OSForensics Boot Camp

Course Objectives

This 4 day class is designed to provide the student with the skills and techniques to effectively use the OSForensics software. In addition, the course will provide background and knowledge on digital forensics foundation topics.

Prerequisites

This hands-on course is geared towards forensic investigators with nominal experience with forensic case work or digital forensic foundations. While this course is not a substitute for a dedicated forensic foundation training, it will provide an understanding of partitions, file systems and artifact files.

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

Course Outline

The course will follow adult learning principles through practical instructor lead examples. The course contains no presentations and uses practical exercises exclusively Students will be given the opportunity throughout the course to ask questions and discuss objectives covered in more detail. The course will utilize instructor led exercises along with student practical exercises to enforce the training topics.

The course will be structured as follows:

Introductions and course overview

- Introductions by the course instructor and students
- Installation of software and course material review

Imaging and adding evidence

- Creating forensic copies with OSForensics
    - Physical and Logical Images
    - Image file restoration
    - Cloud data capture
- Creating cases and adding evidence
    - Creating cases and folder structure
    - Case configuration and settings

System Information

- Collection of System Information
    - Initial investigation data collection
    - Live evidence vs. forensic image files

File Identification

- File Name Search
- Deleted File Search
- Mismatch/Header File Search

File and System Viewers

- File Viewer windows
- File System Browser
- Disk Viewer

Documentation

- Adding Items to the case
- Tagging items
- Item Categorization

User Activity

- Configuration and Settings
- Activity Filters
- File and Folder Activity
- Anti-Forensic tools
- Internet Browser Activity
- Introduction to Event Logs
- Registry Artifacts
- Recycle Bin
- Prefetch
- Network Data
- Windows Timeline and Windows Search

Thumbnails and Thumbcache

- Thumbs.db files
- Thumcache Files
- Windows.edb database

Registry Viewer

- Registry file overview
- Searching the registry
- Understanding hives, values and key data

File Hashing

- Verifying evidence files
- Creating hash libraries
- Eliminating ignorable files
- Identifying notable files
- Importing NSRL or Project Vic hash libraries

Indexing and Searching

- Creating an index
- Merging multiple indexes
- Search techniques
- Regular Expression searching

Shadow Copy Analysis

- Identifying Shadow Copies
- Mounting Shadow Copies
- Shadow Copy analysis for identification of new, modified or deleted items

Event Logs

- Windows Event Logs
- Extended Event Logs
- Filtering log data

Databases and Logs

- SQLite databases
- $LogFile
- $USNJrnl
- ESE databases
- PList files

Encryption

- Identifying encrypted files
- Mounting Bitlocker volumes
- Recovering Bitlocker keys
- Dictionary and brute force attacks

Virtualization

- Mounting and booting forensic image files
- Circumventing logon passwords

Auto Triage and Live Response

- OSF Portable & OSF Bootable
- Processing live data
- Collecting data from a live machine
- Memory forensic analysis

Reporting