COURSE DESCRIPTION

Advanced Windows Forensics

Course Overview

The Advanced Windows Forensics training class is a four-day course that will introduce the participant to the many forensically relevant artifacts on a Microsoft Windows system.

Students will learn to use various applications and utilities to successfully identify, process, understand and document numerous Windows artifacts that are vitally important to forensic investigations. Students will gain knowledge in identifying where and why Windows stores information in Registry files, Recycle Bin, Recent folder, User directory and many system folders. The participant will also gain knowledge on how to process Edge browser history, cookies, temp files and other Windows 10 specific artifacts. The course includes gaining an in depth look into link files, and prefetch files and how they relate to forensic investigations.

Course Type
Advanced

Course Length
4 days

Course Code
DF - AWF

What You Will Learn

NTFS File System Review

- 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

exFAT Review

- 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

COURSE DESCRIPTION

Operating Systems Overview

- Review the differences between NT operating systems
- List the key artifacts contained on modern Windows based systems
- Review common folders on an NT Operating System.

Windows System Artifacts

- Examine how Desktop Search stores data
  - Learn recovery options from the Windows.edb file
- Examine different backup option on Windows 10 systems and how to recover data in the ShadowCopy stores.

Windows Registry

- Define the Windows Registry
- Discuss Forensic benefits of the Registry
- Examine a Registry block structure
- Define a Registry key structure
- Locating deleted registry data
- Explore the many evidentially relevant data found in the following registry files:
  - SAM – User Account information
  - SYSTEM – Hardware data
  - SOFTWARE – Installed application settings
  - NTUSER.DAT – User preferences and recent activity
  - UsrClasses – User data
  - Settings.dat – Immersive application preferences.

Windows Shortcuts

- Review of Windows Shortcuts
- Link File Anatomy
- Jump Lists
  - Deep dive into Jump List Analysis
  - Learn of the intricate link with the NT File System.

Windows Immersive Applications Examination

- Describe the purpose of Live Tiles
- Examine backend structures of Immersive apps
- Describe the function of each folder location storing user cached data.

COURSE DESCRIPTION

Edge Browser Forensics

- Review the Edge Browser application
- Locate key folders of interested within the user profile
- Identify cached data from untrusted and trusted sites
- Learn of Edge Recovery stores and processing techniques
- Discover registry data and explain synchronization concerns
- Review processing techniques.

Windows 10 Mail

- Learn of the function of the default Mail client
- Explore the locations of Trusted and Untrusted data
- Review the “Comms” folder and ESE structured database
- Extract key data from the Store.vol ese database
- Review the storage of email data within the sub-folders of the Comms and S0 folders

Introduction to Office 365 data

- Learn of the many artifacts hosted on the local system pertaining to user activity while using the office 365 suite.

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.