opentext™

Training overview

DF120 Foundations in Digital Forensics with OpenText™ EnCase™ Forensic

Training facilities

Ondata International SL
Avenida de Brasil 17, planta 3
28020, Madrid
Tel. 91 417 4468
sales@ondata.es
https://www.ondata.es

Syllabus

Day 1

Day one starts with instruction on using OpenText™ EnCase™ Forensic version 8 to create a new case, as well as navigation within the EnCase interface. Students participate in a practical exercise, which allows them to test their newly acquired navigation skills and provides an understanding of how to search for files based on metadata.

Attendees then use EnCase to acquire a forensic copy of media while protecting the original media from change. Methodologies used within a computer system for the allocation of storage areas are also discussed, along with the concepts of digital evidence and how to validate evidence verification.

Day 1 will cover:

- Creating a case file in EnCase
- Navigating within the EnCase environment
- Understanding concepts of digital evidence and disk/volume allocation:
  - Types of evidence
  - Terminology describing data storage, including unallocated space, unused disk area, volume slack, file slack, RAM slack and disk slack
- Documenting EnCase concepts including:
  - Evidence files
  - Case files and backups
  - Configuration files
  - Object icons within EnCase
  - Acquiring media in a forensically sound manner

Day 2

Day two begins with a continuation of the acquisition concepts lesson, which is followed by a quiz that reviews presented concepts. Students next learn how to properly preview a live computer system prior to acquisition using the Direct Network Preview function.

Attendees then utilize the OpenText™ EnCase™ Evidence Processor to run modules on evidence files to obtain results that are reviewed during subsequent lessons. Attendees bookmark and tag data to be incorporated into an examination report during the report creation lesson.

Students next perform a practical exercise during which they backup the case with customized settings and bookmark items for reporting purposes. Participants then run two different searching processes: raw searching (on raw data, indexed or not) and index searching (on interpreted, indexed data).

opentext™

Day 2 will cover:

- Previewing a running computer (even one using full disk encryption) using multiple techniques, including the Direct Network Preview function
- Running EnCase utilities to capture RAM
- Processing evidence:
  - Running processes, including file signature analysis, protected file analysis, hash and entropy analysis, email and internet artifact analysis, and word/phrase indexing
  - Executing modules, including file carver, Windows artifacts parser and system info parser
  - Bookmarking and tagging data for inclusion in the final report
  - Creating and conducting raw keyword searches and index search queries to locate search expressions of interest

Day 3

Day three begins with the completion of the index searching lesson. Participants perform a practical exercise, which allows them to practice the discussed searching and bookmarking techniques.

Attendees next define and install external viewers within EnCase and copy data from within an evidence file to the file system for use with other computer programs. Participants employ the use of file signature analysis to properly identify file types and to locate renamed files.

Students are then provided instruction on the principal and practical usage of hash analysis. Attendees create a hash library containing hash sets and hash values of notable files to identify and known files to exclude from an evidence file. Hash analysis tools, such as EnScript™ programs and other utilities, are then employed to analyze hash libraries and to incorporate commonly available hash libraries/sets into the examination environment.

Day 3 will cover:

- Creating and conducting index search queries and raw keyword searches
- Incorporating the use of installed external viewers used by examiners into EnCase
- Copying files, folders and data from EnCase to the local file system using different methodologies within EnCase, including mounting devices, volumes and folders as a network share within the local file system for analysis by other tools
- Incorporating external files within EnCase and creating a logical evidence file of selected objects within the case
- Including external files within EnCase and creating a logical evidence file of selected objects within the case
- Performing signature analysis to determine the true identities of file objects and to ascertain if files were renamed to hide their true identities
- Conducting hash analysis using unique values calculated based on file logical content to identify and/or exclude files
- Importing and exporting data to/from Project VIC

Day 4

Day four begins with a demonstration of entropy analysis techniques to assist in the identification of files that nearly match notable files. Next, students will complete a practical exercise on conducting signature, entropy and hash analyses.

The program continues with a lesson on searching and recovering data from unallocated space. Students then discover how to customize and organize a report using bookmarked data and how to include pertinent file metadata in the report.

Students are also given advice and guidance on properly archiving and later reopening a case. During the archiving process, attendees use procedures to reacquire an evidence file to change evidence file parameters, such as compression, evidence file format or segment size to facilitate effective archiving. The course concludes with a final practical exercise on the week's instruction.

Day 4 will cover:

- Running entropy analysis to locate files that may be near matches to other files or that may be password protected, obfuscated or encrypted
- Locating and recovering evidence, including images, documents and videos in unallocated space manually and by using EnScript programs
- Creating a report of files and data bookmarked during the examination:
  - Exporting reports
  - Modifying basic reporting formats
  - Creating templates for future case utilization
  - Reacquiring evidence to change evidence file settings
  - Restoring evidence to run proprietary software or as required by a court order
  - Archiving and reopening an archived case
  - Completing a comprehensive final practical exercise