DF420 Mac Examinations with OpenText Forensic (EnCase)

Syllabus

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

Munich, Germany
Technopark 2 Werner-von-Siemens-Ring 20 Munich (Grasbrunn) Grasbrunn D-85630 Germany

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

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. 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. A practical exercise concludes the activities on day one, which will continue at the start of day two.

Day 1 will cover:

- Issues associated with the forensic preservation of Mac on-disk data.
- Acquisition methods using direct connection, Target Disk Mode, forensic-boot disk, RecoveryOS, and the OpenText™ Forensic EnCase, and OpenText™ Endpoint Investigator agents.
- The Mac 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.
- An introduction to Mac file systems and how both HFS+ and APFS use b-trees to store file-system records.
- 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 the OpenText Forensic (EnCase)/OpenText Endpoint Investigator 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.
- Locating and examining the structure of Catalog file and folder records manually and by using EnScript modules.

Day 2

Instruction on the second day starts with material relating to the Apple File System (APFS) and a group exercise involving recovery of a deleted movie-clip file from a deleted, overwritten APFS partition. The day will progress with a look at fundamental aspects of Mac OS® operation.

Day 2 will cover:

- 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 OpenText Forensic (EnCase) software.
- The potential for recovering redundant APFS file-system data including that from APFS snapshots.
- An examination of some fundamental aspects of Mac OS that are likely to play a part in any Macintosh examination.
- Basic Mac OS folder structure, including the use of file-system domains to group relevant data.
- APFS volume groups, signed system volumes, and firmlinks.
- The purpose and contents of the special Library folder.
- The structure, content, and examination of XML and binary-format property list (plist) files, including the recovery of binary plist files from unallocated clusters.
- Mac OS applications and their sandbox, iCloud®, Darwin, and group-container folders.
- 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+ and APFS compressed data in OpenText Forensic (EnCase).

Day 3

Day 3 will begin with instruction on Mac 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 Mac disks and disk images using the examiner's own forensic Mac computer.
- The need for this type of examination and the effects of Intel T2 and Apple Silicon Macs.
- Instruction with regards to the Disk Arbitration Framework, its consequences 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 OpenText Forensic (EnCase) on a Mac and under Microsoft Windows.
- Decrypting disk images in OpenText Forensic (EnCase) using the associated password and/or keychain credentials.
- 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 OpenText Forensic (EnCase) evidence files to be mounted on an examiner's Mac computer, including the use of PDE in conjunction with iSCSI.
- A discussion of the methodologies available for booting a forensic disk image as a virtual Mac machine.
- Instruction regarding the identification, operation, and examination of MacOS software RAID.
- 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 (including unified logs, KnowledgeC, and BIOME/SEGB), network, and firewall configuration.
- Time-zone settings.
- User account configuration, including log-in settings and deleted user accounts.
- Trash settings.
- The operation of Time Machine® and the examination of its data.
- Evidence of connected Bluetooth® devices.
- A review of user-specific Mac OS operating system artifacts.
- Recently accessed servers, documents, applications, folders, removable media, and hosts.
- Understanding the operation of the Quick Look thumbnail cache and the extraction of the thumbnails contained therein.

- Reading/locating extended file-system attributes including folder/file tags, comments and custom icons.
- Understanding and parsing Apple Double files.
- Spotlight® operation and artifacts, including examination of Spotlight volume and user metadata during a forensic examination.
- Recently accessed folders.
- Identifying the contents of a user's Dock; also, the applications set to auto-start thereby.
- 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.
- 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.
- 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®).