opentext™

Training overview

DF410 NTFS Examinations with EnCase

Training facilities

Los Angeles, CA (Pasadena, CA)
1055 East Colorado Boulevard
Suite 400
Pasadena, CA 91106-2375

Washington, DC (Gaithersburg, MD)
9711 Washingtonian Blvd
6th floor, Room 601 (Paris Room)
Gaithersburg, MD 20878

London, UK (Reading)
420 Thames Valley Park Drive
Earley, Reading
Berkshire
RG6 1PT

For a complete listing of locations, including Authorized Training Partners around the world, please visit
opentext.com/encasetraining

EnCaseTraining@opentext.com
opentext.com/encasetraining

Syllabus

Day 1

Day one begins with an introduction to the new technology file system (NTFS), its notable features and the reasons for its introduction. Students then examine the role played by NTFS on both BIOS and UEFI systems during the Windows® boot process. Following this, students study the various Windows partitioning methods, with a focus on how drive letters are mapped in conjunction with the Windows Registry. Finally, students examine the NTFS volume creation process and the purpose/structure of the NTFS Volume Boot Record (VBR). A practical exercise reinforces their knowledge.

Day 1 will cover:

- An introduction to the New Technology File System (NTFS), as well as the Common Log File System (CLFS) layered above NTFS in later versions of the Windows operating system.
- Windows device and device-driver information stored in the Windows Registry, including the time of first and last connection and how certain removable disks store encryption passwords in the user's Registry using the Windows Data Protection application programming interface (DPAPI).
- The Windows boot process on both BIOS and UEFI systems, including the purpose and structure of the Boot Configuration Database (BCD).
- Master Boot Record (MBR), GUID Partition Table (GPT) and dynamic disk structures, including Windows Registry drive-letter mapping.
- The purpose and structure of the NTFS Volume Boot Record, as well as the NTFS volume creation process.

Day 2

Day two commences with a lesson on the purpose of the internal NTFS system/metadata files, as well as an overview of the Master File Table (MFT), its records and record attributes. The day continues with an analysis of the Standard Information, Filename, Volume Name and Volume Information MFT record attributes, including their significance during digital investigations. Two practical exercises and a quiz will help students remember their new-found technical knowledge.

Day 2 will cover:

- An overview of the NFTS metadata files, paying particular attention to $LogFile, $Attrdef and $, (the NTFS root directory).
- The location, purpose and structure of the Master File Table (MFT) and MFT Zone.
- The purpose and structure of MFT records, paying specific regard to the structure of the MFT record header, MFT record reuse, MFT record validation, base vs. extension MFT records, MFT record slack and the potential significance of the MFT record end marker when written by non-Microsoft NTFS implementations.

opentext™

- The purpose and structure of MFT record attributes and attribute headers, including the reason for the padding bytes contained therein, as well as the significance of the instance number associated with each one.
- The purpose and structure of the NTFS Standard Information attribute, with a focus on the timestamps it contains and when they are updated, as well as the meaning and effect of NTFS tunneling.
- The purpose and structure of the NTFS Filename attribute, including the nature/validity of data also to be found in the Standard Information or Data attributes and the significance of the Filename Attribute when recovering deleted NTFS files and folders and why some such files may be identified as lost.
- The purpose and structure of the NTFS Volume Name and Volume Information MFT record attributes.

Day 3

The start of day three focuses on how the NTFS Data attribute is used to store the data belonging to small files, as well as how it tracks the clusters containing the data belonging to larger ones. This is followed by an examination of the NTFS Attribute List attribute and the part it plays in tracking the extent of highly fragmented files. Students will then complete a substantial practical exercise, which challenges them to use what they have learned to perform advanced recovery of a fragmented file from an overwritten NTFS volume. The last two lessons on day three detail the purpose and structure of NTFS alternate data-streams and the operation and structure of reparse points, which allow NTFS folders to act as mount-points for other folders, volumes or external data. Additional practical exercises help strengthen the students' understanding throughout the day.

Day 3 will cover:

- The purpose and structure of the NTFS Data attribute and how it usually contains the data belonging to small files, as well as how it references the clusters used to store the data belonging to larger files.
- What happens when a small file grows too large for its data to be stored in its MFT record and the effect of the NTFS Encrypting File System (EFS) on where file data is stored.
- The difference between virtual cluster numbers (VCNs) and logical cluster numbers (LCNs).
- Purpose and structure of the NTFS Attribute List attribute.
- The purpose and structure of NTFS alternate data streams.
- The purpose and structure of NTFS reparse points, including junctions and volume mount points.

Day 4

Day four starts with study of the structure and analysis of NTFS Update Sequence Number (USN) change-journal records and their considerable value during digital investigations. This is followed by an examination of NTFS folders and the filename index-records they contain. A subsequent lesson discusses file/creation deletion and the potential for recovering index records relating to deleted files and folders. Students then examine how the object IDs stored in NTFS Object ID MFT record attributes are used to uniquely identify/track shortcut-link-file targets. Day four concludes with lessons documenting NTFS compression and the storage of user-account information and NTFS file-system permissions. The course closes with a final practical exercise encompassing all of the material.

Day 4 will cover:

- The purpose, location and structure of the NTFS USN change-journal and the records it contains.
- Using an EnScript application to parse current change journal records, as well as those from unallocated clusters and $LogFile
- The purpose and structure of the NTFS Index Root MFT record attribute associated with all NTFS folders, the Index Allocation MFT record attribute associated with large NTFS folders (including the index-buffers referenced thereby) and the structure of NTFS index entries.
- The consequences of file creation/deletion, focusing on the recovery of index records relating to deleted files and folders.
- Shortcut ink file creation and behavior, the purpose and structure of the NTFS Object-ID MFT record-attribute, the purpose and structure of the NTFS $ObjId file and the mode of operation of the Windows Link Tracking Service (LTS).
- NTFS compression.
- User accounts and security groups, as well as the purpose and content of the NTFS $Secure file and the security descriptors it contains.

opentext.com/contact