Hands-On How-To® Forensics Training

Overview & Courses

Alumni's Accolades

"I found the NetSecurity's Malware Analysis training excellent and a potential benefit to CND personnel (your other classes sound good also)…It [the class] was rewarding and would help soldiers prepare for CEH and other CND certs…"
-- Major, Army National Guard

"I am looking forward to being able to attend more classes at NetSecurity and plan on bugging the heck out of my boss to let me!"
-- Forensics Investigator, GeoSpatial-Intelligence Agency

"The advertisement did not highlight how good the training really is… The instructor is truly an expert in the forensic field… I have attended over 20 training classes, but this is the first class where I have seen an instructor willing to stay long in class"
-- Victor Kalu, Department of Health and Human Services

"The course was all and more than I expected."

"This was my first course on computer forensics. It has been a tease on wanting to learn more."

"The lab exercises were a great way to apply the theory and the processes discussed in the presentation. They helped reinforce the information learned."

"[The Instructor's] level of knowledge and expertise was apparent and he was very helpful and patient during the exercises."

"I liked using the actual programs. [It] gave me a good understanding of what they do."

"A big plus I noticed [with the lab exercises] was instead of telling me what to look for in the tools, the questions focused more on '*What's wrong here?*'"
-- Elizabeth Hayes, Army National Guard

"He [the instructor] is very knowledgeable in the field"
-- Cyber Forensics Investigator, U.S. Army

"The labs helped to reinforce my learning so much…I am planning to have additional team member attend"
-- Manager of Incident Response, United States International Trade Commission

"This [course] should be the standard"
-- Malware Analyst, FBI

"This course was an excellent introduction for attorneys and private investigators to computer/cell phone forensics and a great refresher course for current computer examiners."

"All materials went hand in hand to gain a hands on understanding."

"The instructor was a great one to have. It is obvious that he enjoys this and that makes a better learning experience."

"The interaction between the students and teacher and [the use of] a lot of tools [is what I liked best about this course.]"

"This course has been very educational both in getting to use the latest tools and to interact with others in forensics."

"The instructors were very knowledgeable in computer science/forensics. [The] material was presented in 'easy to understand' format."

"[The Instructor] was extremely knowledgeable! Presentation very nicely designed and delivered. [The Instructor] was always open to questions and discussion."

Computer Forensics Challenges

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, smart phones, and handheld devices, vital information can be anywhere and easily passed from one device to another. Information stored in these changing media can be crucial sources of evidence in corporate, civil, and criminal investigations.

Moreover, today's cyber adversaries are highly skilled and sophisticated hackers who are either part of state-sponsored or organized crime. These elite attackers are so advanced that current security measures do not detect, let alone prevent their attacks. These criminals are paid and spend ample time conducting reconnaissance about their targets, then customizing their attack towards the victim. The firewall doesn't prevent the attack and the Intrusion Detection System (IDS) doesn't detect these intrusions. These cyber criminals continue to leverage users' susceptibility to social engineering attacks and vulnerable applications to infiltrate critical networks. Once inside the network, since there are no known signatures, the adversaries lay low on the radar while exfiltrating valuable network data.

Forensic investigation is a time-consuming effort that requires specialized expertise, procedures, tools, latest techniques, and real-world knowledge of excavating digital evidence. Moreover, hackers and cyber criminals are continuously crafting techniques to defeat current forensics and evidence discovery processes. NetSecurity's proprietary Hands-On How-To® computer forensics courses teach students the step-by-step process for locating, acquiring, preserving, analyzing, and producing solid digital evidence that can withstand legal scrutiny. Hands-On How-To Lab Exercises (HOHTLEs) covered in each 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 gained from supporting Fortune 500 companies and federal agencies such as the IRS, DHS, VA, BBG, DOL, NSF, and DoD, NetSecurity delivers the following benefits in our Hands-On How-To forensics training:

- Vendor-neutral course content, covering commercial and freeware tools
- Requisite skills to establish security, e-discovery, forensics, and incident response capabilities
- Customized private sessions, tailored towards students' unique challenges
- Detailed step-by-step and how-to instructions
- Instructor-led and student-performed Hands-On How-To Lab Exercises (HOHTLEs)
- 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 and techniques
- Small class sizes of 8-13 students ensuring high student-instructor ratio
- Free limited support from our instructors to answer questions relating to your investigation
- Enforcement of course prerequisites

Course Topics

NetSecurity's forensics courses cover emerging topics that pose the most challenge to forensics professionals, employing mechanisms for discovering hackers and anti-forensics techniques, and incorporating real-world scenarios and HOHTLEs. Depending on the course, students will possess relevant knowledge and real-world hands-on skills to investigate certain cases in the topics listed below:

Emerging Forensics Topics		Typical Cyber Crime Cases
• Advanced Persistent Threat (APT) • Zero-Day Attacks • Anti-Forensics • Passwords & Encryption • Events Reconstruction • Live Volatile Data • Network Forensics • Malware Analysis	• Memory Analysis • Reverse Engineering • Internet Events • Incident Response • Evidence Preservation • Registry Analysis • Unix/Mac Analysis • Mobile/Handheld devices • E-Discovery	• Intellectual Property Theft • Illicit Pornography • Deleted/Hidden Files • Malicious Software • Evidence Tampering • Network Hacking • Computer Misuse • Money Laundering • Insider Trading

Hands-On How-To® Course Listing

NetSecurity provides customized, hands-on training courses to accommodate your unique requirements.

Hands-On How-To® Computer Forensics (3 days; $2,995 Per Student)

Tailored towards existing forensics professionals, this vendor-neutral course covers emerging topics, challenging issues, and anti-forensics techniques, while leveraging the latest tools of the trade for solving real-world problems.

Hands-On How-To® Computer Forensics for Attorneys – CLE Credits (2 days; $1,995 Per Student)

This course teaches legal professionals the forensics process for locating, acquiring, preserving, analyzing, and producing solid digital evidence that can make the difference between winning and losing a case. We provide tips for selecting, preparing, and grilling expert witnesses. The course offers CLE credits.

Hands-On How-To® Hacking for Forensics Examiners (3 days; $2,995 Per Student)

To conduct a thorough investigation, forensic analysts need to know how a system intrusion is carried out by cyber criminals. This course provides the knowledge on how hackers break into systems as well as the mandatory skills needed for investigating systems or network compromises using tricks of the attackers.

Hands-On How-To® Electronic Discovery (e-Discovery) Training (2 days; $1,995 Per Student)

Learn how you can institute an e-discovery readiness plan to enable your organization to respond to litigation or regulatory investigation. Gain the knowledge you need to establish proven process for identifying, collecting, preserving, and producing electronic data to ensure that you comply with e-discovery requests promptly.

Hands-On How-To® Incident Response (3 days; $2,995 Per Student)

This course provides incident responders and forensic analysts the mandatory knowledge necessary to investigate zero-day attacks, security breaches, or perform other live investigations. Students learn how to establish incident response capabilities and prepare their organizations to carry out investigations.

Hands-On How-To® Malware Analysis (3 days; $2,995 Per Student)

The Malware Analysis course provides forensic analysts, incident responders, and malware analysts the skills needed to excavate and analyze malicious software, resulting from Advanced Persistent Threats, zero-day attacks, and other emerging intrusion techniques. Students learn how to dissect malware and formulate mitigation strategies for preventing future penetration.

Hands-On How-To® Malicious Document Analysis (1 day; $1,495 Per Student)

Cyber attackers now use malicious documents as an attack vector to bypass enterprise perimeter defensive measures and anti-virus solutions. This course teaches students how to analyze malicious Microsoft Office and Adobe PDF files for the presence of hidden malware. Course participants learn the tools and techniques for disassembling and reverse-engineering malicious documents, finding and extracting hidden codes, Shellcodes, JavaScripts, and VBA macros from an infected document.

Hands-On How-To® Memory Forensics (2 days; $1,995 Per Student)

This course teaches students about volatile data stored in memory, which are lost when the system is powered down. Course participants learn to pluck evidentiary information such as memory-resident malware, passwords/passphrases, Internet history, and other information running in memory. Upon memory acquisition, students learn about conducting analysis on a memory image and generating reports.

Hands-On How-To® Course Alumni Organizations

Many Federal, law enforcement, defense, and intelligence agencies; educational institutions; and commercial organizations send their security/forensics professionals to NetSecurity's Hands-On How-To® training courses. NetSecurity continues to be a reliable partner that satisfies real-world training needs of these organizations:

Department of Defense (DoD)	Sonnenschein, Nath & Rosenthal LLP
Internal Revenue Service (IRS)	Central Bank of Malaysia
U.S. Army	SAIC
Federal Bureau of investigation (FBI)	Booz Allen Hamilton
National Aeronautics and Space Administration (NASA)	Harris Corporation
Army National Guard	Northrop Grumman
Health and Human Services (HHS)	The Boeing Company
National GeoSpatial-Intelligence Agency (NGA)	Mitre
National Credit Union Administration	Avaya
United States International Trade Commission	The George Washington University
Department of Interior	BDO Seidman LLP
National Institute of Health (NIH)	Raytheon
Loudoun County Sheriff's Office	SRA, Inc.
U.S. Coast Guard	The George Washington University
Radio Free Asia	Tangible Software
Your Agency Here!	***Your Organization Here!***

Corporate Overview

Founded in 2004, NetSecurity Corporation provides vendor-neutral digital forensics, hands-on security consulting, and Hands-on How-To® training solutions that are **high-quality**, **timely**, and **customer-focused.** Through **NetSecurity Forensic Labs**, we deliver world-class forensics solutions that withstand the scrutiny of litigation. Armed with seasoned security and forensics experts with deep experience with real-world problems, NetSecurity delivers unparalleled forensics and security solutions to law firms, law enforcement, Fortune 500, and government entities. We help you reach your goals in engagements involving e-Discovery, digital forensics, incident response, R&D, ethical hacking, and **Hands-On How-To® Training**. As a private investigative firm, NetSecurity is one of a handful of companies that can legally conduct computer forensics investigations in Virginia.

Media Coverage

NetSecurity has received media coverage in prestigious media outlets, including:

SC MAGAZINE FOR IT SECURITY PROFESSIONALS	Forbes.com	CNBC
MarketWatch From DOWJONES	YAHOO! FINANCE	Securities Industry News
SECURE PC	NorthernVirginia MAGAZINE	Human Resource Executive Online

Course Registration

For registration information or to learn how NetSecurity can provide you with essential security and forensics knowledge necessary to deliver outstanding results in the field tomorrow, contact us at **training@netsecurity.com** or call **1-866-66-HOW-TO** (**1-866-664-6986**).

NetSecurity Forensic Labs
NetSecurity Corporation
22375 Broderick Drive
Suite 235
Dulles, VA 20166

SBA 8(a) Certified SDB

GSA Contract # GS-35F-0288Y

Phone: 703.444.9009
Toll Free: 1.866.66.HOW-TO
Fax: 703.444.6899
Email: training@netsecurity.com
Web: www.netsecurity.com