opentext™

Training overview

DF420 Macintosh Examinations with EnCase

Training facilities

Ondata International SL
Avenida de Brasil 17, planta 3
28020, Madrid
Tel. 91 417 4468
sales@ondata.es
https://www.ondata.es

Syllabus

Day 1

The first day of the course begins with instruction on the forensic acquisition of data from Mac® disks, Mac partition and volume structure and an in-depth analysis of how file data is stored within HFS+ volumes.

Day 1 will cover:

- Issues associated with the forensic preservation of Macintosh® on-disk data
- Acquisition methods using direct connection, Target Disk Mode and forensic boot disk
- The Macintosh boot process and how the examiner can ascertain the accuracy of the Mac hardware clock
- The structure of Mac on-disk data and low-level information regarding the Apple Map and GUID Partition Table (GPT) partitioning schemes
- The impact of Apple's implementation of GPT as opposed to that used by Microsoft® Windows®
- The structure of HFS+ volumes
- A comparison of the features associated with HFS and HFS+ volumes
- HFS+ volume layout and header structure
- Recovery of intact but deleted HFS+ partitions using OpenText™ EnCase™ software
- An overview of file storage on HFS+ volumes and the use of data and resource forks
- An introduction to the Catalog, Extents Overflow, Allocation, Attributes and Startup HFS+ internal files
- The structure of the Catalog file
- The concept of HFS+ b-tree files and how the b-tree nodes in the Catalog file are used to index and store HFS+ file and folder records
- Locating and examining the structure of Catalog file and folder records manually and by using EnScript™ modules

opentext™

Day 2

The second day starts with instruction on the Extents Overflow file structure. Following this, the class will participate in a group exercise, demonstrating how they can use their new knowledge to recover a deleted, fragmented movie-clip file from a deleted HFS+ partition on a GPT Mac disk, one that has been repartitioned as a Master Boot Record disk. This is followed by material relating to the Apple File System (APFS) and a group exercise demonstrating the use of the APFS checkpoints to recover deleted file-system metadata relating to a deleted file. The day will progress with a look at fundamental aspects of Mac OS® operation.

Day 2 will cover:

- The structure of the Extents Overflow file
- An examination of how HFS+ uses this special file to manage highly fragmented files, i.e., those with more than eight file extents
- Manually locating and decoding additional file extents in the Extents Overflow file
- An introduction to APFS, including a discussion of notable APFS features and their impact on forensic examinations
- An outline of the forensic impact of SSD storages, including TRIM operations
- The use of EnScript programs to visualize and explain the on-disk APFS data interpreted by EnScript
- Data recovery using APFS checkpoints
- An examination of some fundamental aspects of Mac OS that are likely to play a part in any Macintosh examination
- Basic Mac OS volume structure, including file system domains used to organize folders on a Mac HFS+ system volume
- The purpose and contents of the special Library folder
- The structure and installation of Mac OS applications
- The structure, content and examination of XML and binary-format property list (plist) files, including the recovery of binary plist files from unallocated clusters
- The structure and nature of aliases and a comparison with Microsoft Windows shortcut link files
- The structure of symbolic links and hard links
- File-system permissions and how they are linked to the account information stored in Open Directory
- Mac OS user-login information, passwords and password recovery
- Access control lists (ACLs)
- Additional Mac OS security information relating to the use of the guest and root user accounts
- Handling of HFS+ compressed data in EnCase

Day 3

The day will begin with instruction regarding Macintosh disks and disk images. The next lessons will look at the Mac OS system and user artifacts. The students will participate in practical exercises throughout the day to reinforce the learned techniques.

Day 3 will cover:

- Examination of Macintosh disks and disk images using the examiner's own forensic Macintosh computer
- The need for this type of examination
- Instruction with regards to the Disk Arbitration Framework, the consequences of it on forensic disk examination and how it may be disabled
- A look at Mac disk-image files, how they are created and how they can be examined
- Identification of encrypted disk images
- Understanding and viewing Mac OS keychain files both within EnCase on a Mac and under Microsoft Windows
- Decrypting disk images in EnCase using the user's password
- Understanding the nature of File Vault 1 and the forensic methodologies that are available to deal with it
- Instruction regarding the forensic acquisition of decrypted File Vault 2 images using the user's password
- Understanding the options available to allow EnCase evidence files to be mounted on an examiner's Macintosh computer, including the use of PDE in conjunction with iSCSI
- A discussion of the methodologies available to boot a forensic disk image as a virtual Macintosh machine
- An examination of the Mac OS operating system artifacts associated with the system as a whole rather than a specific user
- Operating system version, installation and update information
- Log files, network and firewall configuration
- Time-zone settings
- User account configuration, including log-in settings and deleted user accounts
- Trash settings

opentext™

Day 3 *(cont.)*

- Evidence of connected Bluetooth® devices
- The operation of Time Machine® and the examination of its data
- Location and content of the swap and hibernation files
- A review of user-specific Mac OS operating system artifacts
- Recently accessed servers, documents, applications, folders, removable media and hosts
- The structure and nature of bookmarks in comparison with aliases
- Understanding the operation of the Quick Look thumbnail cache and the extraction of the thumbnails contained therein
- Spotlight® operation and artifacts, including examination of Spotlight metadata during a forensic examination
- Understanding the contents of the HFS+ $Attributes file and examination of the extended attributes that it contains
- Understanding and parsing Apple Double files
- Recently accessed folders
- Identifying the contents of a user's Dock
- Printer artifacts, including the use of EnScript programs to decode Common UNIX® Printing System (CUPS) printer control files
- User-specific log files

Day 4

Day four's activities begin with a group exercise relating to User artifacts discussed on Day 3. This is followed by an examination of the data associated with Mac applications and their associated artifacts. Instruction continues with a lesson on Mac internet activity. The course concludes with a practical exercise that focuses on the last day's curriculum.

Day 4 will cover:

- An examination of Mac OS application artifacts
- Mac OS application structure, icons and data, including application cache data
- Understanding and examining sandboxed application data
- Locating and recovering auto-saved file data and the previous versions of files
- Location and examination of iCloud® documents
- An examination of application and configuration data, including SQLite data, where applicable, associated with common Mac OS applications, such as Address Book, Calendar, FaceTime®, iTunes® and more
- Recovery of Digital Rights Management (DRM) data from media files purchased from the iTunes store
- Operation of Photos and the extraction and mapping of Global Positioning System (GPS) data from digital pictures
- An examination of internet-related Mac OS application
- Safari® configuration settings, cache content, internet history, downloads, web page previews, bookmarks, cookies, top sites, session data, form data, cached log-ins credentials and Spotlight metadata
- Location of Firefox® data
- Location and examination of Mail (the default Mac OS email application), Thunderbird® and Microsoft® Outlook® email data
- Location and examination of data associated with Messages (formerly iChat®) and Skype®