COURSE DESCRIPTION

Digital Forensics – Windows Artifacts Foundations

Course Overview

The Windows® Artifacts Foundations training is a three-day course that will introduce the participant to the many forensically relevant items stored on a Windows based system through user interaction and host operating system functionality.

Students will use various applications and utilities to successfully identify, process, understand and document numerous Windows® artifacts that are vitally important to perform a successful forensic investigation of the seized system. Students will gain knowledge to identify where and why Windows stores information in the Registry files, Recycle Bin, Recent folder, User directory and system folders. The participant will also learn how to process Internet Explorer history, cookies, temp files and user settings and compare them with the Edge browser released with Windows® 10.

Course Type
Intermediate

Course Length
3 Day

Course Code
DF – WAF

What You Will Learn

During this 3-day hands on course students will learn the following:

Operating Systems Overview

- Learn to identify the core features of each NT Operating System
- List the key artifacts contained on modern systems
- Identify and review common folders on a NT Operating System.

Windows® System Artifacts

- Describe the purpose of User Account Control
- Discuss the forensic importance of Windows Prefetch and Superfetch
- Learn how to examine ShadowCopies
- Examine the function and forensic importance of the Recycle Bin.

Introduction to the Windows® Registry

- Define the Windows Registry
- Discuss Forensic benefits of examining the Registry
- Recovering evidentially relevant data from the following registry files:
  - SAM
  - SYSTEM
  - SOFTWARE
  - NTUSER.DAT

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. Spyder Forensics makes no warranties, expressed or implied, in this document for registered trademarks of Spyder Forensics in the United States and/or other countries. Other trademarks referenced are property of their respective owners.

COURSE DESCRIPTION

Windows® Shortcuts

- Introduction to Windows Shortcuts
- Examine Link File Anatomy
- Introduction to Jump Lists and analysis.

Thumbnail Caching

- Learn of the functions Windows uses to cache thumbnail images
- Discuss user interaction characteristics
- Examine the internal structure of each cached database.

Windows® Start Screen Examination

- Describe the purpose of Windows Immersive Applications
- Examine how the Live Tiles database functions
- Explore the storage areas for Immersive Applications.

Browser Examination

- Gain an overview of Internet Explorer
  - Discuss Legacy Features
- Examination of data storage locations and artifacts of forensic interest
- Introduction to Microsoft Edge
  - Examine storage locations
  - Learn of travel logs and their examination
  - Discuss implications of InPrivate browsing
- Introduction to ESE Database analysis
- Overview of Cortana digital assistant
  - Examine cached data from user interaction.

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.

SPYDER FORENSICS

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. Spyder Forensics makes no warranties, expressed or implied, in this document for registered trademarks of Spyder Forensics in the United States and/or other countries. Other trademarks referenced are property of their respective owners.