IACIS

The International Association of Computer Investigative Specialists

IACIS Certified Forensic Computer Examiner (CFCE)
Core Competencies

IACIS Certified Forensic Computer Examiner (CFCE) Program

The CFCE 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.

Certified Forensic Computer Examiner Core Competencies
There are Seven (7) competency areas addressed in the CFCE Program:

I. **Pre-Examination Procedures and Legal Issues**
II. **Computer Fundamentals**
III. **Partitioning Schemes**
IV. **Windows File Systems**
V. **Data Recovery**
VI. **Windows Artifacts**
VII. **Presentation of Findings**

I. Pre-Examination Procedures and Legal Issues

a. Knowledge of the legal process, rules of evidence and the IACIS Code of Ethics and Professional Conduct as applicable to computer forensics, laws, and procedures.
b. Ability to explain on-scene actions taken for the preservation of physical and volatile digital evidence.
c. Knowledge of proper computer search and seizure methodologies to include photographic and/or scene sketch procedures and documentation.
d. Ability to establish, maintain and document a forensically sound examination environment.

II. Computer Fundamentals

a. Recognize and document various computer hardware and small-scale devices.
b. Understand the BIOS, UEFI and Boot sequence.
c. Understand binary, decimal and hexadecimal numbering systems to include bits, bytes and nibbles.
d. Knowledge of sectors, clusters, volumes and file slack.
e. Understand the difference between logical and physical drives.
f. Understand the difference between logical and physical files.
g. Knowledge of what happens when media is formatted.

III. Partitioning Schemes

a. Ability to identify current partitioning schemes.
b. Knowledge of individual structures and system areas used by different partition schemes.
c. Understand that partition schemes can be used with different file systems and operating systems.
d. Understand the difference between a primary and extended partition.
e. Define Globally Unique Identifier (GUID) and explain its application.

IV. Windows File Systems

a. Understanding of file system concepts and system files.
b. Understand FAT tables, root directory, subdirectories and directory entries.
c. Understand how FAT directories store dates and times.
d. Understand the structure of ExFAT directory entries.
e. Ability to distinguish, examine and analyze the NTFS master file table.
f. Understand the structure of $MFT records.
g. Understand the Standard Information, File Name and Data attributes, to include parsing their contents.
h. Understand how the $MFT stores dates and times.

V. Data Recovery

a. Be able to validate forensic hardware, software and examination procedures.
b. Ability to generate and validate forensically sterile media.
c. Ability to generate and validate a forensic image of media.
d. Understand hashing and hash sets.
e. Understand file headers.
f. Ability to extract file metadata from common file types.
g. Understanding of file fragmentation.
h. Ability to extract component files and data from compound files, to include database files.
i. Knowledge of encrypted files and strategies for recovery.
j. Knowledge of Internet and browser artifacts.
k. Understand Email headers.
l. Knowledge of search strategies for examining electronic evidence.

VI. Windows Artifacts

a. Understand the purpose and structure of the component files that create the Windows registry.
b. Be able to identify and extract important data from a registry.
c. Understand the importance of volume shadow copy services.
d. Knowledge of the locations of common Windows artifacts.
e. Be able to analyze the Windows thumbcaches.
f. Be able to analyze the recycle bin.
g. Be able to analyze link files and Jump lists.
h. Be able to extract and view Windows event logs.
i. Ability to locate, mount and examine virtual drive files.
j. Understand the Windows swap and hibernation files and the evidence they may contain.

VII. Presentation of Findings

a. Ability to draw sound conclusions based on examination findings.
b. Be able to report findings using industry standard/technically accurate terminology.
c. Ability to explain complex technical concepts or processes in terms easily understood by non-technical people.
d. Be able to give consideration to local legal requirements when undertaking a forensic examination.