opentext™

Training overview

ED290-eDiscovery Training with EnCase Information Assurance

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

For a complete listing of locations, including Authorized Training Partners around the world, please visit **opentext.com/encasetraining**

EnCaseTraining@opentext.com
opentext.com/encasetraining

Day 1

Day one of this course begins with a detailed discussion of the eDiscovery process and focuses on planning an eDiscovery project so it proceeds efficiently and accurately.

Students are introduced to fully tested methods for planning an eDiscovery project. The day's instruction walks them through a complete and thorough understanding of the various infrastructure components.

The students are introduced to the OpenText™ EnCase™ Information Assurance tools that facilitate planning and project management. An introduction to conditions, a key element of EnCase Information Assurance, is provided next. Students participate in practical exercises throughout the day, reinforcing the learned techniques. At the end of the day, activities conclude with instruction on the global-level interface and associated functions.

On day one, students will participate in an overview of EnCase Information Assurance. The instruction covered includes:

- Detailed discussions on current issues encountered during eDiscovery projects and how EnCase Information Assurance features and functions are mapped into the Electronic Discovery Reference Model (EDRM).
- A demonstration of the EnCase Information Assurance infrastructure.
- Software and hardware requirements.
- Culling from the point of collection.

Given that planning for an eDiscovery process is both challenging and crucial for success, students will participate in detailed discussions regarding effective planning activities.

Topics covered will include:

- Data mapping.
- Identifying custodians and targets.
- Collection strategy.
- Secondary culling.
- Avoiding common collection obstacles.

Additional tuition includes:

- Use of tools to help in the eDiscovery planning stage.
- Examination of the Case Screening module, which provides the examiner with an overview of the composition from sampled data.
- Instruction on how to use the Matching Files Exporter module to create a hash set of files that will be excluded or included during collections or processing.
- Instruction on how to leverage EnCase Endpoint Investigator as a tool in the planning phase as well how it can be used to assist in validating collection or processing criteria.
- How to configure a global-level interface of EnCase Information Assurance.

opentext™

Day 2

Day two begins with a review of the previous day's instruction and a confirmation of proper configuration of the global settings.

The instruction resumes with the definition of sources and targets of electronically stored information (ESI), and students will be tasked with defining a case and sources of ESI as well as targets. Global criteria are imported for use by participants later in the course and global encryption keys are discussed.

Students then learn about the case-level interface to be used to configure settings for the case as well as for various job types.

Participants then create custom data sets for the workflow that will be established for eDiscovery matters and configure and run a pre-collection analytics job to lay the framework for all future jobs by collecting metadata from targets.

The information covered on day two includes:

- Adding custodians and their ESI targets, such as workstations, laptops, shares, etc.
- Importing custodian and target information.
- Creating, managing, and exporting global-level criteria.
- Discussing methods of safeguarding data using global encryption keys.
- Exploring and configuring the EnCase Information Assurance case-level interface.
- Learning about the initial preview and determination of potentially relevant data called “pre-collection analytics” or “early case assessment.”
- Creating data sets to contain data that is culled during the eDiscoveryworkflow.
- Running the pre-collection analytics function, which provides the framework for all future jobs, including:
  - Creating criteria/conditions
  - Creating jobs
  - Selecting targets
  - Creating a metadata-only logical evidence file

opentext™

Day 3

Continuing from Day 2, students will complete an examination of the information gathered through the pre-collection analytics phase of the eDiscovery process.

Students will then duplicate and refine the pre-collection analytics job to further examine the collection possibilities during eDiscovery. Students then use a previously created data set to house imported evidence/data, including full disk images, LEFs of PSTs and raw PSTs.

Students conclude the day by processing the ESI, which involves the application of filtering criteria and separating or bifurcating the data into different data sets.

The information covered on day three includes:

- Examining results of pre-collection analytics and using this information to craft collection jobs, which may be extremely targeted or extremely broad for future culling.
- Importing additional evidence, including:
  - Full disk images received from the forensic team
  - Logical evidence files (LEFs), representing PSTs extracted from a server (perhaps a Microsoft® Exchange server or an IBM® Domino® server) for different custodians. Each LEF must be assigned to the proper custodian
  - Raw mail archives received from the appropriate information technology team

Additional instruction will be provided on how to create various jobs, including:

- Manual bifurcation processing job of imported entries
- Manual deduplication processing job of records
- Workflow to link together multiple jobs and data sets
- Internal jobs

opentext™

Day 4

Instruction continues with a review of the created workflow. Students will then refine the criteria used within the workflow and create keyword set using terms provided by the legal team. These keyword sets as well as when these files/emails are created/written, are added to the criteria.

Students will gain an understanding of how to utilize the EnCase Web component to review collected and processed data as well as perform index queries.

Students will then create output files or deliverables using various methods. These delivery jobs may be output in different formats and may be ingested into a myriad of repositories. Reporting mechanisms are discussed as well as the use of case templates. Lastly, attendees will discuss the remediation functionality of EnCase Information Assurance as well the requirements for enabling remediation.

The information covered on day four includes:

- A review of the workflow and instruction on refining the criteria used with the workflow to include:
  - Keyword sets
  - Hash sets (also known as “matching file sets”)
  - Date ranges contained within file/email metadata, creating deliverables for output to:
    - EDRM
    - kCura relativity
    - EnCase LEFs
    - Email archive files
    - EnCase Information Assurance review native files
    - OpenText Axcelerate
    - Concordance
    - Using the EnCase Web component to review collected and processed data
  - Creating and interpreting reports, such as:
    - Case screening report and matching files set
    - Result logs as well as criteria and condition reports
    - Custodian and target listing
    - General meet-and-confer documentation
    - Other reports, including executive case summary, detailed job, custodian job history and exception
    - Creating and using case templates
    - Using EnCase Information Assurance to perform remediation jobs as part of information governance