DFA — Digital Forensics Advanced

ADVANCED LEVEL

Course Objectives

This 3 day advanced class is designed to familiarize the student with the many artifacts left behind on a Windows NT platform. Operating systems analyzed:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8/10

The course will focus on the traditional artifacts associated with normal operating system functions and user interactions. Detailed discussions focusing on operating system processes will lead to analysis of the artifacts left behind after normal user / system interaction.

Prerequisites

This hands-on course is geared towards forensic investigators with at least 6 months experience in forensic case work with a basic understanding of Microsoft data structures.

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
- Have previous investigative experience in forensic case work
- Be familiar with the Microsoft Windows environment and data recovery concepts

Course Outline

The course will follow adult learning principles through training aids presentations, diagrams, and practical instructor led examples. Each artifact covered will be presented in either one or two 50 minute sessions followed by review questions. Students will be3 given the opportunity throughout the course to ask questions and discuss objectives covered in more detail. At the end of the day each student will have practical exercises to work that reinforce topics taught during the day's training.

The course will be structured as follows:

Introduction and Tools Used During Training

- Introductions by the course instructor and students
- An overview of the tools used during coursework for demonstrations and student practicals. References may be made to commercial products such as EnCase and Forensic ToolKit in addition to tools that are free and in the public domain.

Windows NT Versions and Key Features

- As with most operating system upgrades, Microsoft has always incorporated features and functions from previous versions of Windows. In this module students will compare the features of XP, Vista, and Windows 7/8/10 including the differences between Home, Media, Professional, and Ultimate editions

Windows Directory Structures

- Identify the default locations of user data
- Identify the default locations of system data
- Explanation of directory junctions including their identification
- Forensic implications of directory junctions in Windows

Partition Tables and GUID Partition Tables

- Explanation of the master boot record and master partition table
- Explanation of GUID partition tables
- Forensic examination of GPT's
- Instructor led labs on parsing partition tables

BitLocker Encryption

- Detailed explanation of Windows BitLocker
- Examination of BitLocked system volumes
- Detailed examination of Windows 7 BitLocker ToGo encryption
- Forensic recovery options and examiner's best practices

Windows 7/8/10 - Windows Libraries

- Examination of Windows libraries
- Examination of XML files associated with custom libraries
- Examination of registry artifacts associated with Windows libraries
- Forensic artifacts associated with Windows libraries

Recycle Bin Functionality Across NT Systems

- Examination of Windows XP recycle bin functionality and the structure of the recycle folder
- Examination of Windows Vista and Windows 7/8/10 recycle bin implementation and the $R \ $I file pairs
- Parsing of data associated with INFO2 and $I files
- Registry artifacts associated with recycle bin operation
- Forensic implications of recycled files

Link Files and Jump Lists

- Describe the function of Windows shortcut files
- Identify the date of interest contained in a link file
- Describe the purpose of jump lists
- Identify data associated with automatic destinations and custom destinations
- Examine the forensic implications of link files and jump lists

User Account Control and Internet Explorer Key Artifacts

- Describe the function of Microsoft's "Defense in Depth" model
- Describe and identify artifacts left behind by Internet Explorer on Windows systems
- Identify objects stored in lower privileged locations in the directory structure
- Discuss the forensic implications of data found within a user profile for internet facing applications

Thumbs.db vs. ThumbesCache

- Identify locations of thumbnails from viewed graphics on an NT system
- Compare the data structures of Thumb.db files and ThumbsCache file
- Forensic analysis of the data contained in each database file
- Discussion on other types of thumbnail db's found on a Windows system

Windows Event Logs

- Describe the location of event log files across various Windows NT systems
- Describe the differences between XP and Windows 7/8/10 event logs
- Instruction on using Windows event log viewer to locate items of interest in event logs
- Forensic significance of records contained in event logs

Prefetch and Superfetch

- Description of XP prefetch files and Vista / Windows 7/8/10 superfetch files
- Locating and viewing data files associated with prefetching
- Forensic significance of the layout.ini and *.pf data files

Volume Shadow Copy

- Describe the function of volume shadow copies
- Locating volume shadow copies
- Examination of volume shadow copy files
- Forensic implications of data found in shadow files
- Forensic analysis of shadow files

Windows Registry

- Identifying the key locations and forensic importance of Windows registry files
- Definitions of key registry structures and data
- Identification of key artifacts associated with registry files
- Protected storage system provider vs. IntelliForms
- Hardware device identification and analysis
- User account activity analysis and reporting

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