GUIDANCE SOFTWARE

ENCASE COMPUTER FORENSICS I

Syllabus

Day 1

Day one starts with instruction on using EnCase® Forensic version 7 (EnCase) to create a new case and navigate within the EnCase interface. The students participate in a practical exercise, which allows them to test their newly acquired navigation skills and understanding of searching for files based on metadata. Attendees use EnCase to acquire a forensic copy of media while protecting the original media from change. Methodologies used within a computer system for the allocation of storage areas are discussed. The concepts of digital evidence and how to validate evidence verification are also discussed.

The main areas covered on day one include:

- Creating a case file in EnCase
- Navigating within the EnCase environment
- Understanding concepts of digital evidence and disk/volume allocation
    - » Types of evidence
    - » Terminology describing data storage, including but not limited to unallocated space, unused disk area, volume slack, file slack, RAM slack and Disk slack
- Documenting EnCase concepts
    - » Evidence files
    - » Case Files and backups
    - » Configuration files
    - » Object icons within EnCase
- Acquiring media in a forensically sound manner

Day 2

Day two begins with a continuation of the acquisition concepts lesson, which is followed by a quiz, which reviews presented concepts. The students learn how to properly preview a live computer system, prior to acquisition, using the Direct Network Preview function. The attendees utilize the EnCase® Evidence Processor to run modules on evidence files to obtain results that are reviewed during subsequent lessons. Attendees bookmark and tag data to be incorporated into an examination report during the Report Creation lesson. Students perform a practical exercise during which they backup the case with customized settings, and bookmark items for reporting purposes. Participants then run two different searching processes, raw searching (on raw data, indexed or not) and index searching (on interpreted, indexed data).

The main areas covered on day two include:

- Using the Direct Network Preview function to preview a live running computer, perhaps one that is employing full disk encryption
- Running other EnCase utilities to capture RAM and to image a live running computer
- Processing evidence
    - » Using the Evidence Processor
    - » Managing and using the various Evidence Processor settings and toolbars
    - » Modules
- Bookmarking and tagging search results for reporting purposes
- Creating and conducting raw keyword searches and index search queries to locate keywords of interest

Day 3

Day three begins with the completion of the index searching lesson. The participants perform a practical exercise, allowing them to practice the discussed searching and bookmarking techniques. Attendees define and install external viewers within EnCase and copy data from within an evidence file to the file system for use with other computer programs. Participants employ the use of file signature analysis to properly identify file types and to locate renamed files. Students are then provided instruction on the principal and practical usage of Hash Analysis. Students create a hash library, containing hash sets and hash values of notable files to identify, and known files to exclude from an evidence file. Hash Analysis tools, such as EnScript® programs and other utilities, are then employed to analyze hash libraries and to incorporate commonly available hash libraries/sets into the examination environment. Entropy analysis techniques are demonstrated to students to assist in the identification of files that nearly match notable files.

The main areas covered on day three include:

- Creating and conducting index search queries and raw keyword searches
- Incorporating the use of installed external viewers used by examiners into EnCase
- Copying files, folders, and data from EnCase to the local file system for analysis by other tools
- Performing signature analysis to determine the true identities of file objects and to ascertain if files were renamed to hide their true identities
- Conducting hash analysis using unique values calculated based on file logical content to identify and/or exclude files
- Running entropy analysis to locate files that may be near matches to other files or that may be password protected, obfuscated, or encrypted.

Day 4

Day four begins with a practical exercise on conducting signature, entropy, and hash analyses. The day's instruction begins with a lesson on searching and recovering data from unallocated space. The students then discover how to customize and organize a report using bookmarked data and how to include pertinent file metadata in the report. The students are given advice and guidance in properly archiving and later reopening a case. During the archiving process, attendees use procedures to reacquire an evidence file to change evidence file parameters, such as compression or evidence file format or segment size to facilitate effective archiving. The course concludes with a final practical exercise on the week's instruction.

The main areas covered on day four include:

- Locating and recovering evidence, including images, documents, and videos in unallocated space manually and by using EnScript programs
- Creating a report of files and data bookmarked during the examination
  - » Exporting reports
  - » Modifying basic reporting formats
- Reacquiring evidence to change evidence file settings
- Restore evidence to run proprietary software or as required by a court order
- Archiving and reopening an archived case
- Comprehensive final practical exercise