DF310 EnCase Certified Examiner Prep

Syllabus

Training facilities

Los Angeles, CA (Pasadena, CA)
1055 East Colorado
Boulevard Suite 400
Pasadena, CA 91106-2375

Washington, DC
(Gaithersburg, MD)
9711 Washingtonian Blvd
6th floor, Room 601 (Paris Room)
Gaithersburg, MD 20878

London, UK (Reading)
420 Thames Valley Park Drive
Earley, Reading
Berkshire
RG6 1PT

Munich, Germany (Grasburnn)
Werner-von-Siemens-Ring 20
85630 Grasburnn / München
Germany

For a complete listing of locations, including Authorized Training Partners around the world, please visit

opentext.com/learning-services/learning-paths

EnCaseTraining@opentext.com

This course is designed as a review of the skills that are applicable to the EnCE certification process. These skills are taught during the OpenText DF120-Foundations in Digital Forensics and DF210-Building an Investigation courses. The course prepares students to successfully complete the Phase I and Phase II EnCE (EnCase certification) examinations.

This instruction is intended as a review of previously delivered material and is purposely not as in-depth as that provided during the full-length courses. This course should not be construed as a replacement for the full-length DF120-Foundations in Digital Forensics and DF210-Building an Investigation courses and, due to the pace at which this class runs. Experience using OpenText™ Forensic (EnCase) is encouraged.

Day 1

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

Instruction continues with attendees discussing how to export files and data from OpenText Forensic 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 one include:

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

Day 2

Day two begins with a review of the functionality and use of OpenText Forensic to efficiently examine digital evidence. The day starts with a review of the process to perform a hash analysis of data in OpenText Forensic 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 OpenText Forensic, identifying and viewing the structure of compound files, and bookmarking evidentiary data from an OpenText Forensic evidence file. Instruction then moves to searching evidence in OpenText Forensic, including the use of raw and index searches and keyword development and their respective differences.

Searching instruction continues with the implementation of the OpenText Forensic GREP operators in raw searches. The day concludes with a review of the Windows registry and determining/implementing time zone settings in OpenText Forensic.

The main areas covered on day two include:

- Performing hash analysis
    - Creating hash libraries and hash sets in OpenText Forensic
    - 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 OpenText Forensic
- 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 OpenText Forensic
    - Creating keywords for raw searching
    - Implementing physical and logical raw searching with OpenText Forensic
    - Using GREP operators within OpenText Forensic 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
- 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 OpenText Forensic

Day 3

Instruction on day three continues with examining data in OpenText Forensic 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 OpenText Forensic 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 OpenText Forensic. Following a review, the students will take the Phase I examination.

The main areas covered on day three 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 OpenText Forensic to locate and parse email data stores
  - Navigating email, including different view modes in OpenText Forensic 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 OpenText Forensic
- Create, edit, and export an examination report using OpenText Forensic
  - Hands-on review of editing the report template and saving it as an OpenText Forensic template for use in future investigations
- Reviewing course content in preparation for the EnCase certification examination