COURSE DESCRIPTION

Digital Forensics – Data Storage Foundations

Course Overview

This three-day course is designed for the examiner tasked with recovery of data on collected electronic evidence. The course covers in depth architecture and functionality of the Windows NT File System (NTFS), the FAT and the ExFAT File Systems and related directory entry information for locating files on electronic devices. Attendees will gain insight into partitioning structures and disk layouts and the effects of formatting partitions and learn of system area data. File management and directory structures characteristics will be examined in detail as well as techniques for discovering potential evidence that maybe pivotal to a successful examination. This will be followed by topical areas of interest to include file headers and file hashing and recovery of deleted files. This course incorporates an investigative scenario, providing hands-on experience with examination of collected evidence.

Course Type
Intermediate

Course Length
3 day

Course Code
DF-DSF

What You Will Learn

During this 3-day hands on course students will learn the following:

Partitioning and Format Review

- Describe the differences between MBR and GPT partitioned disks
- Examine the structure of a MBR and GPT partitioned disk
- Learn of the effects of formatting a volume to FAT
- Learn of the effects of formatting a volume to exFAT
- Learn of the effects of formatting a volume to NTFS.

FAT File System

- Describe the structure and functionality of the system area
- Examine the concept of clusters and data area
- Describe changes that occur when a file or folder is saved
- Examine the effects of data when a file is deleted
- Describe the process to recover deleted files on a FAT volume.

COURSE DESCRIPTION

NTFS File System deep dive

- List file system support for each NT operating system
- Identify NTFS Metadata Files
- List the function of each Metadata file
- Describe a File Record Entry
- List the components of an NTFS Attribute
- Examine the B+ Tree structure of directories
- Describe the effects of data when a file is deleted.

exFAT Introduction and full examination

- Describe the history of exFAT
- Identify the system areas of the volume
- Breakdown the Volume Boot Record
- File Allocation Table
- Describe the function of Bitmap
- Breakdown a directory entry
- Describe the effects of data when a file is deleted and review recovery techniques.

PREREQUISITES

To get the most out of this class, you should:

- Have 6 months experience of forensic examinations.
- Be familiar with Windows Operating systems.

CLASS MATERIALS AND SOFTWARE

You will receive a student manual, lab exercises and other class-related material.