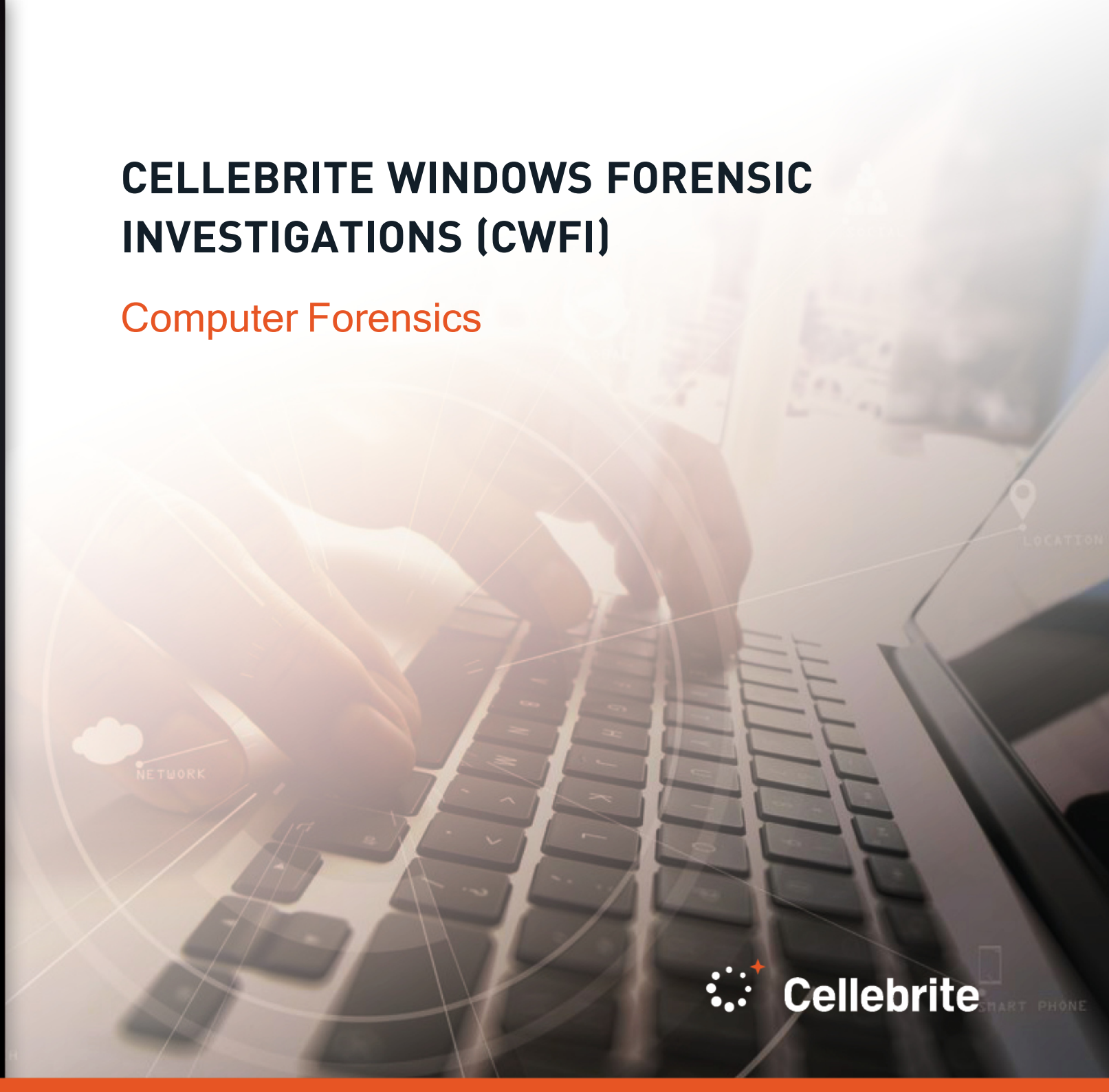
CELLEBRITE WINDOWS FORENSIC INVESTIGATIONS (CWFI)

Computer Forensics



Cellebrite

Level

Advanced

Length

Four-Day (28 hours)

Training Track

Computer Forensics

Delivery Mode

Instructor-Led
Live Online

Course Description

Cellebrite Windows Forensic Investigations (CWFI) is a four (4) day intermediate level training course designed to teach and improve practitioners Windows forensic analysis skills. Students will receive detailed instruction about Windows-based file systems, operating systems, user data, and application artifacts, including Windows 10 artifacts. Emphasis is placed on teaching file system functions and where critical information is stored for insightful, expedited investigations.

Computer Forensics

Cellebrite aims to support learners in the pursuit of excellence in Digital Intelligence specialty areas without the need to commit to any degree program. Cellebrite's Academic & Learning Paths provide guided training programs and continuous skill set development to achieve various levels of educational or professional goals.

By following a learning path, students can target personal, professional, and leadership skills in a Digital Intelligence career for law enforcement, military, intelligence, and private sector practitioners. Cellebrite's curriculum reflects its commitment to digital intelligence excellence by helping Below are general audiences and focus areas relative to this course.

- Digital Forensic Examiners

Course Learning Objectives

Upon successful completion of this course, students will be able to:

- Identify windows-based evidence and distinguish between related file systems
- Describe basic requirements of file systems and supporting data structures
- Navigate and explain significance of Windows evidence
- Utilize digital forensic searching techniques using BlackLight across Windows evidence
- Explain Windows registry and interpret time zone settings
- Analyze registry for evidence of device, application, and file access
- Examine additional registry stored data including UserAssist and ShellBags and interpret results
- Describe the function of various NTFS Metafiles and the importance of the data they contain
- Interpret log, journal files, and databases utilized by the Windows operating systems
- Examine Windows Prefetch, Link Files, JumpLists, and Recycle Bin and articulate findings
- Investigate Windows Users and compressed entries
- Identify and explore Volume Shadow Copy evidence
- Process and scrutinize Windows memory for evidence

WINDOWS FORENSIC FOUNDATIONS

- Recognize Windows-based file systems and operating systems
- Explain how operating and file systems impact evidence seizures
- Describe evidence seizure and collection steps and considerations
- Interpret and convert different data structures
- Describe varying units of data and how they are encoded
- Identify various partition schemes and their related elements
- Examine volume boot records and file slack areas
- Describe requirements and functions of a file system
- Identify the various Windows-based file systems
- Explain the storage and deletion operations of Windows-based file systems
- Utilize file system knowledge to investigate digital evidence
- Recognize Windows-based evidence
- Examine Windows User, program, and application data
- Identify links and other Windows-based mechanisms for user navigation and experience
- Utilize forensic software to navigate Windows evidence
- Utilize filter and tagging features of BlackLight to locate and mark evidence
- Describe how filtering methods can help and their potential to hinder your examinations
- Explain tagging findings and its relation to analyzing data and building reports
- Utilize various evidence extraction methods to further analyze digital evidence
- Utilize keyword searching features in forensic tools
- Process file signatures and utilize results for further analysis
- Investigate digital evidence to salvage data through file carving methods
- Utilize hash analysis functions to identify or exclude data from a case

WINDOWS REGISTRY

- Explain the functions of Widows Registry and how it stores data
- Identify system and user registry files
- Utilize forensic software to examine registry data
- Investigate prominent registry data
- Identify where time zone settings are stored in the registry
- Explain how different file systems impact time zone information
- Analyze time zone registry data
- Utilize forensic software to adjust time zone settings
- Identify registry-based device access evidence
- Recognize evidence from fixed and other device types
- Explain methodology of investigating devices in registry data and related limitations
- Interpret findings of device access in registry data
- Identify Windows registry areas containing file access evidence
- Utilize forensic software to parse registry-based file access data
- Identify various Windows registry areas containing application access evidence
- Utilize forensic software to parse registry-based file access data
- Explain UserAssist function in the Windows operating system
- Identify the manner and location UserAssist data is stored
- Utilize forensic software to interpret and investigate UserAssist data
- Explain ShellBag registry data function in the Windows operating system
- Identify the manner and location ShellBag data is stored within the registry
- Utilize forensic software to interpret and investigate ShellBag data

WINDOWS EVIDENCE PART 1

- Recognize and explain functions and importance of various NTFS MetaFiles
- Interpret pertinent areas of file table record data
- Recognize various Windows operating and related file system logging and journaling functions.
- Investigate and examine log and journal files
- Interpret findings and explain their meaning
- Identify locations of Windows user and account information
- Interpret user identifiers
- Examine and correlate user and membership data
- Describe alternate login methods and related data
- Describe Windows Recycle Bin operations
- Identify and explain Recycle Bin data and how it is impacted by the file system
- Examine and investigate Recycle Bin evidence

WINDOWS EVIDENCE PART 2

- Explain link file purpose
- Identify location of link file data
- Interpret values from the structure of link files
- Utilize forensic software to investigate link file evidence
- Describe the purpose of JumpLists
- Identify the location and manner of storage for JumpList data
- Interpret JumpList values from data structures
- Utilize forensic software to investigate JumpList evidence
- Describe function of Prefetch
- Articulate location and values stored in Prefetch data structure
- Parse the Prefetch values from the data structure
- Utilize forensic software to investigate Prefetch evidence
- Explain Windows Volume Shadow Copy operations
- Describe different methods of backing up Windows operating system data
- Examine Windows evidence for Volume Shadow Copy and backup system data
- Utilize forensic software to analyze Volume Shadow Copy data

WINDOWS EVIDENCE PART 3

- Describe different manners of archiving data by compression
- Identify data compressed into archives or packed
- Explain methods for handling packed or compressed files
- Examine packed or compressed evidence
- Recognize Window-based evidence and varying states of database files
- Explain ESE databases and functions of Windows operating system EDBs
- Analyze evidence from Windows Notification and Timeline databases
- Interpret data from Windows SRUM databases
- Identify methods to collect and parse Windows memory evidence
- Explain purpose of Windows memory
- Describe objects that can be parsed from memory
- Examine Window memory with forensic software

PRACTICAL EXERCISES

- Utilize forensic software to search Windows-Based evidence, identify attached devices, and investigate system and user data in a case investigation
- Utilize forensic software to search Windows registry evidence and investigate user, device, and application data in a case investigation
- Utilize forensic software to analyze evidence related Windows logging, users, and Recycle Bin data in a case investigation
- Utilize forensic software to analyze Prefetch and Link File evidence data in a case investigation
- Utilize forensic software to analyze Prefetch and Link File evidence data in a case investigation

Get skilled. Get certified.

"Every day around the world, digital data is impacting investigations. Making it intelligent and actionable is what Cellebrite does best.The Cellebrite Academy reflects our commitment to digital forensics excellence; training forensics examiners, analysts, investigators and prosecutors around the world to achieve a higher standard of professional competency and success."

Learn more at: cellebritelearningcenter.com

Cellebrite

Cellebrite Windows Forensic Investigations