opentext™

Training overview

DF210
Building an Investigation 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 an overview of the OpenText™ EnCase™ Version 8 (EnCase) environment. The students then learn how to collect encrypted information by examining files encrypted with Windows® BitLocker™. Attendees go on to study the Master Boot Record partitioning model and deleted partition recovery.

Instruction continues with an examination of compound files, their structures and issues surrounding their examination. Students move on to explore a very important type of compound file structure, the Windows® Registry hive file. They explore mounting and examining these files and learn the relationship of the hive files to the structure of the Registry in its online state.

Students then progress to examining the time zone information contained within the Registry, its importance to their case and how they apply it in EnCase. The students are provided intermediate-level instruction regarding the methods for creating conditions to filter data. Next, students are provided with an overview of the Evidence Processor and the Malone case, which will be used throughout the rest of the course.

Day 1 will cover:

- Reviewing EnCase case creation and adding evidence

- Examining data encrypted with BitLocker

- Understanding the Master Boot Record partitioning scheme

- Recovering data lost through the partitioning process

- Understanding partition recovery

- Understanding compound files

- Mounting and searching compound files

- Documenting data contained within these compound files

- Examining compound files

- Understanding single files and logical evidence files

- Examining the Windows Registry
- Examining the elements of the Registry
- Understanding Registry keys (folders) and values
- Understanding Registry value types
- Locating and mounting the Registry hive files
- Examining time zone settings with the Registry
- Applying time zones within EnCase
- Using conditions to filter data
- Reviewing Evidence Processor

Day 2

Day two begins with instruction on the ExFat and NT file systems. Students will then participate in a practical exercise on examining all three files systems and their differences.

Instruction is provided on the use of the EnCase™ Physical Disk Emulator (PDE) Module. The program then focuses on specific analysis of common artifacts that often provide vital information to investigations. These specific areas reveal data that can provide a clearer indication of user activities, including examining Cortana and EDB artifacts.

The students participate in practical exercises throughout the day to underscore the learned techniques. Instruction for the day concludes with the processing of our second case.

Day 2 will cover:

- ExFAT and NT Files Systems
- Windows artifacts
- User account information and associated data
- System folders and files of interest
- Thumbnail cache files
- Windows 7 specific artifacts
- Folder structure and the effect of junctions (folder mount-points)
- User/administrator privileges and impact on storage of data
- Links and Library folder content
- System files

- Cortana and EDB artifacts
- Functionality of Cortana available since the release of Windows 10, supplementing Windows Search
- Windows Search file for data
- Cortana artifacts
- Windows EDB file repair and recovering EDB data on the later Windows operating systems
- Microsoft Exchange Database EDB file identification
- GREP, proper syntax and potential results

Day 3

Day three focuses on file storage, including link files and how data located on removable USB devices can be examined and recovered. Students will explore the methods that EnCase offers to provide detailed information to the examiner. Instruction is also provided on identifying, locating and recovering email messages and attachments. Students participate in practical exercises throughout the day, and the final lesson for day three is focused on examining various internet artifacts.

Day 3 will cover:

- Reviewing shortcut or link files
- Deconstructing link files to reveal internal structures related to their target files
- Using link files to help determine drive letter assignment
- Identifying removable USB devices
- Reviewing the Windows Recycle Bin
- Linking Recycle Bin data with the associated user
- Registry entries controlling operation of the Recycle Bin
- Examining the Recycle Bin, its properties and function
- Exploring the implementation of Recycle Bin
- Exploring email and internet history
- Examining both client-based and web-based email and methods available within EnCase to locate and parse email data stores
- Recovering and analyzing email attachments
- Exploring internet artifacts

opentext™

Day 4

Day four begins with instruction on the use of the GREP operator functionality of EnCase to perform advanced searches and continues with a lesson on the artifacts associated with the print spooler. Next, students will learn how to search through unallocated space. The week of instruction concludes with a lesson on report creation followed by a final hands-on review of all the instruction covered in the course.

Day 4 will cover:

- Using the GREP within EnCase to construct advanced search terms

- Recovering the print spooler

- Understanding the printing process and associated files

- Recovering SPL and SHD files as well as understanding and extracting graphical data and metadata

- Conducting searches through unallocated space

- Understanding advanced reporting techniques

OpenText Authorized Training Partner
Ondata International SL | Tel. 91 417 44 68 | https://www.ondata.es | sales@ondata.es