

- Computer forensic checklists and resources
- Computer forensic resources