EnCase Computer Forensics I Syllabus

Day 1

Day one starts with instruction on using EnCase® Forensic version 7 to create a new case and navigating in the EnCase Forensic v7 interface. Attendees are shown how to use EnCase Forensic v7 to acquire a complete copy of the data from removable media in a forensically sound manner. The concept of digital evidence and how to verify evidence are also included.

The main areas covered on day one include:

- **Creating a case file in EnCase Forensic v7**
- **Navigating within the EnCase Forensic v7 environment**
- **Understanding the concept of digital evidence and its impact on an investigation**
- **The importance and practicalities of evidence handling**
- **EnCase Forensic v7 concepts**
  - Safeguarding and preserving evidential data
- **The basics of acquiring a forensically sound copy of data from removable media, including the use of the Guidance Software write-blocking software, FastBloc® SE**
- **Verification of an evidence file to demonstrate validity**
  - How to conduct a test, validating that hash and CRC values or data block validation used in the evidence file integrity check verify the evidence files

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 an explanation of how computers work (paying particular regard to the associated impact on forensic examination). Hard disk acquisition is covered, using a forensically sound Linux CD, LinEn, and drive-to-drive connection methods. The students will learn how to properly preview a computer system prior to acquisition, using the Direct Network Preview function. Attendees will learn how to bookmark data and use the tagging feature included in EnCase Forensic v7. Instruction will proceed with a detailed discussion of the FAT file systems as well as an overview of the NT and ExFAT file systems and the attendees will learn how to properly process evidence files.

The main areas covered on day two include:

- **Understanding how computers work**
  - Hardware and associated terminology
  - The CMOS, BIOS, and boot sequence
  - Interpreting binary and hexadecimal data
  - The basics of text encoding
- **Acquisition of a hard disk or other media from a powered-off computer using LinEn**
- **How to use the Direct Network Preview function to preview a live running computer and the abilities to capture RAM and process memory will also be shown**
- **Bookmarking and tagging search results**
- **NT/FAT/ExFAT File Systems**
  - How these file systems track data on their respective volumes as well as what occurs when a file is created or deleted
- **Processing evidence**
  - Using the EnCase® Evidence Processor
  - Preparing evidence for processing
  - Managing and using the various Evidence Processor settings and toolbars

Day 3

Day three begins with an introduction to the basic methods of search techniques and how to view the results. Instruction continues on file descriptions and the use of file signatures to properly identify file types. The students will participate in a practical exercise, allowing them to practice the searching and bookmarking techniques covered so far. Attendees will install external viewers within EnCase Forensic v7 and will then learn how to copy data from within an evidence file. The day's activities conclude with instruction on the principal and practical usage of digital fingerprints (hash value) to identify files of interest and exclude known files is also covered.

The main areas covered on day three include:

- **Creating and conducting index search queries and raw keyword searches**
- **Viewing search results**
  - Reviewing methods
  - How to examine results
- **Installing external viewers**
- **File descriptions**
  - Discussion of the categories of files and folders and the icons employed by EnCase Forensic v7
- **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

Day 4

Day four 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. Next, the students will learn how to compile evidence into simple reports. The remaining instruction focuses on maintaining and safekeeping evidence. Attendees will learn how to use the new Case Backup feature now included in EnCase Forensic v7. The students 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 Forensic 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**
- **Basic report creation and how to use the Review Package functionality**
  - Exporting reports
  - Consolidating search results into a review package
- **Using Case Backup to protect and secure stored evidence**
- **Reacquiring and 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**