XIONEGROUP
Authorised Training Partner
34 Circular Road
Singapore 049390

opentext™

DF120 - Foundations in Digital Forensics with OpenText™EnCase™

Formerly EnCase v7 Computer Forensics I

COURSE INFORMATION

Course duration:
4 days

CPE Credits:
32

Delivery method:
Group-Live

Instructor:
Frank Butler

NASBA defined level:
Basic

Prerequisites:
Basic computer skills.

CONTACT INFORMATION

Call:
+65 6610 3488

Email:
enquiries@xionegroup.com

Website:
www.xionegroup.com/training

Syllabus

Day 1

Day one starts with instruction on using OpenText™ EnCase™ Forensic (EnCase) to create a new case and navigate within the EnCase interface. Participants discuss general forensic methodology and learn how to use the case templates included with EnCase. Methodologies used within a computer system for the allocation of storage areas are discussed. The concepts of digital evidence identification and preservation are discussed. Students participate in a practical exercise toward the end of the day, which allows them to test their newly acquired navigation skills and provides an understanding of how to search for files based on metadata.

The main areas covered on day 1 include:

- Understanding general forensic methodology
- Creating a case file in EnCase
- Configuring and navigating the EnCase environment
- Utilizing the case templates included with EnCase
- 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 EnCase to facilitate examinations:
- Evidence files
- Case files and backups
- Configuration files

Day 2

Day two 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. Participants employ the use of file signature analysis to properly identify file types and to locate renamed files. Students are then provided instruction on the principal and practical usage of hash analysis tools such as EnScript™ programs and other utilities. 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 by learning how to utilize the EnCase Evidence Processor to run modules on evidence files to obtain results that are reviewed during subsequent lessons.

The main areas covered on day 2 include:

- Learning of acquisition concepts
- Incorporating the use of installed external viewers used by examiners into EnCase
- 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
- Identifying and adapting time zones within EnCase
- 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

Students start the day with a lesson regarding data allocation and file descriptions. Next, attendees 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 backup the case with customized settings and bookmark items for reporting purposes. Participants then will run a raw searching process and will have a lesson on GREP operators. Attendees will then perform index queries and will finish the day with an exercise to practice their newly learned searching and bookmarking processes.

The main areas covered on day 3 include:

- Understanding concepts of data allocation and EnCase
- object descriptions
- Tagging and bookmarking data for inclusion in the final report
- Creating and conducting and 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 tuition begins with the participants learning how to create a hash library, containing hash sets, and hash values to identify notable files and to exclude known files from an evidence file. Following, the students will learn the definition of entropy and how it can be helpful during the forensic analysis. The attendees 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.

The main areas covered on day 4 include:

- 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 EnCase to the local file
- system using different methodologies within EnCase, 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