

Windows 10 Advanced Analysis

Course Overview

The Advanced Windows 10 Forensic analysis class is an expert-level four-day training course, designed for examiners who are familiar with the principles of digital forensics and keen to expand their knowledge on advanced forensics using a host of third-party tools to improve their computer investigations.

The Spyder Forensic Advanced Windows 10 Forensic Analysis course will give participants unbiased knowledge and skills necessary to analyze artifacts left behind through system and user interaction with the host system, utilizing industry standard tools and open source applications to explore the data in greater depth by learning how applications function and store data in the file 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, Windows Action Center (Notifications SQLite Database) and other Windows 10 specific artifacts. The course includes gaining in depth knowledge of JumpLists, Registry analysis and prefetch files and how they relate to forensic investigations and conclude with an in-depth look into OneDrive and synchronization processes between trusted devices.

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.

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 Type

Advanced

Course Length

4 days

Course Code

DF – WAA

Law Enforcement Stream

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 to 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 correlation 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 Immersive Applications review

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

Windows 10 Notifications

- Learn of the Action Centre functionality
- Review the backend storage locations of notifications
- 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

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.

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

Photo's Application Artifacts

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

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.