DF120 - Foundations in Digital Forensics with EnCase

**Formerly EnCase v7 Computer Forensics I.

Duration: 4 Days

This hands-on course involves practical exercises and real-life simulations in the use of OpenText™ EnCase™ software (EnCase). The class provides participants with an understanding of how EnCase may be used to examine data related to an incident response, an employee misconduct investigation, and/or a law enforcement criminal and/or civil investigation. Participants create cases using EnCase, configure the application to maximize its utilization, and learn evidence acquisition concepts and how to validate the data collected. Instruction progresses to the analysis of the data whether related to criminal investigations, cybersecurity incidents, or other matters. The course will cover techniques, such as keyword or indexed searching along with hash analysis. Participants will learn how to bookmark, export, and create reports relating to examination findings. The course concludes with instruction on archiving, validating the data, and restoring the case.

Delivery method: Group-Live.

NASBA defined level: Basic

CPE Credits - 32

Students attending this course will learn the following:

- The EnCase digital forensic methodology and how to create a case
- How to configure and navigate the EnCase interface
- How to use case templates included with EnCase
- How to the understand EnCase concepts
- How to create an evidence file
- How to install external file viewers to EnCase
- How to create conditions within EnCase
- How to analyze file signatures and view files
- How to adjust time zones within EnCase
- How to extract data and files from your evidence
- How to decipher data allocation and file descriptions
- How to tag and bookmark evidence files, file sets, and data structures
- How to conduct raw and index searches
- How to conduct hash and entropy analyses and import hash sets
- How to import and export data
- How to prepare reports using templates provided with EnCase
- How to create reports
- How to restore evidence
- How to archive files and data created through the analysis process
- The proper techniques for handling and preserving evidence

Audience

This course is intended for digital forensic investigators, including law enforcement, government, military, corporate, IT security, and litigation support professionals.

Participants may have minimal computer skills and may be new to the field of computer forensics.

Prerequisites

- Basic computer skills. Advance preparation for this course is not required.