

j8FM6PmLNqq3ghDg0uCsM/Ach5ZVKZET7gURoaqTGzBZ8+T+8d2W538ke3c7t  
02jjdk1haMFCQHihQAEcWMCAQIZAQAKCRDafWsA0nHzRmAeAJ9yABw8v2fGxaq  
sKEu29e-DiscoverysdXRpb25zIDxsA0n8d2W5mpbmNoCyberCrimeTheorie  
0KLB RXF/j5jJQPxXaNUu/It1TQHSiyEumrHNSnn65aUMPnrbV0VJ8hV8NQvsUE  
/kVaWuF1XQDPXDa2ocjP/SmokingGunNo9CrammingJ75nx9AVfPQB8bLQ6mU  
h1cj43qMDok/76VekyCzsAAgIIANnG7yLbuEIllicitPornographyY2m5muB  
Y05Ag3qMDoVekyCzkv76No1BootnCampsoDcS7esD0a2ocj6/MDoku076Y05Ag  
71q1C Deleted/Hidden Files8wXo+VMR0U+028Wb5Szgg2gGnVqMUB9AVfP  
XaNUu/It1TQHSi7jb3HZNo2CrashhCourses0KLB RXF/j5jJQPxXaNUu/It1TQ  
vaWuF1XQDPXDa20a2ocj60a2ocHNetworkHackingd/P2NtVfX82jbTaqTCnM  
2GkHrAWEvidence Tampering G5p1YKTkd/P2 NoxCertificationshQAEcWM  
0k3jxInsiderTradingMDok/76Y05Ag aoebRXF/j5jJQPxXaNUu/It1TQHSi  
1q1C8wXo+VMR0U+02 GwG8Wb83M/Ac83M/Add25gIncidentResponse5Szgg  
h8+Q9 GwG5p1YKTkgNoe(Web-BasedLecture8FM6PmLNqq3ghDg0uCsM/Ach  
/xm+aYGg9 MDok/76Y05Asg Mobile Evidence0bLkwtu+SIfCtz7GTvf/wfEb  
Da7AYY9VaWuF1XQDPXDa2ocj6HDTtOpWG5p1YKTkd/P2NtVfWE5JqcYxX22azM



# Hands-On How-To® Computer Forensics Training for Attorneys

VaWuF1XQDPXDa2ocj6HDTtOpWG5p1YKTkd/P2NtVfX82jbTaqTCnMMa7AYhSIO  
2Gk/mjsBADfXnmZvQG51NSjJCqHNSnn65aQMRReal-World2SimulationsumrH  
gtypmICQ8mUAE5J2Ct1GainForensicsKnowledgeLG3fijkDwKzszmSGZcf  
dHkdHands-OnfExercisesgU29sdXRpb25zIDxpbmZvQG51dHNLmNvbT6JAFQE  
Uafn/QCjMTQHFQTB8EGBECAAwFAjD0sCx ExpertcInstructorszVxCAAwFAj  
haMFCQHihQAEcWMCDaScrutinizeDigitalEvidenceBADfXnmZvQG5652df  
HzRmAeAJ9QAKCRDfWsA0HzRmAeAJ9yABw8v2fGxaqJI9/VftBADfXnmZvQG51N  
gekyCTailoredcCourseszsAAgIIANnG7yLuELGDY2UpdatedzContent1FeI7  
1XQDPXDAKCRDAKCRDAKCCrossExamineExpertsSPIxNu 1j9WE5J2CtJ3k2  
deralbITjAudArsenalbofwBADfXnmZvQG51NSjs ZAQAKCRDafWsA0n0KLB RXI  
ZAQAKCRDafWsA0n0KLB RXF/j5securityMTake-AwaysV8NQvEGBEF9DG+zVx0E  
TGBKXipdQgtYwdXfSjxsZ0bybhCXHfV1HHVaJ01zBBADfXnmZv ZAQAKCRDafW  
CzsumtmAea2ocj6HDTtFBeForensicallySavvy9yABw8KCZAQAKCRDafWsA  
TrainingkSupport1haMFCQHihQAEQIZAQ ZAQAKCRDafWsA0n0KLB RXF/j5ha  
F CQHihQAEcWFQ hAKCRDafWDSbf2cDEq1VekyCzsAAgIIANnG7yLuELGDY2m5m  
QAE35yW2jj SatisfactiostjWinkYourCasearanteed1haMFCQHihQAEcWM  
dk1haMFCQHihQAEcWMCAQIZAQAKCRDafWsA0n0KLB RXF/j5jJQPxXaNUu/It1T  
HzRmAeAJ9yABw8v2fGxaqJI9/VftzM0KLB RXF/j5jJQPxXaNUu/It1TQHSiyE

## 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, cyber criminals are continuously crafting ways to evade existing forensics tools and techniques. NetSecurity's **Computer Forensics Training for Attorneys** course teaches legal professionals the process of locating, acquiring, preserving, analyzing, and producing solid digital evidence that can make the difference between winning and losing a case. The Hands-On How-To Lab Exercises (HOHTLEs) covered in the course incorporate significant real-world experiences necessary to prepare or scrutinize a forensics investigator.

## NetSecurity Benefits:

Through years of real-world hands-on security and forensics experience, NetSecurity has supported Fortune 500 companies, law firms, and federal agencies—such as the IRS, DHS, VA, BBG, DOL, NSF, and DoD. The benefits of our **Computer Forensics Training for Attorneys** include:

- Customized private sessions, tailored towards your unique requirements
- Instructor-led and student-performed hands-on exercises
- Seasoned security and forensics experts with
  - Real-world hands-on consulting and training experience
  - Media publication and industry speaking experience
- Arsenal of take-aways (guides and relevant forensics resources)
- Up-to-date course content, addressing emerging forensics topics
- Small class sizes ensuring maximum student-instructor interaction
- Vendor-neutral content

## Target Audience:

This course is targeted towards legal professionals, including Cyber Crime Attorneys, Paralegal Professionals, Magistrates/Judges, Private Investigators, and Compliance Officers

## Course Format:

- Interactive presentations by forensics expert
- Hands-On How-To Lab Exercises (HOHTLEs) in performing computer forensics

**Course Duration:** Two (2) Days

**Course Cost: \$1,695** (List Price)

## Course Objectives:

Upon successful completion of the **Computer Forensics Training for Attorneys** course, each participant will be armed with the required knowledge to understand and analyze computer evidence that can withstand legal scrutiny. Attendees will also learn to dissect evidence produced by opposing counsel. Specifically, attendees will possess relevant knowledge in:

- Tried and proven forensics investigation processes
- Evidence authentication, handling, preservation, and security
- Common mistakes to avoid in an investigation
- Preparing your own experts and scrutinize those of opposing expert teams
- Getting an organization ready for forensics investigations and e-discovery

## Course Topics:

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

Topics	Discussion and HOHTLEs
<b>Computer Overview</b>	Computer Fundamentals Computer Storage Media Mobile Storage Devices Computer Networks Computer Hacking Overview
<b>Forensics Overview</b>	Computer Forensics Fundamentals Benefits of Computer Forensics Computer Crimes Computer Forensics Evidence and the Courts Legal Concerns and Privacy Issues
<b>Forensics Process</b>	Forensics Investigation Process Securing the Evidence and Crime Scene Chain of Custody Law Enforcement Methodologies



**Hands-On How-To® Computer Forensics Training for Attorneys**  
Training Syllabus



Topics	Discussion and HOHTLEs
<b>Forensics Evidence</b>	Evidence Sources Evidence Duplication, Preservation, Handling, and Security Forensics Soundness Order of Volatility of Evidence Collection of Evidence on a Live System Court Admissibility of Volatile Evidence
<b>Forensics Readiness</b>	Benefits of Forensic Readiness Preparing an Organization for Forensics Investigations Managing an Investigation
<b>Forensics Lab</b>	Benefits of a Computer Forensics Lab Forensics Lab Requirements Securing the Forensics Lab
<b>Acquisition and Duplication</b>	Sterilizing Evidence Media Acquiring Forensics Images Acquiring Live Volatile Data
<b>Data Analysis</b>	Metadata Extraction File System Analysis Performing Searches Recovering Deleted, Encrypted, and Hidden files
<b>Internet Forensics</b>	Reconstructing Past Internet Activities and Events E-mail Analysis Messenger Analysis: AOL, Yahoo, MSN, and Chats
<b>Mobile Device Forensics</b>	Evidence in Cell Phone, PDA, Blackberry, iPhone, iPod, and MP3 Evidence in CD, DVD, Tape Drive, USB, Flash Memory, Digital Camera
<b>Court Testimony</b>	Testifying in Court Expert Witness Testimony Evidence Admissibility
<b>E-Discovery</b>	Federal Rules of Civil Procedure (FRCP) Collection and Preservation of Electronically Stored Information Legal and IT Requirements Developing Computer Investigation and E-Discovery Capabilities

**More information:**

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