No Theories...

No Cramming...

No Boot Camps...

No Crash Courses...

No Certifications...

No Information Dumps...

No (Web-Based) Lectures...

Hands-On How-To® Computer Forensics Training

How-To Instructions

Real-World Simulations

Hands-On Exercises

Expert Instructors

Small Class Sizes

Tailored Courses

Updated Content

Arsenal of Security Take-Aways

Post-Training Support

Satisfaction Guaranteed

Course Overview:

Digital information continues to grow at an exponential rate. Data is no longer stored solely in computer hard drives, backup tapes, or compact discs (CDs). With the growth of emerging portable data and storage devices, such as portable digital assistants (PDAs), cell phones, and Blackberry devices, crucial information can be anywhere and easily passed from device-to-device. Information stored in these changing media can be crucial sources of evidence in corporate, civil, and criminal investigations.

Moreover, forensic investigation is a time-consuming effort that requires specialized expertise, procedures, tools, and real-world knowledge of excavating digital evidence. NetSecurity's Hands-On How-To® Computer Forensics course teaches students the step-by-step process of locating, acquiring, preserving, analyzing, and producing solid digital evidence. The Hands-On How-To Lab Exercises (HOHTLEs) covered in the course incorporate significant real-world experience necessary for delivering world -class results in the field.

NetSecurity Benefits:

Through years of real-world hands-on security and forensics experience, NetSecurity has supported Fortune 500 companies and federal agencies such as the IRS, DHS, VA, BBG, DOL, NSF, and DoD. The benefits of our Hands-On How-To Computer Forensics include:

- Skills to establish and fortify an organization's security, forensics, and incident response capabilities
- Customized private sessions, tailored towards organizations' unique environments
- Detailed step-by-step and how-to instructions
- Instructor-led and student-performed hands-on exercises
- Real-world simulations of forensics challenges
- Seasoned expert instructors with real-world hands-on consulting and training experience
- Arsenal of take-aways (tools, templates, guides, and relevant forensics resources)
- Up-to-date course content, addressing emerging forensics challenges
- Small class sizes ensuring maximum student-instructor interaction
- Vendor-neutral content – covering commercial and freeware tools

Target Audience:

The course is targeted towards technical professionals, including:

- Computer Forensics Investigators
- Law Enforcement Personnel
- Information Security Managers
- Incident Responders
- IT Professionals
- Cyber Crime Attorneys
- Private investigators
- Compliance Officers
- Auditors

Course Format:

- Interactive presentations by security and forensics expert instructor
- Hands-On How-To Lab Exercises (HOHTLEs) in performing computer forensics and incident response

Course Duration: Three (3) Days

Course Cost: **$2,995** (List Price)

Course Objectives:

Upon successful completion of the **Hands-On How-To® Computer Forensics** course, each participant will be armed with the knowledge, tools, and processes required in producing computer evidence that can withstand legal scrutiny. Specifically, students will possess relevant knowledge and real-world hands-on skills in:

- Requisite technology knowledge relevant to forensics investigations
- Laws relating to computer crime investigations
- Tried and proven forensics investigation processes
- Getting an organization ready for forensics investigations
- Forensics tools and techniques of the trade
- Evidence acquisition and duplication
- How-to analyze evidence for forensics artifacts
- Performing forensics analysis of common operating systems
- Internet forensics
- Analyzing Mobile device
- Passwords and encryption
- Information recovery
- Capturing volatile data from a live computer
- Conducting memory analysis
- Analyzing malware and conducting reverse engineering
- Developing forensics reports
- Testifying in courts
- Anti-Forensics techniques

Course Topics:

NetSecurity's Computer Forensics course includes in-depth coverage of real-world scenarios and HOHTLEs in the following areas:

• Topics	• Discussion and HOHTLEs
• **Computer Overview**	• Computer Fundamentals • Computer File Systems • Computer Hard Drive Structure • Hard Disk Interfaces (SCSI, IDE, USB, SATA, etc.) • Mobile Storage Devices • Windows, Linux, and Macintosh Boot Processes • Hard Drive Erasure and Degaussing • Virtualization and Virtual Machines (Parallels, VMware, etc.)
• **Networking Technology**	• Fundamentals of Networking • The Open System Interconnect (OSI) Model • The TCP/IP Model • TCP/IP Protocol Addressing
• **Forensics Overview**	• Computer Forensics Fundamentals • Benefits of Computer Forensics • Computer Crimes • Computer Evidence • Computer Forensics Evidence and Courts
• **Laws**	• Justice System • Legal Concerns and Privacy Issues • The Fourth Amendment • Internet Laws and Statutes
• **Forensics Process**	• The Forensics Process • Steps in Forensics Investigations • Authentication and Verification of Suspects • Identification of Evidence Source • Securing the Evidence • Chain of Custody Form • Professional and Unbiased Conduct • Law Enforcement Methodologies • Collaboration: Working with Upstream and Downstream Providers • Collaboration: Dealing with Law Enforcement • Collaboration: Dealing with the Media • Collaboration: Working With Other Organizations

• Topics	• Discussion and HOHTLEs
• **Forensics Evidence**	• Evidence Sources • Evidence Seizure • Evidence Collection: Duplication and Preservation • Evidence Collection: Verification and Authentication (Forensics Soundness) • Evidence Collection: Order of Volatility • Evidence Integrity: Preventing Tampering and Spoliation • Evidence Collection: Bagging, Tagging, Marking, Secure Storage and Transmittal of evidence. • Evidence Handling: Chain of Custody • Handling and Securing Evidence
• **Forensics Toolkits**	• Common Forensics Toolkits • Uncommon Forensics Tools • Creating Forensics Toolkits
• **Acquisition and Duplication**	• Sterilizing Evidence Media • Forensic Duplication of Source Evidence with Hardware • Acquiring Forensics Image with Software • Acquiring Live Volatile Data • Using Write blockers
• **Data Analysis**	• Metadata Extraction • File Signature Analysis • File System Analysis • Examining Unallocated and Slack Space • Identifying Known Bad/Good Files • Performing Searches • Data Carving • Recovering Deleted Data and Partitions
• **Windows Forensics**	• Registry Fundamentals and Analysis • Executable File Analysis • Windows Live Response • Alternate Data Stream (ADS) • Recycle Bin Forensics • Windows Prefetch Files • Evidence Recovery from Print and Spool Files • Simulating/Booting Suspect Environment

• Topics	• Discussion and HOHTLEs
• **Internet Forensics**	• Domain Name Ownership Investigation • Reconstructing Past Internet Activities and Events • Email Forensics: E-mail Analysis • Email Forensics: Email Headers and Spoofing • Email Forensics: Laws Against Email Crime • Messenger Forensics: AOL, Yahoo, MSN, and Chats • Browser Forensics: Analyzing Cache and Temporary Internet Files • Browser Forensics: Cookie Storage and Analysis • Browser Forensics: Web Browsing Activity Reconstruction
• **Mobile Device Forensics**	• Introduction to Handheld Forensics • Collecting and Analyzing Cell Phone, PDA, Blackberry, iPhone, iPod, and MP3 Evidence • Analyzing CD, DVD, Tape Drives, USB, Flash Memory, and other Storage Devices • Digital Camera Forensics • Reconstructing Users Activities • Recovering and Reconstructing Deleted Data
• **Passwords and Encryption**	• Files and Data Encryption • Password Attacks Tools and Techniques • Working with Rainbow Tables • Passwords and Storage Locations • Encryption Types (Symmetric and Asymmetric) • Password Cracking and Recovery
• **Steganography**	• Steganography Overview • Steganography Tools and Tricks • Data Hiding • Data Recovery
• **Volatile Data**	• Collection and Analysis on a Live Windows System • Collection and Analysis on a Live Linux System • Collection and Analysis on a Live Mac OS System • Collection and Analysis of Physical and Process Memory • Volatile Evidence in Incident Response • Court Admissibility of Volatile Evidence
• **Memory Forensics**	• Memory Fundamentals • Memory Data Collection and Examination • Extracting and Examining Processes

• Topics	• Discussion and HOHTLEs
• **Malware Analysis**	• Malware Analysis Basics • Analyzing Live Windows System for Malware • Analyzing Live Linux System for Malware • Analyzing Physical and Process Memory Dumps for Malware • Discovering and Extracting Malware from Windows Systems • Discovering and Extracting Malware from Linux Systems • Rootkits and Rootkit Detection and Recovery • Reverse Engineering Tools and Techniques
• **Forensics Resources**	• Forensics Forms and Checklists
• **Presentation and Reporting**	• Writing Computer Forensic Reports • Report Requirements • Guidelines for Writing Final Reports • Sample Forensic Report
• **Court Testimony**	• Credibility and Success in Court • Testifying in Court • Expert Witness: The Expert Witness • Expert Witness: Becoming an Expert Witness • Expert Witness Testimony • Evidence Admissibility
• **Anti-Forensics**	• Anti-Forensics Tools and Techniques (Data Hiding, Steganography, Encryption, Deletion of Data) • Defeating Anti-Forensic Schemes • Erasing Evidence

More information:

For more information about NetSecurity's Hands-On How-To® Training, please contact us at **Training@NetSecurity.com** or call **1-866-66-HOW-TO** (**1-866-664-6986**).