

FOUNDATIONS IN DIGITAL FORENSICS

Course Name:	DF120 - Foundations in Digital Forensics with EnCase
Dates and duration:	1-4.10.2019 (from Tuesday to Friday), 4 Days
Time:	9:00 to 17:00
Location:	Difseco Oy training centre at Westendinkatu 7, 021600 ESPOO, Finland
Description:	<p>This hands-on course involves practical exercises and real-life simulations in the use of OpenText™ EnCase™ software (EnCase). The class provides participants with an understanding of digital forensic technic may be used to examine data related to an incident response, an employee misconduct investigation, and/or a law enforcement criminal and/or civil investigation. Participants create cases using EnCase, configure the application to maximize its utilization, and learn evidence acquisition concepts and how to validate the data collected. Instruction progresses to the analysis of the data whether related to criminal investigations, cybersecurity incidents, or other matters. The course will cover techniques, such as keyword or indexed searching along with hash analysis. Participants will learn how to bookmark, export, and create reports relating to examination findings. The course concludes with instruction on archiving, validating the data, and restoring the case.</p>
Audience:	Digital forensic investigators, including law enforcement, government, military, corporate, ITsecurity, and litigation support professionals. Participants may have minimal computer skills and may be new to the field of computer forensics.
Additional Information:	Coffee, tea, refreshments and full lunch are provided free of charge

Course price: 2.399,00 EUR (vat 0%)

Students attending this course will learn the following:

- The EnCase digital forensic methodology
- How to navigate the EnCase interface
- How to extract data and files from your evidence
- How to bookmark evidence files, file sets, and data structures
- How to conduct raw and index searches
- How to analyze file signatures and view files
- How to conduct hash and entropy analyses and import hash sets
- How to import and export data to and from Project VIC
- How to install external file viewers to EnCase
- How to prepare reports, using templates provided with EnCase
- How to create a report template
- How to restore evidence
- How to archive files and data created through the analysis process
- The proper techniques for handling and preserving evidence

BUILDING AN INVESTIGATION

Course Name:	DF210 - Building an Investigation with EnCase
Dates and duration:	8-11.10.2019 (from Tuesday to Friday), 4 Days
Time:	9:00 to 17:00
Location:	Difseco Oy training centre at Westendinkatu 7, 021600 ESPOO, Finland
Description:	<p>This hands-on course is designed for investigators with solid computer skills, prior computer forensics training, and experience using OpenText™ EnCase™ Forensic (EnCase). This course builds upon the skills covered in the DF120 – Foundations of Digital Forensics course and enhances the examiner's ability to work efficiently through the use of the unique features of EnCase. This course will build an investigation using analysis techniques, such as recovering volumes, registry analysis, and examining compound files. The course progresses through the analysis of Windows artefacts, shortcut link files, Recycle Bin, stored internet data, and email. This course will assist criminal, corporate, and cybersecurity analysts.</p>
Audience:	Digital forensic investigators, including law enforcement, government, military, corporate, ITsecurity, and litigation support professionals. Participants may have minimal computer skills and may be new to the field of computer forensics.
Additional Information:	Coffee, tea, refreshments and full lunch are provided free of charge

Course price: 2.399,00 EUR (vat 0%)

Focusing on commonly conducted investigations, students will learn about the following:

- How to recover encrypted information particularly that which was encrypted using Windows BitLocker™
- How to locate and recover deleted partitions
- Students will learn how to deal with compound file types
- Students will learn about the Windows® Registry
- How to determine time zone offsets and properly adjust case settings
- How to create and use conditions for effective searching
- Students will learn how to use the EnCase™ Evidence Processor
- Students will gain an overview of the FAT, ExFAT, and NT file system
- How to conduct keyword searches and advanced searches using GREP
- The differences between single and logical evidence files and how to create and use of logical evidence files
- How to identify Windows operating system artifacts, such as link files, Recycle Bin, and user folders
- How to recover data from the Recycle Bin
- How to recover artifacts, such as swap files, file slack, and spooler files
- How to conduct a search for email and email attachments
- Students will learn how to examine email and Internet artifacts
- How to identify and recover data relating to the use of removable USB devices