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.

The core competencies have been identified through a job analysis process which identified the tasks and skillset for successful performance as a computer forensic examiner.

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

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

I. Pre-Examination Procedures

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

II. Computer Fundamentals

a. Recognize and understand the evidential potential of various computer hardware and small-scale devices.
b. Understand the BIOS, UEFI and Boot sequence.
c. Understand binary, decimal and hexadecimal numbering systems 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. Partition Schemes

a. Ability to identify current partition 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. File Systems

a. Understand file system concepts and system files.
b. Understand the structure of FAT directory entries.
c. Understand the structure of exFAT directory entries.
d. Ability to distinguish, examine, analyse, and parse the contents of the NTFS master file table, including the Standard Information, File Name and Data attributes.
e. Knowledge of deleted/orphaned files including how they are identified in their respective file entries.
f. Be able to identify file systems used by Apple and Linux.

V. Data Recovery

a. Understand hashing and hash sets.
b. Ability to generate and validate forensically sterile media.
c. Ability to generate and validate a forensic image of media.
d. Ability to capture data from Random Access Memory.
e. Understand file headers.
f. Understand file fragmentation.
g. Ability to extract file metadata from common file types.
h. Ability to extract data from compound files.
i. Knowledge of encrypted files/media and strategies for recovery.
j. Knowledge of Internet and Browser artifacts.
k. Understand Cloud storage and how to obtain the data.

VI. Windows Artifacts

a. Knowledge of the locations of common Windows artifacts.
b. Understand the purpose and structure of the component files that create the Windows registry.
c. Be able to identify and extract specific data from the registry.
d. Be able to analyze the Recycle Bin.
e. Be able to analyze the Windows thumbcaches.
f. Be able to analyze Shell Link files and Jump lists.
g. Be able to extract and examine Event Logs.
h. Understand the importance of volume shadow copy services.

i. Ability to locate, mount and examine virtual drive files.
j. Understand the 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.