

j8FM6PmLNqq3ghDg0uCsM/Ach5ZVKZETT7gURoaqTGzBZ8+T+8d2W538ke3c7t
02jjdk1haMFCQHiHQAECwMCAQIZAQAkCRDafWsA0nHzRmAeAJ9yABw8v2fGxaq
sKEu29sdXRpb25zIDxpbmZNo9Theories...ofhiLz9E1xTHVQxBBOGknc1Ng
0KLB RXF/j5jJQPXxANUu/It1TQHSiyEumrHNSnn65aUMPnrBV0VJ8hV8NQvsUE
/kVaWuF1XQDPXDa2ocjPm/No9Cramming...J75nx9AVfPQB8bLQ6mUrfdMZIZ
MDok/7b VekyCzsAAgIIANnG7yLuELGDY2m5muBTfjTUcef4gi+ea/nptFB/Q1
Y05Ag 3q MDok VekyCzk/7b No1BootCamps...oDcS7esD0a2ocjb/ MDok/7bY
71q1C8wXo+VMR0U+028W65Szzg2gGnVqMUB9AVfPQB8bLQ6mUrfdMZIZJ+AyD
XANUu/It1TQHSi7jb3HZNo2CrashCourses...0KLB RXF/j5jJQPXxANUu/It
vaWuF1XQDPXDa2ocjbHDTtOpW65p1YKTkd/P2NtVfX82jbTaqTCnMMA7AYhSI0
2GkHrAWG5p1YKTkd/P2 NoxCertifications...hQAECwMCAQIZAQAkCRDafW
0k3jWApxxB+4VnVnsHitSj8+VMR0U+028W65Szzg2gGnVqMUB/mjsBADJCqQMX
3q MDok/7bY05Ag aoe3NoInformation/Dumps...G1rPBvUF7RC4kPVt73hk
1q1C8wXo+VMR0U+028W65Szzg2gGnVqMUB9AVfPQB8bLQ6mUrfdMZIZJ+AyDv
h8+Q09 GwG5p1YKTkgNo(Web-Based)qLectures...j8FM6PmLNqq3ghDg0u
/xm+aYGg9 MDok/7bY05Ag 0bLkwtu+SIfCtz7GTvf/wfEbGMtvzXdsWdAgZ2dS
Da7AYY9VaWuF1XQDPXDa2ocjbHDTtOpW65p1YKTkd/P2NtVfWE5JqcYxX22azM



Hands-On How-To® Incident Response Training

VaWuF1XQDPXDa2ocjbHDTtOpW65p1YKTkd/P2NtVfX82jbTaqTCnMMA7AYhSI0
2GkHrAcHow-ToInstructionsoPrGySbf2cDEq135yWnt9j+/bbf7kc0k3jWA
/mjsBADfXnmZvQG51NSjJCqHNSnn65aQMReal-World2SimulationsumrHNSr
gtypmICQ8mUA7LG3fi jK0wKzszmSGZcfsCGbpnqwfXLuh7gSpLQsTmV0U2VjdX
dHkdHands-OnExercisesgU29sdXRpb25zIDxpbmZvQG51dHNLmNvbT6JAFQ
Uafn/QCjMTQHFQTB8EGBECAAwFAjD0sCx ExpertInstructorszVxCAAwFAj
haMFCQHiHQAECwMCAQIZAQAkCRDafWsA0nHzRmAeAJ9yABw8v2fGxaqJI9/Vft
02jjdk1haMFCQHiFsxSmallClassSizesIZAQAkCRDfWsA0HzRmAeAJ9yABw
q3ghDg0uCsM/ 1xitVjLhd&NMD/XwXVD0jHRhs3jMTQHSiyEumrHNSnn65aUMh
VekyCTailoredCourseszsaAgIIANnG7yLuELGDY2UpdatedzContent1FeI7
1XQDPXDa2ocjbHDTt fFstjvbyzSPIxNu 1j9WE5J2CtJ3k2gpXI61Brwv0YAWC
deralbITjAudArsenalofwSecurityMTake-AwaysV8NQvEGBEF90G+zVx0Eh
Aj0uCsM/Ach5ZVKZETT7gURoaqTG8KXipdQgtYWdXfSjxsZ0bybhCXHfV1HHVa
CzsumtmAeAJ9yABw8KCRDafWsA0v2f2x1Post-TrainingkSupport1haMFCQH
F CQHiHQAECwFQ hAKCRDafWDSbf2cDEq1VekyCzsAAgIIANnG7yLuELGDY2m5m
QAE35yW2jj SatisfactionGuaranteed1haMFCQHiHQAECwMCAQIZAQAkCRD
dk1haMFCQHiHQAECwMCAQIZAQAkCRDafWsA0n0KLB RXF/j5jJQPXxANUu/It1T
HzRmAeAJ9yABw8v2fGxaqJI9/VftzM0KLB RXF/j5jJQPXxANUu/It1TQHSiyE

Real-World Scenario:

Ojehtrade & Co., Inc., a multi-billion dollar brokerage firm with \$789 billion in assets, based in New York, NY, with offices throughout the USA has recently suffered a massive computer intrusion. The target systems involved are running on Unix, Windows, and Mac OS X systems. Ojehtrade knew about this intrusion because the cyber criminals sent a message to the firm's executives demanding \$5 million dollars in "ransom" and have threatened to contact the media and publish the compromised data online if their demands aren't met within 72 hours.

Ojehtrade is surprised, given the heavy investment in corporate IT security measures, that they were hacked. Your firm, The Forensics Gurus LLC, has been hired by Turner Worten Fitzgerald LLP, a prestigious law firm representing Ojehtrade to handle this high-profile investigation at a bill rate of \$450/hr. As the senior incident responder, you have been asked to interrupt your long-scheduled Mediterranean cruise to lead this high-profile incident response engagement. The client wants to know:

- What, if any, is the extent of the damage/compromise?
- What data has been lost or compromised?
- Where did the hacker(s) come from?
- What is the timeline of the hacking activities?
- What can be done to prevent intrusions in the future?

Incident Response is a time-consuming effort that requires specialized expertise, procedures, tools, and real-world investigative skills. NetSecurity's Hands-On How-To® Incident Response 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 legally admissible world-class results in the field.

NetSecurity Benefits:

Through years of real-world hands-on cyber security, digital forensics, and incident response 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® Incident Response course 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 investigating a compromised network
- 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 incident response challenges
- Small class sizes ensuring maximum student-instructor interaction
- Vendor-neutral content, covering commercial and freeware tools

Target Audience:

The Incident Response course is targeted towards technical professionals, including:

- Computer Forensics Investigators
- Incident Responders
- Malware Analysts
- Law Enforcement Personnel
- Information Security Professionals
- Compliance Officers
- Auditors

Course Format:

- Interactive presentations by security, forensics, and incident response expert instructor
- Hands-On How-To® Lab Exercises performing computer forensics and incident response

Course Duration: Three (3) Days

Course Cost: \$2,995

Course Objectives:

Upon successful completion of the **Hands-On How-To® Incident Response** course, each participant will be armed with the knowledge, tools, and processes required in conducting incident response and producing reports that withstand legal scrutiny. Specifically, students will possess relevant knowledge and real-world hands-on skills in:

- Incident Response Process
- Legal Considerations
- Evidence Collection
- Evidence Preservation
- Preparing Incident Response Tools
- Hackers' Methods of Maintaining Presence (Persistence Methods)
- System Compromise Indicators (Quickly Detecting and Confirming Intrusions)
- Advanced Malware
- Malware Analysis
- Building an Incident Response Tool Suite
- Windows Registry Analysis
- Forensics

Course Topics:

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

Topics	Discussion and HOHTLEs
Incident Response Process	<ul style="list-style-type: none"> • Preparation • Incident Readiness Planning • Identification • Containment • Eradication • Recovery • Lessons Learned
Legal Considerations	<ul style="list-style-type: none"> • Internet Laws and Statutes • Legal Concerns and Privacy Issues • Court Admissibility of (Volatile) Evidence
Evidence Collection	<ul style="list-style-type: none"> • Volatile Data Collection <ul style="list-style-type: none"> ○ Pros and Cons of System Shutdown ○ Order of Volatility (Memory, Process, Network, Registry) • Hard Drive Imaging <ul style="list-style-type: none"> ○ Physical Image ○ Logical Image ○ Full/Partial Drive Encryption Scenarios • Documenting the Cyber Crime Scene • Collecting Additional Storage Devices, Sticky Notes, etc.
Evidence Preservation	<ul style="list-style-type: none"> • Securing the Evidence • Chain of Custody
Preparing Incident Response Tools	<ul style="list-style-type: none"> • Statically Linked Binaries • Import Library • Incident Response Tools Selection
Hackers' Methods of Maintaining Presence (Persistence Methods)	<ul style="list-style-type: none"> • Surviving Reboots • Autoruns • Services • Service Host Services • Stubpath • Scheduled Tasks • Windows Firewall

Topics	Discussion and HOHTLEs
System Compromise Indicators (Quickly Detecting and Confirming Intrusions)	<ul style="list-style-type: none"> • Firewall, IDS, etc. • Temporary Internet Files • Anti-Virus Logs • Hosts File • DNS Cache • Running Services • Critical Log Files • Network Connections • Memory • Recycled Bin • Hidden and Protected Files
Advanced Malware	<ul style="list-style-type: none"> • Memory-Resident Malware • Memory Imaging Tools/Techniques • Memory Analysis Tools
Malware Analysis	<ul style="list-style-type: none"> • Malware Analysis • Static Analysis • Dynamic Analysis
Building Incident Response Tool Suite	<ul style="list-style-type: none"> • Building Trusted Toolkits • Testing the Tools
Windows Registry Analysis	<ul style="list-style-type: none"> • Monitoring Registry Changes • System Information • Users Activities • Autostart Locations
Forensics	<ul style="list-style-type: none"> • Time line Analysis • File Signature Analysis • Hash Analysis

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)**.