

# EnCase® Computer Forensics I Syllabus

## Day 1

Day one starts with an introduction to EnCase® Forensic v6 and examination methodology. Attendees are shown how to use EnCase Forensic to acquire a complete copy of the data from a removable disk in a forensically sound manner. The concept of digital evidence and how computers work (paying particular regard to the associated impact on forensic examination) are also included.

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

- **EnCase Forensic methodology**
  - Creating an EnCase Forensic case file
- **Navigating within the EnCase Forensic environment**
- **EnCase Forensic concepts**
  - Safeguarding and preserving evidential data
- **Understanding the concept of digital evidence and its impact on an investigation**
- **The basics of acquiring a forensically sound copy of data from a removable disk**
- **Understanding how computers work**
  - Hardware and associated terminology
  - The CMOS, BIOS and boot sequence
  - Interpreting binary and hexadecimal data
  - The basics of text encoding

## Day 2

Day two expands upon the information provided in day one, and begins with a detailed discussion of the FAT file systems as well as an overview of the NT file system. Hard disk acquisition is covered, using both a forensically sound Linux CD, as well as the use of a hardware write-blocking device. Attendees will learn how to properly preview a computer system prior to acquisition as well as explore keyword searching and bookmarking of relevant data.

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

- **NT/FAT File Systems**
  - How these file systems track data on their respective volumes as well as what occurs when a file is created as well as deleted
- **Acquisition of a hard disk**
  - Write-blocking technologies
  - Acquisition using a forensically sound Linux operating system
    - » Drive-to-drive acquisition
    - » Network crossover-cable acquisition
  - Previewing computer systems
  - Creation of keywords and searching
  - Basic bookmarking

### Day 3

Day three includes more complex bookmarking of data. Instruction is given on the use of file signatures to properly identify file types. The principal and practical usage of digital fingerprints (hash value) to identify files of interest and exclude known files is also covered. Attendees will install external viewers within EnCase Forensic and learn how to copy data from within an evidence file. Restoring an evidence file back to physical media is also covered.

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

- **File types**
  - Discussion of the categories of files/folders and the icons employed by EnCase Forensic
- **Reviewing search hits and bookmarking**
  - A more detailed discussion of bookmarking and related options
- **Signature analysis**
  - An automated comparison of the displayed file extension with the actual content of the file
- **Hash analysis**
  - Using digital signatures to identify/exclude files without visually examining each one
- **Installing external viewers**
- **Detailed copy/UnErase options**
- **Restoring evidence**
  - Often required by court order; necessary to recover data and/or examine the operation of the host system in real-time

### Day 4

Day four explores how to reacquire evidence in order to modify evidence-file parameters but still maintain data integrity. Attendees are given advice and guidance for archiving as well as instruction on how to restore and open an archived case. Attendees will observe first hand how EnCase Forensic can detect and identify any changes to the content of an evidence file. Practical instruction will then be given concerning the use of the Timeline viewer within EnCase Forensic and the recovery of deleted data from the unallocated space of a computer disk. Following this the importance of proper evidence handling will be discussed with the attendees being shown examples of good practice in this area.

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

- **Archiving and reopening an archived case**
- **Verification of an evidence file**
- **Timeline view**
- **Location and recovery of evidence in unallocated space**
  - Manually
  - Using EnScript® programs
- **The importance and practicalities of evidence handling**



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.