DF120 Foundations in Digital Forensics with OpenText Forensic (EnCase)

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)
Werner-von-Siemens-Ring 20
85630 Grasbrunn/München
Germany

OpenText Forensic Learning Courses ›

Day 1

Day 1 starts with instruction on using OpenText™ Forensic (EnCase) to create a new case and navigate within the OpenText Forensic interface. Students discuss general forensic methodology and learn how to use the case templates included with OpenText Forensic. Students learn how computer systems allocate storage.

The concepts of digital evidence identification and preservation are also covered. Students participate in a practical exercise toward the end of the day, which allows them to test their newly acquired navigation skills and fosters an understanding of how to search for files based on metadata.

Day 1 will cover:

- Understanding general forensic methodology
- Creating a case file in OpenText Forensic
- Configuring and navigating the OpenText Forensic environment
- Using the case templates included with OpenText Forensic
- Defining data storage terminology, including but not limited to unallocated space, unused disk area, metadata or administrative storage of file and folder objects, volume slack, file slack, RAM slack, and disk slack

- Documenting files maintained by OpenText Forensic to facilitate examinations:
  - Evidence files
  - Case files and backups
  - Configuration files

Day 2

Day 2 begins with instruction on the various acquisition concepts, defining and installing external viewers, then the students will learn how to create conditions that are key to maximizing search results. Students employ file signature analysis to properly identify file types and to locate renamed files. Next, the students will learn how to access pathways to automate the determination of the time zone settings and subsequent adjustment. The students close out the day’s activities with instruction on the techniques on using Evidence Processor to run modules on evidence files to obtain results.

Day 2 will cover:

- Learning acquisition concepts
- Incorporating the use of installed external viewers used by examiners into OpenText Forensic
- Identifying and adapting time zones within OpenText Forensic
- Creating and employing conditions
- Performing signature analysis to determine the true identities of file objects and to ascertain if files were renamed to hide their true identities
- Processing evidence:
  - Running processes, including but not limited to file signature analysis, protected file analysis, hash and entropy analysis, email and internet artifact analysis, and word/ phrase indexing
  - Executing modules, including but not limited to file carver, Windows artifacts parser, and system info parser

Day 3

At the start of Day 3, students are instructed on data allocation and file descriptions. Next, the students will tag and bookmark data to be incorporated into an examination report during the Report Creation lesson. Students perform a practical exercise during which they back up the case with customized settings and bookmark items for reporting purposes. Students will then perform raw keyword searches and index queries and practice their newly learned searching and bookmarking processes.

Day 3 will cover:

- Understanding concepts of data allocation and OpenText Forensic object descriptions
- Tagging and bookmarking data for inclusion in the final report
- Creating and conducting raw keyword searches
- Creating and conducting raw keyword searches to locate search expressions of interest
- Creating and conducting Index Search Queries

Day 4

The day’s instruction begins on the principal and practical usage of hash analysis libraries. The lesson begins with the students learning how to conduct a hash analysis of a hash library that contain hash sets and hash values to identify notable files and to exclude known files from an evidence file.

The students then learn the definition of entropy and how it can be helpful during the forensic analysis. They will also practice the various ways to export and import files to and from an evidence file. The students then discover how to customize and organize a report using bookmarked data and how to include pertinent file metadata in the report.

The students are given advice and guidance in 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 or 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:

- Conducting hash analysis using unique values calculated based on file logical content to identify and/or exclude files
- Running entropy analysis to locate files that may be near matches to other files or that may be password-protected, obfuscated or encrypted
- Copying files, folders and data from OpenText Forensic to the local file system using different methodologies within OpenText Forensic, including mounting devices, volumes and folders as a network share within the local file system for analysis by other tools
- Importing and exporting data to/from Project VIC
- Creating a report of files and data bookmarked during the examination
- Exporting reports
- Modifying basic reporting formats
- 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