EnCase® Computer Forensics I Syllabus

Day 1

Day one starts with instruction on using EnCase® Forensic version 7 (EnCase v7) to create a new case and navigating in the EnCase v7 interface. Attendees are shown how to use EnCase v7 to acquire a complete copy of the data from removable media 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 one include:

- **Creating a case file in EnCase v7**
- **Navigating within the EnCase v7 environment**
- **Understanding the use of the timeline viewing function with EnCase v7**
- **Understanding the concept of digital evidence and its impact on an investigation**
- **EnCase v7 concepts**
  - Safeguarding and preserving evidential data
- **The basics of acquiring a forensically sound copy of data from removable media, including the use of Guidance Software's write-blocking software, FastBloc® SE**
- **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 begins with a practical exercise on the techniques learned on the previous day for creating an evidence file and then continues with a detailed discussion of the FAT file systems as well as an overview of the NT file system. The students will learn how to properly preview a computer system prior to acquisition. Hard disk acquisition is covered, using both a forensically sound Linux CD, LinEn, and drive-to-drive connection methods. Attendees will learn how to properly process evidence files and will be introduced to basic methods of search techniques.

The main areas covered on day two 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 or deleted
- **Acquisition of a hard disk**
  - Acquisition using a forensically sound Linux operating system
    - » Drive-to-drive acquisition
    - » Network crossover-cable acquisition
- **Processing evidence**
  - Using the EnCase® Evidence Processor
  - Preparing evidence for processing
  - Managing and using the various Evidence Processor settings and toolbars
- **Creating and conducting raw and index searches**

Day 3

Day three begins with a review and then launches into instruction on how to view the results of various search techniques. The students will learn how to bookmark data and use the new tagging feature included in EnCase v7. 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 v7 and learn how to copy data from within an evidence file. Instruction is provided on report creation techniques available in EnCase v7. The students will participate in practical exercises during the day's activities and the day will conclude with an exercise in signature and hash analysis.

The main areas covered on day three include:

- **Viewing search results**
  - Reviewing methods
  - How to examine results
- **Bookmarking and tagging search results**
- **File types**
  - Discussion of the categories of files and folders and the icons employed by EnCase v7
- **Installing external viewers**
- **Detailed copying options**
- **Signature analysis**
  - An automated comparison of the displayed file extension with the actual content of the file
- **Hash analysis**
  - Using unique values calculated based on file logical content to identify and/or exclude files
- **Basic report creation and how to use the Review Package functionality**
  - Exporting reports
  - Consolidating search results into a review package

Day 4

Day four begins with a practical exercise on conducting signature and hash analyses. The day's instruction begins with a lesson on searching and recovering data from unallocated space. Attendees are given advice and guidance for archiving as well as instruction on how to restore and open an archived case. The students will explore how to reacquire evidence in order to modify evidence-file parameters but still maintain data integrity. Attendees will observe first hand how EnCase v7 can detect and identify any changes to the content of an evidence file. The importance of proper evidence handling will be discussed and the attendees will be given examples of good practice in this area. 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 in unallocated space manually and by using EnScript® programs**
- **Restoring evidence**
  - Often required by court order; necessary to recover data and/or examine the operation of the host system in real-time
- **Archiving and reopening an archived case**
- **Verification of an evidence file to demonstrate validity**
  - How to conduct a test, validating that hash and CRC values used in the evidence file verification are accurate
- **The importance and practicalities of evidence handling**