

### DAY 1

#### EnCase Concepts

- Case File
- Evidence File
- Case File Backup
- Configuration Files

#### What Constitutes Digital Evidence

- Computers as an instrumentality of the crime
- Computers as a repository of evidence
- Examples of mediums of storing digital evidence

#### How Computers Work

- Power-up Sequence
  - BIOS
  - POST
  - Etc...
- Bits/Bytes/Hex/Binary

#### EnCase Navigation

#### Diskette Preview/Acquisition

- Create Case
- Options

Day one provides an understanding of the proper handling of digital evidence from seizure to acquisition. Students receive a basic overview of how computers function, as well as what constitutes digital evidence.

### DAY 2

#### NTFS/FAT File Systems

- How these file systems track data
- What happens when a file is created
- What happens when a file is deleted

#### Creating a Boot Disk

- Why a forensically sound boot disk is needed
- Components of a forensically sound boot disk

#### Hard Drive Preview and Acquisitions

- Physical disk versus logical drive
- Fastbloc
- DOS based via disk to disk
- DOS based via crossover cable

#### Creation of Keywords and Searching

- Global versus Case Specific
- Selecting Keywords
- Selecting where/what to search
- Viewing results

#### Bookmarking/Preserving Findings

- Highlighting sections of data
- Pointing to file(s)

Day two begins with a 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 boot diskette, as well as 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.



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)

## DAY 3

### ■ File Types

→ Icons/Description column

### ■ Bookmarking Techniques

→ Pointing to file(s)

→ Comments

→ Organizing Report

### ■ Signature Analysis

→ Search Button

→ All or Selected

→ Compares Extension to Header

→ Interpreting results

### ■ Installing External Viewers

→ Link Application to EnCase

→ Can link file extensions to Application

### ■ Copy/Unerase Options

### ■ Restoring Evidence

### ■ Reacquiring an Evidence File

→ Don't need original hardware to change options

→ Quick Reacquisition

Day three includes more complex bookmarking of data, and examination of file signatures to accurately identify file types. Attendees will install external viewers within EnCase and learn how to copy data from within an evidence file. Students learn how to restore an evidence file back to physical media and reacquire an evidence file with different options.

## DAY 4

### ■ Archiving/Reopening an Archived Case

→ What to archive

→ Specify path to EnCase of Evidence file to reopen case

### ■ Verification of Evidence File

→ Change 1 bit; EnCase detects change

→ Manually re-verify at any time

### ■ Timeline

→ Define four Date/Time stamps

### ■ Windows Artifacts

→ User Accounts

→ Recently Accessed Files

→ Internet Cache

→ Desktop/My Documents

### ■ Searching Unallocated Space

→ Use file header for image

→ Display image

Day four explores how to archive a completed case, as well as how to reopen this case if needed in the future. Attendees will observe how EnCase can detect and identify any changes to the content of an evidence file, as well as take a detailed look at the Timeline view within EnCase. Pertinent areas of interest within the Windows operating system and user accounts are explored as well as locating data in unallocated space.