DF210 - Building an Investigation with EnCase

**Formerly EnCase v7 Computer Forensics II

Duration: 4 Days

This hands-on course is designed for investigators with strong computer skills, prior computer forensics training, and experience using the OpenText™ EnCase™ software (EnCase). This course builds upon the skills covered in the DF120–Foundations in Digital Forensics course and enhances the examiner's ability to work efficiently using the unique features of EnCase. During this course, students will build an investigation using analysis techniques, such as recovering deleted volumes, registry analysis, Recycle Bin examination, and examining compound files. Other analysis techniques, such as searching unallocated clusters, parsing current Windows artifacts, examining email and Internet artifacts, and analyzing USB device artifacts will be included.

Students must understand EnCase Forensic concepts, the structure of the evidence file, creating and using case files, and data acquisition and basic analysis methods. It is also important that the students are familiar with the methods for recovering deleted files and folders in a FAT environment, conducting indexed queries and keyword searches across logical and physical media, creating, and using EnCase bookmarks, file signature analysis, and exporting evidence.

Delivery method: Group-Live.

NASBA defined level: Intermediate.

CPE Credits - 32

Focusing on commonly conducted investigations, students will learn the following:

- How to identify and open a volume that was encrypted using Windows BitLocker™
- How to locate and recover deleted partitions
- How to deal with compound file types
- How to determine time zone offsets and properly adjust for the time zone in EnCase
- About the Windows® Registry
- How to create and use conditions for effective searching
- About the ExFAT and NT file system through an overview of the systems
- How to identify Window system artifacts, such as the User folders, pagefile.sys, Recycle Bin, and other folders
- How to locate and examine shortcut files
- How to identify and recover data relating to the use of removable USB devices
- How to recover data from the Recycle Bin
- How to conduct a search for email and email attachments
- How to examine email and Internet artifacts
- How to employ the EnCase Media Analyzer during an investigation
- How to employ GREP operators to enhance searching techniques
- How to recover artifacts from the print spooler

- How to search and recover files from unallocated space
- How to use the EnCase Physical Disk Emulator (PDE) Module
- How to create reports to present investigation findings

Audience

This course is intended for cybersecurity professionals, litigation support, and forensic investigators.

Prerequisites

- DF120 – Foundations in Digital Forensics with EnCase

*Participants should have attended the EnCase course, DF120–Foundations in Digital Forensics.