opentext™

Training overview

DF210 Building an Investigation with OpenText™ EnCase™ Forensic

Syllabus

Day 1

Day one starts with an overview of the OpenText™ EnCase™ Forensic 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. Students progress to examining the time zone information contained within the Registry, its importance to their case and how they apply it in EnCase They explore mounting and examining Windows Registry files and learn the relationship of the hive files to the structure of the Registry in its online state.

Next, students participate in processing 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 MBR and GPT 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
- Examining time zone settings with the Registry
- Applying time zones within EnCase
- 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

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

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

www.opentext.com/encasetraining
EnCaseTraining@opentext.com
opentext.com/encasetraining

Day 2

Day two begins with intermediate-level instruction regarding the methods for creating conditions to filter data followed by a practical exercise to solidify the tuition. Next, students are provided instruction on the ExFat and NT file systems and participate in a practical exercise on examining all three files systems and their differences.

The curriculum 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 the Windows EDB and other Windows 10 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:

- Using conditions to filter data
- ExFAT and NT Files Systems
- Windows artifacts
- User account information and associated data
- System folders and files of interest
- Thumbnail cache files
- Windows 10 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
- 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

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:

- 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
- Exploring internet artifacts
- Windows EDB artifacts
- Windows Search file for data
- Windows EDB file repair and recovering EDB data on the later Windows operating systems

Day 4

Day four activities continues with more instruction on the databases included with Windows. Next, the students learn how to use the EnCase Media Analyzer and instruction continues with a lesson on the artifacts associated with the print spooler. Students will learn how to search through unallocated space and then how to use the EnCase™ Physical Disk Emulator (PDE) Module. 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:

- Microsoft Exchange Database EDB file identification
- The use of EnCase Media Analyzer to identify images containing visual threats, such as adult content, violence, extremism, drugs, child-abuse material, weapons, and other relevant categories
- 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
- Report creation

opentext.com/contact Twitter | LinkedIn