EnCase® v6 Field Intelligence Model Network Forensics

Day 1

Day one provides an understanding of the EnCase® Field Intelligence Model (FIM). Using FIM students will learn how FIM and the SAFE work. Students will learn the basic concepts of cryptology, TCP / IP technology and servlet methodology and installation. Students will complete the FIM SAFE setup and deploy FIM to preview and acquire a remote machine. Students will learn how to troubleshoot any problems.

The activities of day one include:

- **The overview of FIM, consisting of a high-level, thorough review of EnCase® Enterprise (Enterprise) and FIM and the differences between the two**
- **Introduction to cryptology, preparing the students for the encryption concepts built into FIM**
  - Understanding and processing volatile data
- **Installing and building the FIM and Secure Authentication for EnCase® (SAFE)**
  - Understanding and processing volatile data
- **TCP/IP overview, explaining the relevance of TPC/IP to FIM including**
  - TCP/IP protocols and how those protocols are bundled into a TCP/IP stack
  - How data flows through the TCP/IP protocol stack
  - The functionality of the core protocols
- **Illustration of how FIM meets the NIST requirements for incident response and computer forensics, including real-world scenarios of how FIM is being used**
- **Configuration of the SAFE network**
- **SAFE administration, including creating an investigator account and establishing permissions for the account on the SAFE**
- **A comprehensive review of all trouble shooting techniques needed during a FIM deployment**
- **Previewing and acquiring a remote machine**

Day 2

Day two begins with a review and quiz to reinforce the knowledge gained during day one. Preview and acquisition activities will continue from day one, and the students will be given an in-depth understanding of the basic structure of the EnCase® interface within FIM. The students will also gain hands-on experience using FIM in a variety of situations. They will deploy their servlet, preview and then acquire live evidence on a software RAID, using port forwarding and through a firewall. The instruction for the day will conclude with the students deploying FIM from a secure machine in a public place.

The instruction covered during day two includes:

- **Detailed discussion of EnCase® concepts and FIM**
  - The structure of evidence files, including the file header, data blocks and MD5 hash
- **Introduction to VMware FIM deployment**
  - Familiarizing students with the set up and use of virtual machines as FIM target machines
  - Building a virtual network in which to deploy FIM
  - Building a Red Hat Linux virtual machine
- **Previewing a RAID5 configured in either a software or hardware array with FIM**
  - Understanding Microsoft® Internet Information Services (IIS) and how its popularity may play a role in vulnerability
- **Port forwarding, firewall and networking essentials**
  - Understanding how networking essentials like routers, DHCP servers and firewalls work, how to administer them and how to let the EnStart service pass through them
  - Students will administer the router and firewall and connect to a target machine from a public IP to a private IP
- **Deploying FIM to ultimately reverse port forward traffic from a target machine protected by a firewall or behind a router**

Guidance® SOFTWARE
The World Leader in Digital Investigations™

Day 3

The activities on day three begin with a review and quiz to reinforce the course information so far followed by a practical exercise on troubleshooting FIM. When the day's instruction begins, the students will build on the skills previously learned by capturing and inspecting FIM TCP packets and confirming that encryption is in use. Using FIM the students will conduct an examination of the Windows® registries. A bootable CD will be created and used to deploy the FIM servlet on a Windows machine without using user credentials or having administrator access. The students will learn how to use FIM to obtain a snapshot of volatile data and discover hidden processes and root kits. Additionally the students will learn about encrypted volumes and how FIM can be used to image a mounted encrypted volume.

The activities of day three include:

- **Understanding ports**
  - An explanation of the role of ports and sockets in network communication and understanding the difference between port types
  - Becoming familiar with well-known ports and services as well as the concept of firewalls
  - The use of packet sniffing software to capture all packets associated with a FIM deployment
- **Examining both an online and offline Windows registry with FIM**
- **Deploying the servlet without credentials**
- **Understanding what makes up volatile data and how it is captured using EnCase® Snapshot**
- **Understanding the nature of encrypted volumes and how to examine the data**

Day 4

Day four's activities continue the examinations of Windows rootkits. The activities on day four begin with creating logical evidence files from single files. Next the students will learn to deploy the Linux servlet, examine live Linux systems and learn advanced servlet pushing technologies. Students will learn how to combine all discoveries into a readable, coherent report. They will also perform a final practical exercise within the given scenario to summarize the week's instruction.

The instruction covered during day four includes:

- **Adding single files to cases, creating logical evidence files from them and understanding the differences**
- **Examining a Linux system by using FIM**
- **How the Metasploit framework can be used to compromise a system**
- **Performing advanced servlet pushing technologies by using a live machine**
- **Using the EnCase interface to prepare written reports and exporting the reports in HTML or other formats**

Guidance® Software
The World Leader in Digital Investigations™

Guidance Software, Inc. is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE sponsors, 150 Fourth Avenue North, Nashville, TN, 37219-2417. Web site: www.nasba.org

About Guidance Software (GUID)
Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 30,000 licensed users of the EnCase technology worldwide, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from *eWEEK, SC Magazine, Network Computing*, and the *Socha-Gelbmann survey*. For more information about Guidance Software, visit www.guidancesoftware.com.