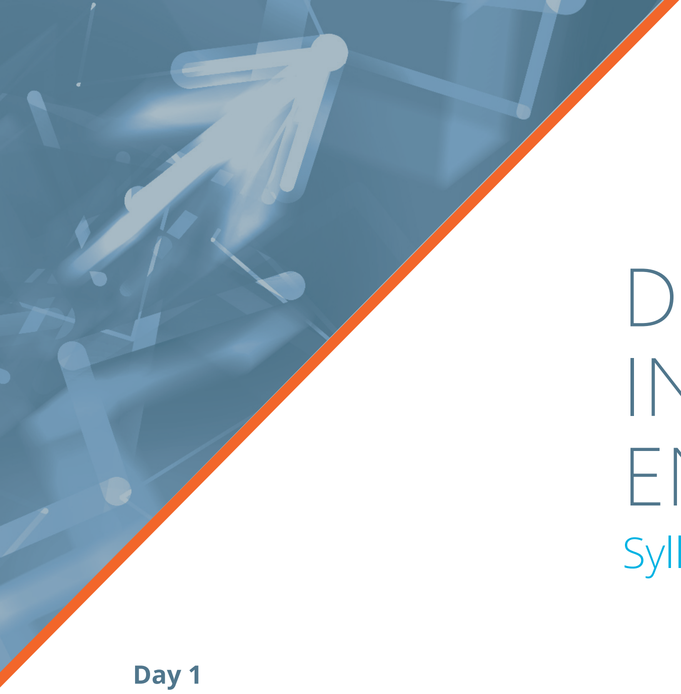

GUIDANCE SOFTWARE

DF210—BUILDING AN INVESTIGATION WITH ENCASE® FORENSIC

Syllabus

Day 1

Day one starts with an overview of the EnCase Forensic version 8 environment. The students then learn how to collect encrypted information by examining files encrypted with Windows® BitLocker™. Attendees go on to study the Master Boot Record partitioning model and deleted partition recovery. Instruction continues with an examination of compound files. Their structures are explored and issues surrounding their examination are discussed. Students move on to explore a very important type of compound file structure, the Windows® Registry hive file. They explore mounting and examining these files and learn the relationship of the hive files to the structure of the Registry in its online state. Students then progress to examining the time zone information contained within the Registry, its importance to their case, and how they apply it in EnCase Forensic. The students are provided intermediate-level instruction concerning instruction regarding the methods for creating conditions to filter data. Next the students are provided with an overview of the Evidence Processor and the processing of the Malone case, which will be used throughout the rest of the course.

The main areas covered on day one include:

- Review of EnCase Forensic case creation and adding evidence
- Examining data encrypted with BitLocker
- Understanding the Master Boot Record partitioning scheme
- Principles of attempting to recover data lost through the partitioning process
- Partition recovery
- Compound files
  - Mounting and searching compound files
  - Documenting data contained within these compound files
  - Pitfalls of not examining compound files properly
- Windows Registry
  - Elements of the Registry
  - Registry keys (folders) and values
  - Registry value types
- Locating and mounting the Registry hive files
- Examination of time zone settings with the Registry
- Applying time zones within EnCase Forensic
- Using conditions to filter data
- Evidence Processor overview

Day 2

Day two begins with instructions about the FAT, ExFat, and NT file systems and then the students will participate in a practical exercise, examining all three files systems and their differences. The course continues with the use of the GREP operator functionality of EnCase Forensic to perform advanced searches. Single-file functionality as well as the value of logical evidence files are explored. A practical exercise and review follows with the processing of our second case, which concludes the instruction for the day.

The main areas covered on day two include:

- FAT, ExFAT, and NT Files Systems
- Using the GREP operators within EnCase Forensic to construct advanced search terms
- Suitability of GREP, proper syntax, and potential results
- Single files and logical evidence files

Day 3

Day three focuses upon specific analysis of common artifacts that often provide vital information to investigations. These specific areas reveal data that can provide a clearer indication of user activities. Students will explore the methods that EnCase Forensic offers to provide detailed information to the examiner. The final lesson for day three is focused on identifying, locating, and recovering email message and attachments.

The main areas covered on day three include:

- Advanced search techniques
- Windows artifacts
  - User account information and associated data
  - System folders and files of interest
  - Thumbnail cache files
  - Windows 7 specific artifacts
  - Folder structure and the effect of junctions (folder mount points)
  - User/administrator privileges and impact on storage of data
  - Links and Library folder content
  - System files

Day 3 Continued

- Shortcut or link files
  - Deconstructing link files to reveal internal structures related to their target files
  - Using link files to help determine drive letter assignment
- The Windows Recycle Bin
  - Linking Recycle Bin data to the associated user
  - Registry entries controlling operation of the Recycle Bin
  - Examination of the Recycle Bin, its properties, and function
  - Exploring the way the Recycle Bin is implemented under
- Print spooler recovery
  - Understanding the printing process and associated files
  - Recovery of SPL and SHD files as well as understanding and extracting the graphical and metadata they contain
- Email and Internet history
  - Examining both client-based and web-based email and methods available within EnCase Forensic to locate and parse email data stores
  - Recovering and analyzing email attachments

Day 4

Day four begins with instruction on examining various Internet artifact and moves on to how the data located on removable USB devices can be examined and recovered. The students will then participate in a practical exercise focusing on these skills. The week of instructions concludes with a final practical exercise that provides the student with a hands-on review of all the tuition dispensed during the course.

The main areas covered on day four include:

- Internet artifacts
- Removable USB device identification

About Guidance Software

At Guidance, we exist 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. Makers of EnCase®, the gold standard in digital investigations and endpoint data security, Guidance provides a mission-critical foundation of applications that have been deployed on an estimated 25 million endpoints and work in concert with other leading enterprise technologies from companies such as Cisco, Intel, Box, Dropbox, Blue Coat Systems, and LogRhythm. Our field-tested and court-proven solutions are used with confidence by more than 70 of the Fortune 100 and hundreds of agencies worldwide. Get to know us at guidancesoftware.com.