opentext™

Training overview

DF410 NTFS Examinations with EnCase

Syllabus

Day 1

The day begins with an introduction to the new technology file system (NTFS) data structures. Students are introduced to the methods used to store binary data on a computer system and use this information to interpret multi byte values throughout the week. The day closes with breaking down the NTFS Volume Boot Record. Practical exercises throughout the day give students the chance to use their new skills and knowledge.

Day 1 will cover:

- NTFS introduction
- History of the new technology file system (NTFS)
- Introduction to NTFS and its features
- Integer Interpretation
- Understanding how to convert binary and hex values to decipher the information stored within the NTFS
- NTFS disk structures
- Understanding how disks are split into sectors and file systems' group sectors into clusters
- Limitations of FAT and NTFS file systems
- Understanding the contents and structure of the master boot record (MBR) and the master partition table (MPT)
- Identifying the different storage structure available with NTFS
- NTFS Volume Boot Record
- Understanding how an active NTFS partition is involved in the boot process
- NTFS volume creation
- Initialization, partitioning and formatting processes associated with disk drives on an NTFS system
- Identifying the internal file system files that are written to the disk during processes
- Understanding the associated artifacts folders created/maintained by the different NT based operating systems

opentext™

Day 2

Day two begins with a discussion on the purpose of the internal system/metadata files and a background of the master file table (MFT). We continue with the discussions covering the standard, filename, volume and data attributes. Students determine what attributes exist within records and break down the information stored within each. Resident and non-resident files are discussed in terms of their administrative storage and recoverability potential.

Day 2 will cover:

- NFTS metadata files
- Identifying the internal metadata files used by NTFS
- Configuring relevant text styles to better analyze the data contained in each file
- Overview of the internal files, including $MFT, $LogFile, $Secure, $Quota, $Bitmap, $AttrDef and $UsnJrnl
- Recovering $USNJournal records from unallocated clusters
- The master file table
- Understanding the purpose and content of the $MFT
- Locating the $MFT within a volume
- Describing, locating and identifying the MFT zone
- Understanding the $MFT record anatomy
- $MFT record headers
- Identifying and decoding the information contained within an MFT record header
- Understanding how an $MFT record is reused once an object is marked for deletion
- Attribute headers
- Resident and non-resident $MFT data
- Standard information attribute (SIA)
- Identifying the SIA, decoding its length and identifying and decoding the SIA data stream
- Filename attribute
- Identifying the filename attribute, decoding its length and identifying and decoding the FNA data stream
- Volume attribute
- Locating and decoding volume attributes, recovering information such as the volume name, NTFS version and by which manner the volume was unmounted

Day 3

Day three begins with instruction on resident and non-resident data and moves on to identifying data attribute streams. Students learn about NTFS compression, NTFS encryption and using the OpenText™ EnCase™ Decryption Suite module to access encrypted data.

Day 3 will cover:

- Data attribute
- Identifying the data attribute by its header and parsing it to identify if the attribute stream (the files data) is resident or non resident
- Alternate data streams
- Identifying alternate data streams and explaining how they are linked to a file by multiple MFT data attributes and examining that data using EnCase software
- Understanding how NTFS handles data compression and sparse files
- Encrypted file system (EFS)
- Understanding the encrypting file system and the differences under Microsoft® Windows® 2000 and Windows XP/2003/ Vista/2008
- Identifying EFS data and recovering plain-text temporary versions of encrypted files
- Cracking EFS encrypted data
- Using EnCase Decryption Suite to decrypt data

Day 4

Day four exposes participants to the NTFS directory structure. Students will identify the directory structure using manual methods as well as an EnScript™ module. Participants will also be introduced to NTFS security identifiers and their forensic value.

Students will examine link files that contain Object IDs, including details about their creation and modification. Participants then learn to detect reparse points and will complete a final comprehensive practical exercise.

Day 4 will cover:

- Identifying reparse/mount points and where they link to a disk volume
- NTFS directories
- Understanding the indexing structure within an NTFS volume
- Identifying and decoding various data structures involved
- Examining MFT records associated with NTFS folders

opentext™

- Identifying MFT record entries relating to folders with both resident and non-resident index streams and locating the relevant index buffers
- Understanding the details of activity when an NTFS file is created and deleted
- NT local user accounts
- Understanding where local account information and Windows domain account information are stored
- Understanding the significance of the SAM Registry hive file
- Mounting the SAM Registry hive file and manually parsing user and group information that it contains
- Link files and object ID
- Understanding the purpose of shortcut link files and how and where they are created

opentext.com/contact