

Introduction to Computer Forensics

| | |
|------------------------------|---------------------|
| Course Duration: | 1 Day |
| CPE Hours: | 8 Hours |
| Level: | Beginner/Group-Live |
| Prerequisites: | None |
| Advanced Preparation: | None |

This course will give participants an introduction to the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Some of today's top tools and the basic methodologies and techniques of forensics will be discussed during this course. 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. This course is for individuals and organizations interested in an overview of the knowledge and skills needed to identify, track, and prosecute the cyber-criminal.

Who Should Attend:

This course is targeted towards auditors, system administrators, IT personnel, and all other security professionals and is designed to introduce attendees to the methodologies, techniques and tools of forensics.

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 and employee rights
 - Internet and 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 and system trackers
- Software recovery tools
 - Data integrity
 - Recovery/Search
 - Data wiping
- Software imaging tools
- Hardware monitoring tools
 - Cameras, key loggers and 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
 - Token
 - Permissions and 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