COURSE DESCRIPTION

Windows® 10 Advanced Analysis

Course Overview

The Advanced Windows Forensics training is a four-day course that will introduce the participant to the many forensically relevant artifacts on a Microsoft 10 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. The participant will also gain knowledge on how to process Edge browser history, cookies, temp files InPrivate browsing challenges and analysis, BitLocker encryption and other Windows 10 specific artifacts. The course includes gaining an in depth look into jump Lists, and prefetch files and how they relate to forensic investigations.

Students will use a variety of open source and leading forensic applications to examine key artifacts through multiple hands on labs and student practical's.

Course Type
Advanced

Course Length
4 days

Course Code
DF – WAA

What You Will Learn

Windows 10® Artifact Overview

- Examine the version characteristics between Windows 10 Operating systems
- Explore the challenges the recent update has presented to the forensic examiner
- Discuss Windows ToGo functionality and forensic examination.

Windows® System Artifacts

- Examine how the Desktop Search 'Windows index' functions
- Explore the types of data found in the Windows Index database
- Learn recovery techniques of data stored in the database
- Examine the function of Prefetch and Superfetch
- Discuss techniques in examining the Prefetch \ Superfetch data files

COURSE DESCRIPTION

BitLocker Encryption

- Learn how BitLocker encryption functions
- Explore System Volume BitLocker implementation and metadata artifacts
- Discuss BitLocker To Go on data volumes and USB devices
- Learn of examination techniques of a BitLocked volume.

Windows® Registry

- Define the forensic importance of Windows Registry artifacts
- Examine a Registry block structure
- Define a Registry key structure
- Learn how the recognise deleted registry data
- Using multiple tools explore the many evidentially relevant data found in the following registry files:
    - SAM – Windows Live accounts
    - SYSTEM – Portable devices and Network settings etc.
    - SOFTWARE – Network, user and hardware examination
    - NTUSER.DAT – User preferences and recent activity
    - UsrClasses – Cloud data.

Windows® Shortcuts

- Overview of Windows Shortcuts
- Deep dive into Jump List Analysis
- Learn of the correction between the Distributed Link Tracking Service and Windows link files
    - Learn of the intricate link with the NT File System.
- Explore the structure of Jump List data files
- Examine effects of destructive processes on jump lists
- Learn of File System artifacts associated with user activity on host files and link file creation.

Windows® 10 Notifications and Timeline analysis

- Learn of the Action Centre functionality
- Review the backend storage locations of notifications
- Explore the Timeline function and artifacts
- Gain knowledge on how SQLite databases function
- Explore artifacts stored in the backend SQLite database
- Describe the correlation between displayed images on live tiles and backend storage.

Photo's Application Artifacts

- Overview of Immersive Application folder structures
- Review the Photo's application from a user perspective
- Identify storage locations of cached data
- Learn of key artefacts identified within the SQL database.

COURSE DESCRIPTION

Cortana Integration

- Learn of Microsoft digital assistant
- Identify storage location of hosted data
- Identify key folder locations of collected data
- Review data stored in txt and cfg files pertaining to Cortana
- Discuss cloud integration and synchronization processes.

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
- Explore InPrivate browsing and learn of recoverable artifacts
- Discover registry data and explain synchronization concerns
- Extensive hands on processing techniques.

OneDrive – Cloud Synchronization

- Review the function of the OneDrive processes
- Locate key folders of interest
- Identify the locations of user files
- Explore the many artifacts located in the Synchronization logs
- Learn how to interoperate user settings
- Learn interpretation of stored settings files
- Discover Office 365 cloud integration
- Use the registry to locate recent file interaction
- Interpret stored data in the subkeys
- Introduction to Office 365 synchronized data.