DFI — Digital Forensics Intermediate

INTERMEDIATE LEVEL

Course Objectives

This 3 day class is designed to familiarize the student with the many artifacts left behind on Windows based media. 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. 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 Forensic Tool Overview

- Introductions by the course instructor and students
- An overview of both commercial products, such as EnCase and Forensic Toolkit, and tools that are free and in the public domain.

MBR Partitioning

- Explanation of the Master Boot Record and its function
- Explanation of the Master Partition table and its function
- 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 the results of its use
- Identify the System and Data area on a formatted logical volume
- Explanation of the changes to a piece of media when a file is created using the FAT file system
- Explanation of RAM and Residual File Slack
- Explanation of the changes to media when a file is deleted using the FAT file system
- Manual review and recovery of deleted files

NTFS File System

- Describe the components of the NTFS File System
- Describe the function of the $Metadata filess
- Describe the MFT entry attributes for files and folders
- Explanation of the changes to a piece of media when a file is created using the NTFS file system
- Explanation of Orphan, or Lost, files
- Manual review and recovery of deleted files

Recyble Bin Functionality Across Windows Systems

- Examination of Windows XP recycle bin functionality and structure of the recycle folder
- Examination of the Windows Vista / Windows 7 / Windows 8/ Windows 10 recycle bin implementation and the $R \ $I file pairs

File Extensions and Headers

- Explanation of the purpose of file extensions
- Explanation of the purpose of file headers
- Describe the forensic concept of Data Carving

Thumbnails

- Identify the locations and purpose of Thumbs.db files
- Identify the locations and purpose of the various Thumbscache files

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
- Identification of key investigative artifacts within the Registry

Link Files

- Explanation of Windows shortcuts
- Indentify data of interest contained in a link file

Email

- Describe the usage of container files by email applications
- Describe the usage 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 applications