

# EnCase® Computer Forensics II Syllabus

## Day 1

Day one starts with a brief review of working within the EnCase® Forensic v6 environment. Attendees then move on to study the Master Boot Record partitioning model, partition recovery, FAT folder structure, NTFS and FAT folder recovery. Instruction is then provided on the use of the EnCase® Virtual File System (VFS) Module and the EnCase® Physical Disk Emulator (PDE) Module. The attendees are shown how to use these technologies to accomplish tasks outside of the EnCase Forensic environment such as virus scanning and rebuilding the target operating system within a VMware environment. Day one finishes with intermediate-level instruction concerning NTFS and its most important metafile, the Master File Table (MFT).

### *The main areas covered on Day 1 include:*

- **Review of EnCase Forensic case creation and adding evidence**
- **Understanding the Master Boot Record partitioning scheme**
- **Principles of attempting to recover data lost through the partitioning or formatting process**
  - Partition recovery
  - Folder recovery
- **Using the EnCase Virtual File System (VFS) Module**
  - External processing
    - » Virus scanning
    - » Dynamic mounting of compound files
- **Single files**
- **Logical evidence files**
- **Using the EnCase Physical Disk Emulator (PDE) Module**
  - Running a target system within a virtual environment
- **Introduction to NTFS**
  - Internal system files and their function
  - \$MFT entries and contained attributes
  - Resident file data
  - Nonresident file data
  - Impact of file deletion

## Day 2

Day two begins with an examination of compound files. Their structures are explored and issues surrounding their examination are discussed in detail. Students move on to exploring a very important type of compound file structure, the Windows Registry hive file. They explore mounting and examining these files and are given instruction on the relationship of the hive files to the structure of the Registry in its on-line state. They then progress to examining the time zone information contained within the Registry, its importance to their case and how they apply it in EnCase Forensic. They then move on to using GREP and text-indexing functionality of EnCase Forensic in order to perform advanced searches. Day two concludes with instruction on how to use EnCase Forensic conditions and queries to filter in information of interest and filter out common data that is of no relevance to the investigation.

### *The main areas covered on Day 2 include:*

- **Compound files**
  - Mounting and searching of compound files
  - Documenting data contained within these compound files
  - Pitfalls of not examining compound files properly
- **Windows Registry**
  - Elements of the Rregistry
    - » Registry keys (folders) and values
    - » Registry value types
  - Locating and mounting the Registry hive files
  - Examination of time zone settings with the Registry
    - » Applying time zones within EnCase Forensic
- **Advanced search techniques**
  - Using the GREP operators within EnCase Forensic to construct advanced search terms
  - Suitability of GREP, proper syntax and potential results
- **Conditions and queries**
  - Uses
  - Creating an index
  - Querying an index

### Day 3

Day three focuses upon specific analysis of common artifacts that often provide vital information to investigations. These specific areas reveal data that can provide a clearer indication of user activities.

We will examine specific artifacts that the operating system creates through the user's interaction with the computer. Students will explore the methods that EnCase Forensic provides to examine common email files, Internet history and cache content, Internet bookmarks, print artifacts, as well as the function and content of the Windows Recycle Bin.

#### **The main areas covered on Day 3 include:**

- **Windows artifacts**
  - User account information and associated data
  - System folders and files of interest
  - Thumbnail cache files
  - Windows restore points
  - Vista-specific artifacts
    - » Folder structure and the effect of junctions (folder mount-points)
    - » User/administrator privileges and impact on storage of data
    - » Public folders
    - » Virtualized folders
    - » Impact of the 'Previous Versions' feature
    - » Windows search indexing artifacts
    - » The Windows 'Photo Gallery'
    - » The Windows 'Contact Manager'
    - » System performance and security enhancements
- **Link files**
  - Deconstructing link files to reveal internal structures relating to their target files
- **Email and Internet history**
  - Examining both client-based and web-based email and methods available within EnCase Forensic to locate and parse email data stores
  - Recovering and analyzing email attachments
  - Exploring the results of activity on the Internet, including cookies, history, web cache and bookmark data

- **Print spooler recovery**
  - Understanding the printing process and associated files
  - Recovery of SPL and SHD files as well as understanding and extracting the graphical and metadata they contain

- **The Windows Recycle Bin**
  - Examination of the Recycle Bin, its properties and function
  - Understanding and parsing the Recycle Bin INFO2 index file; searching for Recycle Bin INFO2 entries
  - Exploring the way the Recycle Bin is implemented under Windows Vista
  - Linking Recycle Bin data to the associated user
  - Registry entries controlling operation of the Recycle Bin

### Day 4

Day four starts with instruction on the recovery and preservation of data from memory sticks, compact flash, XD cards and similar media. A review of the week's work will reveal a significant volume of data within the class case folders. Students will explore methods to document, organize and prepare a professional, accurate and articulate final report.

#### **The main areas covered on Day 4 include:**

The reports will be exported in both RTF and HTM formats to allow students to see the advantages of each format.

- **Examination methods concerning flash cards & similar devices**
  - Identification, recovery and documentation of metadata associated with digital camera media
- **Reporting**
  - Using the data accumulated during the week's work, students will explore various methods to document, organize and prepare professional reports for their agencies
  - Students will export their reports in both RTF and HTM formats and compare the results, allowing them to select the format that best meets the needs of their respective agency
  - Students will be shown how to export all of the metadata relating to the files and folders in their case and the best way to store, present and query this data



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](http://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 27,000 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](http://www.guidancesoftware.com).

©2008 Guidance Software, Inc. All Rights Reserved. EnCase and Guidance Software are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners.