

Windows® 10 Overview Workshop (Win10)

Course Overview

This specialized one-day workshop provides the knowledge and skills necessary to analyse the latest Windows® 10 operating system artifacts, user data and explore the many updates this new Operating System has introduced. During this one-day course, participants will review various Windows 10 features, learn of artifact locations for Microsoft Edge Browser, Cortana, OneDrive, Windows® Mail, Notifications and gain an overview of core registry files and new values of forensic interest pertaining to user activity on a Windows® 10 system.

What You Will Learn

- Windows® 10 Overview
 - General overview Windows 10 functionality, focusing on the new artifacts of interest to the forensic examiner.
- System Artifacts
 - Deep dive into core system artifact updates on a standard Windows 10 environment. Attendees will be exposed to changes and updates to the following items:
 - File System
 - Disk Layout
 - Recycle Bin
 - Prefetch compression
- User Artifacts
 - Windows® 10 brings many new items of interest to the forensic examiner; this session focuses on new items of interest within the user profile where day to day activity on the host system has occurred. Items to be covered include:
 - Edge Browser structures and artifacts
 - Cortana's interaction with the system and user activity including data files located in the package folder structure.
 - Notifications updates and decompiling of data structures
 - Examination of the Timeline function and artifacts
 - Examine Windows® Mail and the 'Comms' folder
 - Review Registry Updates
 - OneDrive synchronization considerations

Course Type
Specialized

Course Length
1 day

Course Code
DF – Win10

