COURSE DESCRIPTION

Windows® 11 Advanced Forensic Exploitation

Course Overview

The Advanced Windows® 11 Forensic Exploitation analysis course is an expert-level week-long training event 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 digital investigations techniques on the latest operating system from Microsoft.

Students will learn to use various applications and utilities to successfully identify, process, understand, and document numerous Windows® 11 artifacts that are vitally important to forensically examine the latest Microsoft operating system. The participant will gain knowledge on how to process the latest chromium Edge browser, deal with BitLocker encryption, analyze the new Windows® Photos app, examine Windows obscured apps, exploit the Windows Subsystem for Linux and Android, plus other Windows® 11 specific artifacts and review data in the newly updated Notepad application.

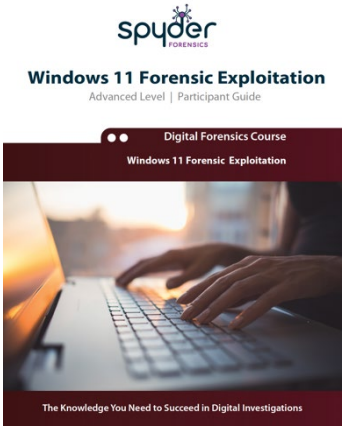
The course includes gaining in-depth knowledge in all aspects of Windows 11 virtualized security, plus learning of new Registry file functions and transaction logging, extraction of Microsoft 365 (Office 365) artifacts on Windows 11, and other core Windows artifacts will be examined and analyzed then concluding with an in-depth look at OneDrive off-line storage and synchronization processes between trusted devices the user account has authenticated to. SQLite forensics plays a major role in the analysis of data therefore students will gain detailed knowledge in scripting and data exploitation.

Students will use a variety of open source and leading forensic applications to examine key artifacts through multiple hands-on labs and student exercises.

Course Type
Advanced

Course Length
4 days

Course Code
DF – Win11
Digital Forensics Track



COURSE DESCRIPTION

What You Will Learn

Windows® 11 Artifact Overview

- Examine the version characteristics between Windows® 10 Operating systems
- What is new in the Microsoft OS
- Walkthrough Windows 11 from a user perspective
    - Explorer updates
    - Visual changes
- Changes to Existing Artifacts
- System updates
- Core Application updates
- Automated data deletions

BitLocker Encryption

- Learn how BitLocker is implemented on system partitions and removable media
- Locate and read the metadata objects located in the encrypted volume
- Describe BitLocker To Go
- Review recovery options when BitLocker fails
- Workflows in analysis of a BitLocked volume

Windows 11 sub-system Analysis

- What is new in the Microsoft Sub-systems
- Explore the uses of Linux Sub-systems on Windows Operating Systems
- Learn of the Android Sub-System introduced with Windows 11
- Examine host-based artifacts through use of WSL and WSA

Exercises in Registry analysis on a Windows 11 system

- Define the Windows Registry
- Discuss Forensic benefits of the Registry
- Explore Windows 11 Account types and updates
- Review how to track removable hardware across a Windows 11 system
- Examine user interactions with the system

Cortana® examinations

- Learn of Microsoft digital assistant Cortana
- Identify storage location of hosted data
- Identify key folder locations of collected data
- Exploit the data in the SQLite db
- Review the data in the settings registry file

COURSE DESCRIPTION

Windows® Action Center

- Notifications Analysis
  - Introduction to Windows Notifications
  - Review of the backend storage locations
  - Identify data of interested within the backend SQLite database
  - Exploit records using SQLite scripting

Recent File Interactions

- Introduction to Windows Shell Links
- Windows 11 Jump Lists
- Jump List Analysis
- Introduction to Windows 11 Recent File lists
- Examination of backend databases
- Exploitation of data fields using comprehensive scripting techniques

Examination of Graphic File Interactions

- Review the function of the Windows 11 Photo's app
- Explore the backend folder structure
- Examine the SQLite database
  - Explore the many tables of forensic interest
- Examine Geolocation data extracted by the app
- Exploit stored data using SQLite Scripts and other techniques
-

OneDrive on Windows 11

- Microsoft OneDrive solution overview
- Review the different options for OneDrive
- Locate key folders of interest
  - User files
  - Synchronization log files
  - User settings
- Learn interpretation of stored settings files

Chromium Based Browsers

- Review the Chromium Edge Browser application
- Locate key folders of interested within the user profile
- Extract browsing artifacts from various SQLite databases
- Learn techniques in the extraction and analysis of JSON encoded artifacts
- Explore Alternate databases using Python
- Introduction to LevelDB's and Analysis

COURSE DESCRIPTION

Windows 11 Mail

- Windows Mail and examination techniques
  - Learn of the function of the Windows Mail client
  - Locations of Trusted and Untrusted data
  - Review the Comms folder and ESE database
  - Extract key data from the Store.vol ese database
  - Review the storage of email data within the sub-folders of the Comms and storage folders

The course will follow adult learning principles through training aids such as presentations, diagrams, and practical instructor lead examples. Each artifact covered will be presented in either one or two 50-minute sessions followed by review questions. Students will be given the opportunity throughout the course to ask questions and discuss objectives covered in more detail. Throughout each day students will have practical exercises to work on in order to reinforce the topics.

PREREQUISITES

To get the most out of this class, you should:

- Have 12 months experience of forensic examinations
- Attended Spyder Forensics Foundations training or similar program
- Be familiar with Windows Operating systems.

CLASS MATERIALS AND SOFTWARE

You will receive a student manual, lab exercises and other class-related material.