DFE — Digital Forensics Essentials

FOUNDATION LEVEL

Course Description

This 2-day, entry-level course introduces fundamental concepts, procedures, and tools used in digital forensic investigations, eDiscovery, and digital archiving. Lessons presented will focus on:

- Identifying various types of digital forensic media
- Best practices for collection and transportation of digital media / electronic evidence
- Digital forensic triage methods and tools
- Forensic duplication of digital media / electronic evidence

This course is designed for Forensic Examiners, eDiscovery Specialists, First Responders, and Digital Archivists.

Course Objectives

Students will develop foundational skills for digital forensics, eDiscovery, and data preservation, including the identification, seizure, transportation, duplication, and examination of physical and electronic evidence.

Prerequisites

This course is well-suited for novice Digital Forensic or eDiscovery practitioners 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 discuss 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, and Digital Archive Overview

- Introductions by the students and course instructor
- Identify the typical components of a digital forensic examination
- Identify the typical components of an eDiscovery examination
- Review foundation of digital duplication / archiving

Hardware Recognition

- Identify common digital hardware components
- Discuss digital forensic items of interest in a forensic examination

Seizure and Transportation

- Identify the proper methods for dealing with live (running) computer systems on scene
- Discuss RAM capture from a live machine
- Discuss proper packaging techniques for transporting digital media

Drive Interfaces

- Identify types of drive interfaces / technology most likely to encounter
- Discuss the purpose and use of drive jumpers
- Explain the purchase and use of drive adapters

BIOS and CMOS

- Discuss the purpose, use, and forensic relevance of system BIOS
- Discuss the purpose, use, and forensic relevance of system CMOS
- Review methods to circumvent / disable passwords associated with the CMOS

Physical and Logical Characteristics

- Identify the physical components of digital media
- Define the terms: sector, track, cylinder, page, block, and LBA
- Discuss logical structures of digital media
- Differentiate physical media from solid state drive media

Computer Data

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

Operating and File Systems

- Discuss the purpose and primary functions of an Operating System
- Identify the most common Operating Systems
- Discuss the role of a File System
- Identify the most common File Systems

Partitioning

- Discuss the MBR and GPT partitioning schemes
- Identify deleted partitions and their recovery methods

FAT and NTFS File Systems

- Review the components of the FAT and NTFS File Systems
- Explain the format command and the results of its use
- Discuss how file creation and deletion affect electronic data

Forensic Triage and Duplication

- Describe the processes used to triage electronic data
- Create forensically sound physical / logical duplicates using a variety of forensic tools
- Create custom content forensic images with various forensic tools
- Discuss common challenges facing forensic duplication, such as: encryption, integrated storage, and RAID data

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