EnCase 21 - Intermediate Forensics

40 APPROVED OPEN TEXT CONTINUING EDUCATION HOURS

Course Objectives

This 5 day class (when combined with Digital Forensics with FRED) is designed to familiarize the student with the man artifacts left behind on Windows based media and how to conduct a forensic examination with EnCase. Operating systems analyzed:

- Windows XP
- Windows Vista
- Windows 10

The course will focus on the traditional artifacts associated with normal operating system functions and user interactions. Topics covered will be those found most commonly in digital forensic examinations.

Prerequisites

This course is designed for a beginning Digital Forensic or eDiscovery practitioner with a basic understanding of Microsoft Windows operating system functionality.

To gain the maximum benefit from this course you should meet or exceed the following requirements:

- Read and understand the English language
- Have attended basic digital forensic training
- Be familiar with the Microsoft Windows environment and data recovery concepts

Course Outline

The course will follow adult learning principles through training aids such as presentations, diagrams and practical instructor lead examples. Each topic covered will be presented in either one or two 50 minute sessions followed by review questions. Students will be given the opportunity throughout the course to ask questions and discus objectives covered in more detail. Ample time will be allotted for hands on exercises to reinforce the topics covered.

The course will be structured as follows:

Introduction and Digital Forensic & eDiscovery Overview

- Introductions by the course instructor and students
- Identify the typical components of a digital forensic investigation
- Identify the typical components of an eDiscovery examination

Drive Interfaces

- Identify the main drive interfaces most likely to be encountered
- Explanation of the purpose of drive jumpers
- Explanation of the use of hard drive adapters

BIOS and CMOS

- Explanation of the system BIOS
- Explanation of the system CMOS
- Identify items of forensic interest in the CMOS
- Discuss methods to circumvent or disable passwords associated with the CMOS

Computer Data

- Explanation of how data is stored on various media
- Discuss the components of the ASCII / ANSI chart and define Unicode
- Explanation of the binary, decimal, and hexadecimal numbering schemes
- Identify various locations of interest where data will be found in various formats

Physical and Logical Characteristics

- Explanation of physical components of media
- Define the terms sector and LBA
- Explanation of logical structures of media

Operating and File Systems

- Explanation of an Operating System
- Identify the most commonly used Operating Systems
- Explanation of a File System
- Identify the most commonly used File Systems

MBR Partitioning

- Explanation of the Master Boot Record and its function
- Explanation of the Master Partition table and its function
- Review primary and extended partition structuring
- Identification of deleted and hidden partitions

GUID Partitioning

- Explanation of Protected MBR
- Explanation of the GUID Partition structure

FAT File System

- Describe the components of the FAT file system
- Explanation of the format command and results of its use
- Identify the system and data area on a formatted logical volume
- Explanation of the changes to media when a file is created using the FAT file system
- Explanation of the changes to media when a file is deleted using the FAT file system

NTFS File System

- Describe the components of the NTFS file system
- Describe the basic functions of the $Metadata files
- Describe the MFT entry attributes for files and folders
- Explanation of the changes to media when a file is created using the NTFS file system
- Explanation of the changes to media when a file is deleted using the NTFS file system

Forensic Triage and Duplication

- Discuss the use of forensic tools to conduct a forensic triage
- Explanation of the key factors used to triage digital media
- Explanation of the different digital forensic duplication options
- Discuss forensic duplication issues most commonly seen
- Examine digital media and forensic image files to conduct a forensic triage
- Created duplicate images of various media types
- Convert forensic duplicate formats

EnCase 21 Overview

- Identification of the configuration files
- Creation of the required storage locations
- Explanation of the method to create a case
- Highlighting to panes and windows within the application
- Explanation of the bookmarking feature

Recovery Module

- Usage of the case processor feature to recover deleted partitions
- Explanation of the recover folders function

Evidence Processor

- Usage of the evidence processor feature to perform forensic analysis

Signature and Hash Analysis

- Explanation of the signature analysis feature
- Explanation of the hash analysis feature
- Importing of NSRL and hashkeeper databases
- Creating and editing custom hash sets
- Data carve subject media for various file types

Searching

- Creating local and global keywords
- Conducting a keyword search and analysis
- Advanced and GREP searching techniques

Recycle Bin Function Across Windows Systems

- Examination of Windows XP recycle bin function and the structure of the recycler folder
- Examination of Windows Vista / Windows 7 recycle bin implementation and the $R \ $I file pairs

Link Files

- Explanation of Windows shortcuts
- Identify data of interest contained in a link file
- Running the link file parser feature of the case processor

Windows Registry

- Explanation of the function of the Windows registry
- Identify the Windows system files that comprise the registry
- Identify key structures and locations within registry hives
- Identify key investigative artifacts within the registry

Email

- Describe the use of container files by email applications
- Describe the use of individual message files by email applications
- Discuss the potential for deleted email file recovery
- Explanation of a basic email header

Internet Artifacts

- Describe the basic artifacts left behind by internet browsers
- Discuss form data and password recovery from internet browser artifacts
- Describe the basic artifacts left behind by instant messenger applications
- Discuss chat log and password recovery from instant messenger artifacts

Contact info
sales@digitalintelligence.com
1.866.344.4683
Outside the US: +1 262.782.3332