RN Trust
The Digital Trust Company

WINDOWS FORENSICS (5 DAYS)

The course is designed to provide participants with a detailed overview of the Windows 10 operating system forensics. It will focus on how the Windows 10 operating system changed over the past versions and how it works "under the hood" so that participants have a better understanding of how various operating system artefacts are created, why certain artefacts appear, and how these artefacts can be leveraged for forensic and investigative purposes in comparison to the previous versions. Since the Windows OS went through a lot of changes from its XP version till version 10, there are now a lot of new artefacts that investigators need to be aware of and know how to utilize them in their investigations.

Course Objectives:

By the end of this workshop, all the students will be able to:

- Recognize file system within windows operating system
- Find and forensically analyze user profiles
- Locate and analyze windows registries with different tools
- Recognize and analyze files encrypted with different versions of BitLocker
- Locate and analyze event logs
- Recognize event logs important for digital forensic analysis
- Understand, locate and analyze superfetch and prefetch files, link files, jump lists, thumbcache, thumbs
- Find recycle bin files, know the difference between recycle bin files form Windows 10 and previous version of Windows OS
- Find all other relevant forensic artefacts, know how to analyze them and what is their forensic value

Prerequisites:

Working knowledge of FTK Imager and Sysinternals suite, good experience with Windows operating system, knowledge of forensic artefacts that are present in Windows OS.

Syllabus

DAY 1

Workshop starts with the short introduction to class, features of Windows 10 operating system and differences between windows versions. Students get familiar with file systems with special emphasis on FAT and NTFS file systems, their structure, forensic value. At the end of day 1, students learn about user profiles, their locations under Windows 10 operating system and how they can be used in forensic investigations.

I. Introduction

- Class outline
- Windows 10 overview
- New features in Windows 10
- Home vs Pro version
- Windows 10 folder structure

II. File system

- FAT
- NTFS

III. User Profiles

- Locations
- User Profile types
- Accounts

DAY 2

Day 2 is reserved for Windows registries and their features, locations, values they contain. At the end of the day, trainers explain BitLocker and the options available through it.

I. Windows Registry

- Live vs Offline Registry
- Live Registry
  - ❖ Locations
  - ❖ Connections
  - ❖ Regedit
  - ❖ Acquisition of live registry
-
- Offline Registry
  - ❖ SAM
  - ❖ SECURITY
  - ❖ SOFTWARE
  - ❖ SYSTEM
  - ❖ NTUSER.dat
- Shellbegs Artifacts

II. BitLocker & BitLocker to Go

- Drive Recovery
- Recognition
- Identification of recovery keys

DAY 3

On day three students learn about event logs on Windows 10 operating system, how to find them, analyse them, what information they contain, how can they make conclusions from given information, what event logs are crucial for forensic investigations. There is short chapter on link files, jump lists, thumbcache. Big part of day three is dedicated to prefetch and superfetch artefacts and their forensic value.

I. Event Logs

- Introduction
- Windows Event Viewer

II. Superfetch & prefetch

- Superfetch
- Prefetch

- ❖ Filtering & exporting
  - Identification of relevant events

III. Link/Shortcut files
IV. Jump Lists
V. Thumbcache
VI. Thumbs.db

DAY 4

Day 4 continues with analysis of different forensic artefacts. It starts with Recycle Bin, differences between Recycle Bin artefacts within different versions of Windows operating system. Day continues with analysis of volume snapshot service, pagefile and hiberfil, Cortana service and information it provides for forensic investigators, Windows store, IE, OneDrive. Day ends with explanation of remote access.

I. Recycle Bin
  - Windows XP vs 7,8,10
  - INFO2 file
  - $I Info file structure
  - Deleted vs Orphaned files

II. Volume Snapshot Service
  - Location & accessing VSS

III. Windows.old
IV. Windows Indexing
V. Pagefile & hiberfil
VI. Cortana
  - Typed searches

VII. Notification center
VIII. Windows store
  - Windows Apps

IX. Edge Browser
X. Internet Explorer
XI. Skype application
XII. OneDrive
XIII. Remote Access

DAY 5

Day 5 starts with the rest of forensic artefacts: VHD, Sandbox, Clipboard and Timeline. The workshop ends with the final exam, survey and certification ceremony for the successful students.

I. Virtual Hard Drives
II. Sandbox - v1906
III. Microsoft People
IV. Clipboard
V. Timeline
VI. Final exam
VII. Survey and certification ceremony