opentext™

Training overview

DFIR130 EnCase Endpoint Investigator Training

Syllabus

Day 1

Day one starts with a short review of the OpenText™ EnCase™ Endpoint Investigator software and its component parts. Students then move on to administration and configuration of the Secure Authentication for EnCase (SAFE) server software.

After a practical exercise to test their new knowledge, students move on to a lesson on installation of the agent application, which makes it possible for the EnCase Endpoint Investigator software to preview and acquire data from remote network nodes.

Finally, students learn how to preview and acquire physical disks, volumes, physical memory, volatile data and logical data (files and folders) from remote machines.

Day one covers:

- Getting familiar with EnCase Endpoint Investigator software, its component parts and licensing
- Logging into the SAFE server for the first time, including troubleshooting steps
- Configuring the SAFE server with regard to the EnCase Endpoint Investigator Enhanced Agent, network layout, roles and users
- Learning local and remote installation of the EnCase Endpoint Investigator agent
- Previewing and acquiring remote disks, volumes, logical data (files and folders) and physical memory
- Using the EnCase Endpoint Investigator Sweep Enterprise function to capture volatile data (running processes, open ports, etc.) and how to identify and retrieve target files based on hash values or file system metadata

Day 2

Day two concludes the remote preview and acquisition lesson. This is followed by a practical exercise to reinforce new skills. Students then learn how to navigate, filter, sort, search and process data presented to them in the EnCase Endpoint Investigator interface.

The last lesson demonstrates the creation of a case report using the different EnCase Endpoint Investigator bookmarking options. This is followed by a final exercise covering all the practical aspects of using EnCase Endpoint Investigator learned so far.

Day 2 covers:

- Practicing basic EnCase Endpoint Investigator navigation, including viewing, sorting, selecting and tagging files, folders and other items in the case
- Determining file type using file extensions and file signature analysis
- Viewing the internal structure of archive and other supported compound file types
- Using the Evidence Processor to identify internet artifacts
- Creating custom conditions to filter data
- Performing raw and indexed keyword searching–also using EnScript applications to perform hybrid keyword searches (searching the raw data of some evidence-items and transcript data of others)
- Exporting and printing report data for individual evidence items
- Extracting tabular data into PDF, HTML, XML, text and other supported formats
- Understanding case and report templates
- Bookmarking case information, examination notes, the structure of folders, evidence items (files, internet artifacts, etc.), raw text, decoded data, transcript data, keyword hits and tabular data
- Moving and ordering bookmark and bookmark folders to create the final case report
- Using the Triage Report function

opentext.com/contact