No Theories...

No Cramming...

No Boot Camps...

No Crash Courses...

No Certifications...

No Information Dumps...

No (Web-Based) Lectures...

Hands-On How-To® Memory 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

Real-World Scenario:

A prominent Government agency has suffered a massive cyber intrusion. The intrusion appears to be a highly sophisticated attack launched by highly skilled hackers who are part of a state-sponsored cyber crime. These "elite" hackers launched a successful and advanced attack that went undetected and unprevented by the agency's current perimeter security measures. Once these attackers penetrated the network, they flew below the radar and went undetected for months while pilfering vital data.

Your firm has been recruited to assist in the investigation. When your team arrives at the cyber crime scene, you notice that some of the compromised systems have been powered down while others are still up and running. Preliminary analysis of the running systems yields no trace of the intrusion on the file systems. Your last resort is to collect volatile data, including memory images of each penetrated system, for later analysis.

Memory forensics analysis is a branch of computer investigation that requires special expertise in excavating relevant artifacts from memory. NetSecurity's Hands-On How-To® Memory Forensics 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 critical information running in memory. Upon memory acquisition, students learn how to conduct analysis on memory images and generating reports. 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® Memory Forensics 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 malicious software in a lab environment
- 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 malware analysis challenges
- Small class sizes ensuring maximum student-instructor interaction
- Vendor-neutral content, covering commercial and freeware tools

Target Audience:

The Memory Forensics course is targeted towards technical professionals, including:

- Computer Forensics Investigators
- Incident Responders
- Malware Analysts
- Information Security Professionals
- Technology Enthusiasts

Course Format:

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

Course Duration: Two (2) Days

Course Cost: **$1,995**

Course Objectives:

Upon successful completion of the **Hands-On How-To® Memory Forensics** course, each participant will learn about volatile data stored in memory, which are lost when the system is powered down. Course participants also learn how to extract 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 memory images and generating reports. Students will be armed with the knowledge, tools, and processes required in conducting memory forensics and producing a report that can withstand legal scrutiny. Specifically, students will possess relevant knowledge and real-world hands-on skills in:

- Introduction to Memory Forensics
- Memory Acquisition
- Volatility for RAM Analysis
- File Carving
- Fuzzy Hashing
- Analysis of Extracted Malware Specimen

Course Topics:

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

Topics	Discussion and HOHTLEs
Introduction to Memory Forensics	• What is in RAM? • Why Physical Memory Analysis • Identify Malicious Property • Memory Analysis Challenges • Memory Analysis Tools
Memory Acquisition	• Acquiring the RAM, Hibernation Files, Page/Swap Files • Acquisition Tools (Winen, FastDump, FTK Imager, MDD, etc.) • Remote Acquisition
Volatility for RAM Analysis	• Memory Analysis with Volatility • Virtual Address Descriptors (VAD) tree • Volatility Modules • Volatility Plug-ins • Network Connections, Loaded DLLs, Open Files, • Extracting Process Memory, EXEs, and DLLs from RAM • Recovering Passphrases and Encryption Keys • Analyzing RAM for Malware
File Carving	• File Extraction using Scapel, Foremost, FTK, and other File Carving Tools
Fuzzy Hashing	• MD5 Hash • Fuzzy Hashing • File Matching • Malware-Injected Processes
Analysis of Extracted Malware Specimen	• Static • Dynamic Analysis • Code 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**).