



**XIONGROUP**

**Authorised Training Partner**

34 Circular Road  
Singapore 049390

**opentext™**

# DF310 - EnCase Certified Examiner Prep

## Syllabus

### Day 1

Day one starts with a review of the OpenText EnCase Forensic software (EnCase) examination methodology. Attendees review the techniques for creating a case and working within the EnCase environment, navigating the EnCase interface, and processing the case with the EnCase Evidence Processor. Participants continue by exploring concepts involving the EnCase acquisition of computer-related evidence, discussing digital evidence handling, and incorporating single files into the case and creating EnCase logical evidence files.

Instruction continues with attendees discussing exporting files and data from EnCase for reporting, reacquiring an evidence file, restoring an evidence file, and archiving a case. Participants engage in a discussion of the FAT, exFAT, and NT file systems and the day's instruction concludes with reviewing the signature analysis process, which reveals the true identity of files regardless of the extension.

### The main areas covered on day 1 include:

- Understanding EnCase methodology
- Creating an EnCase case file
- Navigating within the EnCase environment
- Acquiring evidentiary media with EnCase
- Executing the EnCase Evidence Processor
- Understanding the structure and function of EnCase evidence files, case files, and configuration files
- Examining live and acquired evidence using EnCase Forensic
- Safeguarding, handling, and preserving evidential data
- Creating EnCase logical evidence files from single files or acquired evidence
- Identifying physical and logical disk and file structures relevant to FAT, ExFAT and NTFS
- Defining EnCase file types
- Reviewing exporting and importing options with EnCase
- Exploring proper methodologies in closing the case—reacquiring, restoring, and archiving the case
- Analyzing file signatures to determine the true identity of objects

## COURSE INFORMATION

Course duration:  
**3 days**

CPE Credits:  
**24**

Delivery method:  
**Group-Live**

Instructor:  
**Frank Butler**

NASBA defined level:  
**Intermediate**

Prerequisites:  
**DF210 - Building an Investigation with EnCase**

## CONTACT INFORMATION

Call:  
**+65 6610 3488**

Email:  
**enquiries@xiongroup.com**

Website:  
**www.xiongroup.com/training**

## Day 2

Day two begins with reviewing the functionality and use of EnCase Forensic to efficiently examine digital evidence. The day starts with a review of performing a hash analysis of data in EnCase to locate notable files and to filter known files from view. A review of auditing the physical device, including the examination, identification, and recovery of logical disk structures and encryption is then conducted.

We continue instruction with installing external viewers within EnCase, identifying and viewing the structure of compound files and bookmarking evidentiary data from an EnCase evidence file. Instruction then moves to searching evidence in EnCase, including the use and differences in raw searches and index searches and keyword development.

Searching instruction continues with the implementation of the EnCase GRE operators in raw searches. A presentation of analyzing printing artifacts is conducted and the day concludes with a review of the Windows registry and determining/implementing time zone settings in EnCase

### The main areas covered on day 2 include:

- Performing hash analysis
  - Creating hash libraries and hash sets in EnCase
  - Adding hash values to the hash sets and library
  - Using hash values to identify/exclude files without visually examining each one
- Accessing encrypted drives
- Auditing physical disk allocation and recovering logical structures and file systems with EnCase
- Installing and using external viewers
- Examining compound files
- Viewing compound file structures
- Searching compound files properly
- Preserving evidentiary data for reporting (bookmarking)
- Performing search operations with EnCase
  - Creating keywords for raw searching
  - Implementing physical and logical raw searching with EnCase
  - Using GREP operators within EnCase to construct advanced search terms
  - Creating advanced index search terms to quickly locate responsive data in data and metadata
  - Using index operators to further create robust search terms
  - Saving and working with search terms and results
- Analyzing printing artifacts with EnCase
- Examining the Windows registry
  - Locating the Windows registry hives and defining their function
  - Defining elements of the Windows registry
  - Defining registry keys (folders) and values
  - Locating and setting the time zone in EnCase

## Day 3

Instruction on day three continues with examining data in EnCase followed by a discussion of the location and function of common Windows artifacts and databases that often provide vital information to investigations. We then take a closer look at the function and structure of Windows link files (shortcuts), identifying critical locations within the structure to gather intelligence information for the link file's respective target.

Attendees will also review the function of the Windows Recycle Bin, including the impact on the file system and associating the Window's Security Identifier to a named user account. Examining data in EnCase continues with examining and bookmarking email, Internet history, and cache content, concluding with the exploration and identification of removable USB devices used on a Windows computer. The course concludes with hands-on instruction in creating, editing, and exporting a report in EnCase. Following a review, the students will take the Phase I examination.

### The main areas covered on day 3 include:

- Analyzing Windows artifacts
  - Viewing user account information and associated data
  - Viewing System folders and files of interest
- Examining link files
  - Deconstructing link files to reveal internal structures relating to their target files
- Recycle Bin recovery
  - Examining the Recycle Bin, its properties, and function
  - Linking Recycle Bin data to the associated user
  - Identifying registry entries controlling operation of the Recycle Bin
- Email/Internet examination
  - Examining email and methods available within EnCase to locate and parse email data stores
  - Navigating email, including different view modes in EnCase and locating email attachments
  - Identifying email conversations and their related messages
  - Exploring the results of activity on the Internet, including cookies, history, web cache, and bookmark data
- Identifying registry entries that document USB device usage, and describing the function of the USB device descriptor
- Reporting with EnCase
- Create, edit, and export an examination report using EnCase
  - Hands-on review of editing the report template and saving it as an EnCase template for use in future investigations
  - Reviewing course content in preparation for the EnCase certification examination