IACIS

The International Association of Computer Investigative Specialists

Certified Forensic Computer Examiner (CFCE) Core Competencies

Overview

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 addresses each of these key tasks and its accompanying certification program, the Certified Computer Forensic Examiner (CFCE) measures one's ability to perform these key tasks in accordance with established standards.

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 used to evaluate proficiency within the certification program. The IACIS Standards Committee monitors both programs to ensure strict adherence to guidelines of the established core competencies.

IACIS is an accredited certifying body by the Forensic Specialties Accreditation Board (FSAB). The FSAB is an independent board established to accredit professional bodies that certify forensic scientists and other forensic specialists. IACIS is one of the first computer/digital forensic organizations to achieve this prestigious designation.

This is a challenging and exacting process designed to test the candidates' mastery of the CFCE core competencies. While students who complete the BCFE training program will be well prepared for entering the CFCE certification program, attendance at or completion of the BCFE program is not a requirement to enter the CFCE program.

Certified Forensic Computer Examiner Core Competencies

There are seven 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

Each of the competency areas is considered of equal importance, and CFCE candidates must meet the standards for each knowledge and skill point in each competency.

I. Pre-Examination Procedures and Legal Issues

a. Knowledge of search and seizure, legal process, and rules of evidence as applicable to computer forensics, laws, and procedures.
b. Ability to explain on-scene actions taken for the preservation of digital evidence.
c. Knowledge of proper computer search and seizure methodologies to include photographic and 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.
b. Understand the BIOS 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. Ability to distinguish, examine and analyze the NTFS master file table.
e. Understand the structure of $MFT records.
f. Understand the Standard Information, File Name and Data attributes, to include parsing their contents.
g. 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 from compound files.
i. Knowledge of encrypted files and strategies for recovery.
j. Knowledge of Internet 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 “dead” registry.
c. Understand the importance of restore points and 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.
h. Be able to extract and view Windows event logs.
i. Ability to locate, mount and examine VHD 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 legal boundaries when undertaking a forensic examination.