DF210 Building an Investigation with OpenText Forensic

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 (Grasbrunn)
Technopark 2 Werner-von-Siemens-Ring 20 Munich
Grasbrunn

For a complete listing of locations, including Authorized Training Partners around the world, please visit opentext.com/learning-services/learning-paths.

EnCaseTraining@opentext.com

Day 1

Day 1 starts with an overview of the OpenText™ Forensic (EnCase) environment. The students then learn how to collect encrypted information by examining files encrypted with Windows® BitLocker™. Students then study the MBR and the GPT partitioning model as well as 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 then progress to examining time zone information contained within the Registry, its importance to their case, and how they apply it in OpenText Forensic. They explore mounting and examining Windows Registry files and learn their relationship to the structure of the Registry Hive in its active state.

Next, students participate in processing the Malone case, an evidence file that will be examined throughout the course.

Day 1 will cover:

- Reviewing OpenText Forensic 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 OpenText Forensic
- 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

Day 2

Day 2 begins with intermediate-level instruction on NT file systems and ExFat and continues with a practical exercise on examining the file 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 Thumbnail Cache, Link files and other Windows 10 artifacts.

Students complete 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 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 3 focuses on file storage, including linking a USB drive to a specific computer and how connections can be confirmed between the two devices. Students will explore the methods that OpenText Forensic 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 in the final two lessons of Day 3, students will focus on examining internet artifacts and using Artifact Explorer.

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 OpenText Forensic to locate and parse email data stores
- Exploring internet artifacts
- Introduction and instruction on how to use Artifact Explorer

Day 4

Day 4 begins with instruction on how to leverage GREP operators to enhance searching techniques. Instruction continues with a lesson on the use of Media Analyzer. Participants will learn how to recover specific files from unallocated space and then how to use the Physical Disk Emulator (PDE) Module to virtually boot up a running system from an evidence file.

The week of instruction concludes with a lesson on report creation followed by a final hands-on review of the entire course.

Day 4 will cover:

- Obtaining a basic understanding of main GREP operators.
- The use of Media Analyzer to identify images containing visual threats, such as adult content, violence, extremism, drugs, child-abuse material, weapons, and other relevant categories
- 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