Course Syllabus

Digital Intelligence®

Digitalintelligence.com

DFF – Digital Forensics with FRED™

FOUNDATION LEVEL

Course Objectives

This 1 day course is designed to provide the attendee with an overview of the FRED digital forensic workstation and how to utilize it for forensic triage and duplication. The course also discuss the proper way to configure the system to optimize its use with the most common digital forensic software. The course should be attended by new forensic or eDiscovery practitioners or first responders.

Prerequisites

This course is designed for a novice 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 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 Intelligence Hardware Overview

- Introductions by the course instructor and students
- An overview and discussion of the various FRED systems and configurations
- Discussion of additional Digital Intelligence hardware to include write blockers, adapters, storage solutions, etc.

Getting to Know FRED

- Explanation of the components that make up a FRED system
- Explanation UltraBay write blocker and its functionality
- Explanation of the removable drive bays and their usage
- Explanation of the Forensic Card Reader for removable media

Troubleshooting and Updating

- Identify which components will require periodic updates
- Utilize appropriate software to update various components
- Discuss common technical issues and their solutions

Optimal Configurations

- Discuss the various FRED options to include RAID systems
- Identify optimal configurations for use of storage locations to enhance the various forensic software that will be utilized on the system

Back Up and Restoration

- Discuss the usage of the system restore disc provided with the system
- Discuss the restoration of the SUSE Linux disc provided
- Discuss the methodology of creating a user back up of the FRED system
- Discuss the methodology of restoring a user back up of the FRED system

Forensic and eDiscovery Overview

- Identify the typical components of a digital forensic examination
- Identify the typical components of an eDiscovery examination

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