DF310-ENCE® PREP WITH ENCASE® FORENSIC 8

Syllabus

This course is designed as a review of the skills that are applicable to the EnCE certification process taught during the Foundations of Digital Forensics and Building an Investigation courses. The emphasis throughout the course is to prepare the students to successfully complete the Phase I and Phase II EnCE of the certification examination. The instruction is intended as a review of previously delivered material and is purposely not as in-depth as that provided during the full-length courses. This course should not be construed as a replacement for the full-length Foundations of Digital Forensics and Building an Investigation courses and, due to the pace at which this class runs, basic experience using EnCase Forensic is encouraged.

Day 1

Day one starts with an introduction to the EnCase® Forensic Version 8 (EnCase) and examination methodology. Attendees review the techniques for creating a case and working within the EnCase environment then walk through the steps for acquiring an evidence file, working with single files and creating EnCase logical evidence files. Discussions of the concept of digital evidence and how computers work (paying particular regard to the associated impact on forensic examination) are also included. Attendees are provided instruction on the use of the EnCase® Evidence Processor and participate in a discussion of the FAT, exFAT and NT file systems. The day's instruction concludes with the auditing of a physical device, including the examination, identification, and recovery of logical disk structures.

The main areas covered on day one include:

- EnCase Forensic concepts and acquisitions
  - EnCase methodology
    - Creating an EnCase case file
    - Navigating within the EnCase environment
  - EnCase Forensic concepts
    - Structure and function of EnCase evidence files, case files and configuration files
    - Examination of live and acquired evidence using EnCase Forensic
  - EnCase acquisition concepts
    - Understanding the concept of digital evidence and its impact on an investigation
    - Safeguarding, handling, and preserving evidential data

      The basic techniques of acquiring a forensically sound copy of data from a thumb drive or other removable disk
    - Creation of EnCase logical evidence files from single files or acquired evidence
  - Using the EnCase Evidence processor
- Data allocation and file systems
  - Identification of physical and logical disk and file structures
  - Disk allocation units
  - EnCase description and display of objects
  - Introduction and basic functions of the NTFS, FAT, and ExFAT file systems
  - Auditing physical disk allocation and recovering logical structures with EnCase

Day 2

Day two begins with reviewing functionality and use of EnCase Forensic to efficiently examine digital evidence. The day starts with a review of performing signature and hash analyses of data in EnCase. We continue instruction with the installation of external viewers within EnCase, identifying and viewing the structure of compound files, and copying data out of an EnCase evidence file. Instruction then moves to searching evidence in EnCase, including the use and differences in raw searches and index searches and keyword development. Searching tuition continues with the examination of unallocated clusters and the implementation of the EnCase GREP operators in raw searches. As part of this instruction block, the concepts of bookmarking swept, single, multiple items, and structured items as well as EnCase tagging are reviewed. The day concludes with the first block of instruction of examining data in EnCase, being a review of the Windows registry.

The main areas covered on day two include:

- EnCase functions
  - Signature analysis
    - An automated comparison of the displayed file extension with the actual content of the file
  - Hash analysis
    - Creating hash libraries and hash sets in EnCase
    - Adding hash values to the hash sets and library
    - Using hash values to identify/exclude files without visually examining each one
  - Installing and using external viewers
  - Detailed copy options within EnCase
- Searching evidence in EnCase
  - Advanced search techniques using index and raw searching in EnCase
    - Creating keyword for raw searching
    - Implementing physical and logical raw searching with EnCase
    - Using GREP operators within EnCase to construct advanced search terms
    - Creating advanced index search terms to quickly locate responsive data in data and metadata
    - Using index operators to further create robust search terms
    - Saving and working with search terms and results
  - Compound file examinations
    - Viewing the structure and searching of compound files
    - Pitfalls of not examining compound files properly
- Examining evidence with EnCase
  - Windows registry
    - Location of the Windows registry hives and their function
    - Elements of the Windows registry
      - » Registry keys (folders) and values
      - » Registry value types
    - Location of system time zone settings
    - Setting the time zone in EnCase

Day 3

Instruction on day three continues with examining data in EnCase. The day begins with discussing the location and function of common Windows artifacts that often provide vital information to investigations. We then take a closer look at the function and structure of Windows link files (shortcuts), identifying critical locations within the structure to gather intelligence information for the link file's respective target. Attendees will also review the function of the Windows Recycle Bin, including the impact to the file system and associating the Window's Security Identifier to a named user account. Examining data in EnCase continues with examining and bookmarking email, Internet history, and cache content, concluding with the exploration and identification of removable USB devices used on a Windows computer. The course concludes with hands-on instruction in the creating, editing, and exporting a report in EnCase.

The main areas covered on day three include:

- Examining evidence with EnCase (continued)
  - Windows artifacts
    - User-account information and associated data
    - System folders and files of interest
  - Link files
    - Deconstructing link files to reveal internal structures relating to their target files
  - Recycle Bin recovery
    - Examination of the Recycle Bin, its properties, and function
    - Linking Recycle Bin data to the associated user
    - Registry entries controlling operation of the Recycle Bin
  - Email/Internet examination
    - Examining email and methods available within EnCase to locate and parse email data stores
    - Navigating email, including different view modes in EnCase and locating email attachments
    - Identifying email conversations and their related messages
    - Exploring the results of activity on the Internet, including cookies, history, web cache, and bookmark data
  - Removable USB device identification
  - USB devices and the function of the USB device descriptor
    - Removable USB device information retained by Windows
- Reporting with EnCase
  - Create, edit, and export an examination report using EnCase
  - Hands-on reviewing of editing the report template and saving as an EnCase template for use in future investigations.

GUIDANCE SOFTWARE™

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.