



## The International Association of Computer Investigative Specialists

---

### Windows Forensics Examiner Core Competencies

#### IACIS Windows Forensic Examiner (WFE) Program

The WFE core competencies described in this document are a binding set of competencies that guide the training program to ensure that the skills and knowledge points are delivered within the training program.

#### **IACIS Windows Forensic Examiner (WFE) Core Competencies**

There are six competency areas addressed in the WFE Program:

- i. Windows Virtualization Technologies and inbuilt security mechanisms**
  - ii. Windows Partitioning Schemes**
  - iii. Windows File Systems**
  - iv. Windows Registry**
  - v. Windows Artifacts**
  - vi. Live Memory Acquisition and Analysis**
- 
- i. Windows Virtualization Technologies and inbuilt security mechanisms**
    - a. Understanding of virtualization concepts, definitions, and common technologies, such as Hyper-V and Windows Subsystem for Linux (WSL).
    - b. Ability to identify when virtualization has been used on a suspect computer.
    - c. Ability to locate, mount and examine common virtual hard drives.
    - d. Knowledge of the various security features built into Windows, and the forensic implications related to these features.
    - e. Understand Windows Encryption schemes, and knowledge of strategies for dealing with encryption.
  - ii. Windows Partitioning Schemes**
    - a. Ability to identify current Windows partition schemes such as MBR and GPT.
    - 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.

### **iii. Windows File Systems**

- a. Understanding of file system concepts, technologies, and metadata files.
- b. Ability to parse common metadata files.
- c. Understanding of common file system objects and how they are applied in the Windows operating system.

### **iv. Windows Registry**

- a. Understanding of the limitations of examining a live registry.
- 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 known 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.
- e. Understand Windows event logs and knowledge of common event log entries that can be of forensic relevance.
- f. Knowledge of how to search for and recover various Windows artifacts from unallocated space.

**vi. Live Memory Acquisition and Analysis**

- a. Understand how to capture memory from a computer.
- b. Understand how to examine a memory capture for Windows based artifacts.
- c. Understand what processes are running on a live system.
- d. Knowledge of how to examine and interpret what processes were running on a Windows machine at the time the RAM was captured.
- e. Knowledge of network information available in memory and how to tie connections to a running process.
- f. Understanding of how to carve data from an acquired memory capture.

<b>Submitted by:</b>	<hr/> Felicia DiPrinzio <hr/>
<b>Membership Review Period:</b>	<hr/> N/A <hr/>
<b>Draft of Policy Reviewed by Board:</b>	<hr/> February 13, 2024 <hr/>
<b>Date of Policy Ratification by Board:</b>	<hr/> April 3, 2024 <hr/>
<b>Effective Date:</b>	<hr/> April 4, 2024 <hr/>
<b>Final Version Identifier:</b>	<hr/> 1.1 <hr/>