Windows 10 Forensics

Advanced• Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

This advanced three-day course provides the knowledge and skills necessary to analyze the new Microsoft® Windows 10® operating system artifacts, user data, and file system mechanics. Participants will review features, learn of artifact locations for Microsoft Edge browser and Cortana, OneDrive, and an overview of core registry files and new values of forensic interest pertaining to user activity on a Windows 10 system.

Prerequisites:

To obtain the maximum benefit from this class, you should meet the following requirements:

- Able to understand course curriculum presented in English
- Be familiar with Windows NT file system (NTFS)
- Basic knowledge of computer forensic investigations and acquisition procedures
- Be familiar with the Microsoft Windows environment and basic forensic analysis

Class Materials and Software:

You will receive the associated materials prior to the course or arrival at the classroom.

(Continued on other side)

SYNTRICATE

Windows 10 Forensics

Advanced• Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

(Continued)

Module 1: Introduction

Topics:

- Introductions
- Class materials and software
- Prerequisites
- Class Outline
- Helpful Information
- Class machine preparation

Module 2: Windows 10 Registry

Objectives:

- NTUSER.DAT
- UsrClass.dat
- Settings.dat (individual application registry)
- Amcache.dat
- SAM
  - Live Accounts
  - Local Accounts
  - Password references (Picture,Fingerprint,PIN Passwords)
- SOFTWARE
- SYSTEM
  - HDD tracking
  - W32 Time

Module 3: Windows 10 Introduction

Objectives:

- Features
- User Interface
- File Structure
  - MBR/GPT
  - Security
- File Tracking – Local Browsing History from File Explorer
- Traditional Artifacts and New Utility
  - Link Files and Jump Lists (added apps)
  - VHDs
  - ISO Mounting (from Windows)

Module 4: Edge Browser

Objectives:

- User Interface
- Browsing History
- File System Artifacts
- Page Recovery
- Searches
- Registry Artifacts
- Local Browsing History - File Explorer
- Internet Explorer 11 (IE11) Tracking

Module 5: Cortana

Objectives:

- User Interface
- Relationship to the Edge Browser
- File System Artifacts
- Searches – “Ask me anything”
  - File System
  - Registry

Module 6: OneDrive

Objectives:

- Cloud Overview
- OneDrive Structure
- Registry Information
- Log Files
- Document Tracking
- Online UI
- Office File Cache Storage

SYNTRICATE

Windows 10 Forensics

Advanced • Three-Day Instructor-Led Course

For more information contact: info@syntricate.com

(Continued)

Module 7: OS and Built-in Artifacts

Objectives:

- OneNote
- EFS
- Defrag
- Recycle Bin
- Print Spool Files
- Prefetch
- Thumbcache
- Storage/Backup

Module 8: Applications

Objectives:

- Skype
- Photo App
- Webcam App

Module 9: Office 365 and Office 2016

Objectives:

- Office Overview
- Metadata Changes
- Document Recovery Artifacts
- Roaming Recent Links
- Event Log Entries
- Registry Artifacts

Module 10: Windows 10 Mail

Objectives:

- Format and Interfact
- Storage Artifacts
    - File System
    - Tables
    - Appointments
    - Contacts
- People Application Association
- Attachments
- Temporary File Mail Recovery

Module 11: Xbox

Objectives:

- User Interface Overview
- Application
- File System Artifacts
- Model Manager
- Messaging
- Smart Glass Application

SYNTRICATE