opentext™

TRAINING OVERVIEW

DFIR130 EnCase Endpoint Investigator Training

Syllabus

Training facilities

Los Angeles, CA (Pasadena, CA)
1055 East Colorado Boulevard
Suite 400
Pasadena, CA 91106-2375

Washington, DC (Gaithersburg, MD)
9711 Washingtonian Boulevard
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

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

Day 1

This course begins with a short review of the OpenText™ EnCase™ Endpoint Investigator software and its component parts. Students will then install the Secure Authentication for EnCase (SAFE) server, followed by administration and configuration of the SAFE server software.

After a practical exercise to test their new knowledge, students will learn how to install the agent application, which makes it possible for the EnCase Endpoint Investigator software to preview and acquire data from remote network nodes.

Finally, students will learn how to preview remote machines.

On day one, students can expect to:

- Get familiar with EnCase Endpoint Investigator software, its component parts, and installation.
- Log into the SAFE server for the first time.
- Configure the SAFE server regarding the EnCase Endpoint Investigator Enhanced Agent, network layout, roles, and users.
- Learn how to install the EnCase Endpoint Investigator agent.
- Preview remote disks, volumes, and physical memory.

Day 2

Students will learn how to navigate, filter, sort, search, and process data presented to them in the EnCase Endpoint Investigator interface. Students will then look at the advantages of using filters and conditions, followed by discussions on various acquisition options. Students will also have a practical exercise to reinforce new skills.

opentext™

On day two, students can expect to:

- Use the EnCase Endpoint Investigator Sweep Enterprise function to capture volatile data (running processes, open ports, etc.).
- Learn how to identify and retrieve target files based on hash values or file system metadata.
- Use Rapid Preview and the Enhanced Agent to collect data from endpoints.
- Practice previewing and acquiring endpoints.
- Create custom conditions to filter data.

Day 3

On the final day, students will learn how to perform raw searches. This will be followed by a discussion about how they can leverage external viewers to view file content that can't be viewed inside of EnCase Endpoint Investigator. Students will then create bookmarks that can later be used for the final report.

Students will also discuss how to use the evidence processor and review the results, allowing them to perform index queries. They'll also discuss the use of signature and hash analysis.

The last lesson demonstrates how case reports can be created using the different EnCase Endpoint Investigator bookmarking options. The course concludes with a final exercise.

On day three, students can expect to:

- Perform raw and indexed keyword searching.
- Use external viewers to view the content of files that can't be viewed inside of EnCase Endpoint Investigator.
- Bookmark case information, examination notes, folder structures, evidence items (files, internet artifacts, etc.), raw text, decoded data, transcript data, keyword hits, and tabular data.
- Determine file type using file extensions and file signature analysis.
- Locate files with hash analysis.
- Use the Evidence Processor to identify email and internet artifacts.
- Understand case and report templates.
- Move and order bookmarks and bookmark folders to create the final case report.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: **opentext.com**.

Connect with us:

- **OpenText CEO Mark Barrenechea's blog**
- **X (formerly Twitter)** | **LinkedIn**

opentext.com/contact