EnCase® Examinations of Macintosh and Linux Operating Systems

Course Syllabus

Day 1

The first day of the course will start with an introduction, history, and development of Apple, Macintosh, and Mac OS. It will also outline the philosophy behind the course and discuss the need to possess a Mac in order to examine a Mac. This will be followed by tuition concerning 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 one's instruction will cover:

- **Apple and Mac history**
- **Course purpose, content, and methodology**
- **Necessity to possess a Mac in order to examine Mac data**
- **Issues associated with the forensic preservation of Macintosh on-disk data**
  - Acquisition methods utilizing direct connection, Target Disk Mode, and forensic boot disk
  - The Macintosh boot process and the ways in which 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**
  - Impact of Apple's implementation of GPT as opposed to that used by MS Windows®
- **The structure of HFS+ volumes**
  - Comparison of the features associated with HFS and HFS+ volumes
  - HFS+ volume layout and header structure
  - Recovery of intact but deleted HFS+ partitions using 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

Day 2

Instruction on the second day will start with the continuation of the Catalog file structure lesson and move onto tuition about the Extents Overflow file structure. Following that, the class will participate in a group exercise, demonstrating how the knowledge gained on the first day can be used to recover a deleted, fragmented movie-clip file from a deleted HFS+ partition on a GPT Mac disk that's been repartitioned as a Master Boot Record disk. This will then be followed by a look at fundamental aspects of Mac OS X operation, Mac OS X disk, and disk-image access.

Day two's instruction 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 8 file extents
  - Manually locating and decoding additional file extents in the Extents Overflow file
- **An examination of some fundamental aspects of Mac OS X that are likely to play a part in any Macintosh examination**
  - Basic Mac OS X volume structure; the use of 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 X 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 MS 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 X user-login information, passwords, and password recovery
  - Access control lists (ACLs)
  - Identification of HFS+ compressed data (introduced with Snow Leopard) and the storage of a file's compressed data in its resource fork of the special HFS+ Attributes file
- **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
  - Examination of encrypted disk images, including detailed information about FileVault, the structure, content, and examination of keychains and the options for decrypting a FileVault container using either the associated user's password or the FileVault Master Password

Day 2 cont'd

- Instruction on the forensic mounting and acquisition of Mac disk image files, issues associated with the acquisition of sparse image files, shadow mounting (mounting a disk image with simulated read/write access), the conversion of EnCase® evidence files to Mac disk image format, and finally, the options for live examination of a target Mac OS X operating system

Day 3

Instruction regarding Macintosh disks and disk images continues on day three. The next lessons will be concerned with Mac OS X system and user artifacts. Day three's activities conclude with an examination of the data associated with Mac applications and their associated artifacts.

Day three's instruction will cover:

- **An examination of the Mac OS X 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 login settings and deleted user accounts)
  - Trash settings
  - Evidence of connected iPhone, iPad, and iPod devices as well as 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 X operating system artifacts**
  - Recently accessed servers, documents, applications, folders, removable media and hosts
  - The structure and nature of bookmarks in comparison with aliases
  - Spotlight operation and artifacts; examination of Spotlight metadata during a forensic examination
  - Dock configuration and content
  - Desktop wallpaper and screensaver configuration
  - Saved searches
  - Web and file sharing
  - Printer artifacts (including the use of EnScript® programs to decode Common UNIX Printing System (CUPS) printer control files)
  - User-specific log files
- **An examination of Mac OS X application artifacts**
  - Mac OS X application structure, icons and data; application cache data
  - An examination of application and configuration data (including SQLite data, where applicable) associated with common Mac OS X applications, such as Address Book, iCal, iTunes, and more.
  - Recovery of Digital Rights Management (DRM) data from media files purchased from the iTunes store
  - Identification, structure, and examination of iTunes backupdata for iPod, iPhone, and iPad mobile devices
  - Extraction and mapping of Global Positioning System (GPS) data from digital pictures

Day 4

Day four's activities begin with a lesson on Mac Internet activity, following which the course will turn its attention to examination of the Linux operating system. Instruction will be given on the history of Linux and its operating system architecture and artifacts. The day and course conclude with a lesson regarding the operating system artifacts in Linux.

Day four's instruction will cover:

- **An examination of Internet-related Mac OS X application**
  - Safari configuration settings, cache content, Internet history, downloads, web-page previews, bookmarks, cookies, top-sites, session data, form data, cached login credentials, and Spotlight metadata
  - Location of Firefox data
  - Location and examination of Mail (the default Mac OS X e-mail application), Thunderbird, and Microsoft Entourage e-mail data
  - Location and examination of data associated with iChat, Windows Live Messenger, Yahoo! Messenger, and Skype
- **An examination of Linux, including**
  - An introduction to the Linux operating system and its history
  - A look at some of the key differences between Linux and UNIX, the operating system upon which it is based
- **A review of Linux disk nomenclature and partition structure**
  - How disks and volumes are identified as device nodes within the file system
  - How volumes are partitioned and subsequently mounted using empty folders that act as mount points
  - Examination of disks managed using the Logical Volumen Management (LVM) system
- **An introduction to the second, third, and fourth extended file systems, the concept of Inodes, and their structure**
  - A review of the way in which Inodes are stored, how an Inode for a file is located, its structure, and how it maps file data to clusters on the volume
  - A detailed discussion of the way in which Inodes track allocation for a file
- **A demonstration of how EXT2/3 directories work and an explanation of the link between a file's directory entry and an Inode**
- **The nature of hard links and symbolic links and how they are handled by the EnCase software**
- **Comprehensive coverage of Linux operating system artifacts, including**
  - Folder structure
  - User and group information
  - Password recovery
  - Time-zone settings
  - System and network configuration
  - Log files and log-file management
  - Hidden files
  - Compressed archive files
  - Evidence of user activity