COURSE DESCRIPTION

Foundations in Digital Forensics

Course Overview

This is a five-day course is designed for the investigator/examiner entering the field of digital forensics and provides the fundamental knowledge to comprehend and investigate incidents involving electronic devices. The course covers in depth architecture and functionality of the NTFS and FAT File Systems and their related metadata pertaining to stored objects on the physical media. Attendees will gain insight into partitioning structures and disk layouts and the effects of formatting volumes that contain existing data. File management and directory structure 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 and basic analysis of a windows-based system. This course incorporates an investigative scenario, providing hands-on experience with examination of collected evidence

Course Type
Foundation

Course Length
5 days

Course Code
DF – FDF

What You Will Learn

What is Digital Forensics

General overview of the world of digital forensic investigations.

Reasons for a Forensic Investigation

Discussions on the events that would lead to a request for a forensic examination.

Discuss the types of forensic analysis

Outline the different types of analysis the examiner will encounter
Discuss the challenges of each and questions that need to be asked before an examination begins
Describe the forensic and incident response process.

Incident Response Process

Discuss the role of the first responder
Outline the stages of the incident response
Review best practices in evidence collection
Concepts of a digital fingerprint, HASHing
Discussions in evidence recovery.

COURSE DESCRIPTION

Partitioning and Format Review

Describe the differences between MBR and GPT partitioned disks
Examine the structure of an 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.

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.

Operating Systems Overview

Learn to identify the core features of each NT Operating System
List the key artifacts contained on modern systems
Identify and review common folders on a NT Operating System.

Windows® System Artifacts

Describe the purpose of User Account Control
Discuss the forensic importance of Windows Prefetch and Superfetch
Learn how to examine ShadowCopies
Examine the function and forensic importance of the Recycle Bin.

COURSE DESCRIPTION

Introduction to the Windows® Registry

Define the Windows Registry
Discuss Forensic benefits of examining the Registry
Introduction into the recovering evidentially relevant data from the following registry files:
SAM
SYSTEM
SOFTWARE
NTUSER.DAT

Introduction into Windows® Shortcuts

Introduction to Windows Shortcuts
Examine Link File Anatomy
Introduction to Jump Lists and analysis.

Thumbnail Caching

Learn of the functions Windows uses to cache thumbnail images
Discuss user interaction characteristics
Examine the internal structure of each cached database.

Microsoft Browser Examinations

Gain an overview of Internet Explorer
Introduction to Microsoft Edge
Examine storage locations
Discuss implications of InPrivate browsing
Introduction to ESE Database analysis

PREREQUISITES

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

- Be familiar with Windows Operating systems.

CLASS MATERIALS AND SOFTWARE

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