IACIS

The International Association of Computer Investigative Specialists

Windows Forensics Examiner (WFE)
Core Competencies

Windows Forensic Examiner (WFE) Program

IACIS prides itself on being the world's leading organization for computer forensics practitioners. In addition to providing the highest quality computer forensics training, IACIS strives to foster excellence in the field through its formal certification programs.

Computer forensics is the acquisition, authentication, reconstruction, examination, and analysis of data stored on electronic media. The IACIS Basic Computer Forensic Examiner (BCFE) Program and its accompanying certification program, the Certified Computer Forensic Examiner (CFCE), address each of these key tasks and measure one's ability to perform these key tasks in accordance with established standards.

Like the BCFE Program, the IACIS Windows Forensic Examiner (WFE) Program and its accompanying certification Program, the Certified Advanced Windows Forensic Examiner (CAWFE) Program, expand on the foundational concepts and tasks at the heart of the computer forensic examination process by exploring forensically critical features of the Windows family of operating systems in far greater detail than can be afforded in the BCFE program and CFCE program.

The WFE core competencies described in this document are a binding set of competencies that guide both the training and certification programs to ensure that the skills and knowledge points delivered within the training program are also the same set of standards evaluated within the certification program. The IACIS Standards Committee monitors both programs to ensure each adheres to strict guidelines of the established certification competencies.

Windows Forensic Examiner Core Competencies
There are Six (6) competency areas addressed in the WFE Program:

I. **Windows Partitioning Schemes**
II. **Windows File Systems**
III. **Windows Defaults and Standard Functionality**
IV. **Windows Registry**
V. **Windows Artifacts**
VI. **Live Memory Acquisition and Analysis**

I. Windows Partitioning Schemes

a. Ability to identify current Windows partition schemes.
b. Knowledge of individual structures and system areas used by each partition scheme.
c. Ability to identify the data stored in each of the system areas and how to parse it.
d. Understand that partition schemes can be used with different file systems and operating systems, and knowledge of which schemes are compatible with which file system.
e. Define Globally Unique Identifier (GUID) and explain its application.

II. Windows File Systems

a. Understanding of file system concepts and system files.
b. Knowledge of the basic architecture of volume boot sectors.
c. Understanding of the various Windows file system concepts and technologies.
d. Understanding of common file system objects and how they are applied in the Windows operating system.

III. Windows Defaults and Standard Functionality

a. Knowledge of the default folder structure and fully qualified paths on a standard Windows installation.
b. Understand the Windows boot process.
c. Understand the use of folder virtualization in Windows.
d. Knowledge of the various security features built into Windows, and the forensic implications related to these features.
e. Knowledge of the various virtualization features built into Windows, and the forensic implications related to these features.

IV. Windows Registry

a. Understanding of the limitations of examining a live registry, and knowledge of ways to bypass permission restrictions.
b. Understand how to capture a live registry.
c. Understanding of the purpose and structure of the component files that are synthesized to create the Windows registry at system boot.
d. Knowledge of how to search for and recover registry data located in unallocated space.
e. Understand the concept of “registry virtualization.”
f. Be able to identify and extract key data from a “dead” registry.

g. Be able to use the Windows registry to resolve unfamiliar file types and to gather potentially relevant data about software no longer installed on the system.
h. Understand the importance of restore points and volume shadow copy services as they relate to previous versions of component registry files.
i. Understand the protected storage services of the registry, and know how to access protected data that may be available.

V. Windows Artifacts

a. Knowledge of common Windows artifacts and their locations.
b. Knowledge of how the creation and longevity of various Windows artifacts are controlled by Windows registry settings.
c. Knowledge of Windows artifacts based on Windows installation defaults; and an understanding of the potential forensic relevance.
d. Ability to recover "previous versions" of files as well as the ability to mount and recover data from Windows backup infrastructure.
e. Ability to locate, mount and examine Virtual Hard Disk (VHD) files.
f. Understand Windows Encryption schemes; and knowledge of strategies for dealing with encryption.
g. Understand Windows event logs and knowledge of common event log entries that can be of forensic relevance.
h. Knowledge of how to search for and recover various Windows artifacts from unallocated space.

VI. Live Memory Acquisition and Analysis

a. Understand what processes are running in the various Windows operating systems and understand what information is volatile.
b. Knowledge of methods for live memory acquisition and analysis.
c. Knowledge of the process lists and how to examine and interpret what processes were running on a Windows machine during the acquisition of memory.
d. Understanding of network information available in physical memory and how to correlate connections to a running process.
e. Understanding of how to extract data from an acquired memory capture.