DFE — Digital Forensics Essentials

FOUNDATION LEVEL

Course Objectives

This 2 day class is designed to provide a foundation for a digital forensic examiner, eDiscovery specialist, or first responder. Lessons presented will focus on identification of digital forensic media, proper collection and transportation of digital media and culminating with forensic triage and duplication.

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
- 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 examination
- Identify the typical components of an eDiscovery examination

Hardware Recognition

- Identify common digital hardware components
- Discuss digital forensic items that may hold interest to a forensic examination

Seizure and Transportation

- Identify the proper methodologies for dealing with live computer systems on scene
- Discuss RAM capture on a live machine
- Discuss proper packaging techniques for transporting digital media

Drive Interfaces

- Identify the main drive interfaces likely to be found
- Explanation of the purpose of drive jumpers
- Explanation of use hard drive adaptors

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/disable passwords associated with the CMOS

Physical and Logical Characteristics

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

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 the various formats

Operating and File Systems

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

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

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 a piece of media when a file is created 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
- Explanation of MD5/SHA1/SHA256 hashing as it relates to forensic duplication
- Discuss forensic duplication issues most commonly seen
- Examine digital media and forensic image files to conduct a forensic triage
- Create duplicate images of various media types
- Convert forensic duplicate formats
- Combine a split forensic image into one image file