CCE Certification Competencies

The Certified Computer Examiner (CCE)® has evolved into one of the most desired certifications in the computer forensics industry. The certification is granted only after an applicant has completed a rigorous, standardized testing process. Additionally, an applicant is required to agree to and sign The ISFCE Code of Ethics and Professional Responsibility, submit a notarized statement that all work on the certification is done without assistance, undergo a criminal background check and achieve approval from the ISFCE Certification Board.

The goal of the following core competencies is to outline the necessary level of proficiency required for a valid CCE test candidate. The CCE applicant may or may not be tested on all subject areas listed below. The CCE testing process is designed to test an applicant's proficiency in several areas pertinent to computer forensics. The applicant is required to complete an online test and forensically examine three pieces of media, submitting a report after each examination.

The Certified Computer Examiner (CCE)® certification process is a pure testing process. CCE candidates are not permitted to solicit or accept assistance from anyone at any level after they register for the CCE certification process. Review and comment on CCE practical examination reports is not allowed. CCE candidates are required to abide by a signed ISFCE Code of Ethics and Professional Responsibility and are made aware of all testing requirements and guidelines at the beginning of the certification process:

"All work to complete the CCE certification process must be done solely by the individual CCE candidate. CCE candidates may not corroborate, work jointly, cheat or plagiarize other's work to complete the CCE process."

The following pages outline all core competencies that a candidate who is preparing to sit for the CCE Certification process is expected to have at minimum a basic familiarity. Note that this list does not specifically outline the detail into each of these items an examiner should have working knowledge of. Nor should a candidate expect each of the items to be tested on within the certification testing process. This list also serves as a guideline for ISFCE Authorized Training Centers in course development and alignment with the CCE Certification process.

Ethics

Understand ethics in practice (particularly privacy) and the CCE ethical approach.

- What are the requirements of professionals, privacy and confidentiality?
- What constitutes an ethics issue?
- ISFCE Code of Ethics and Professional Responsibility
- Filing an ethics complaint

Law

Awareness of the existence of key pieces of legislation related to digital forensics and understand that this legislation has a direct impact on the practice of digital forensics. Also ensure students are aware of what is expected of professional examiners in court. This content is not intended to interpret or teach specific law, but only to ensure students become familiar with the existence of such legislation and understand that legal counsel may be necessary to ensure work is done in compliance with legislation.

- Representation of facts
- Components of the Discovery Process
- Rules and regulations affecting digital forensics:
  - If operating within the United States, examples include:
    - The 4th Amendment
    - Electronic Communications Privacy Act
    - Privacy Protection Act
    - Digital Millennium Copyright Act
    - Stored Communications Act
    - 18 USC 2703(d)
    - Federal Rules of Evidence (basics)
  - If operating outside of the United States, refer to your country's individual laws and regulations.
- Cross border state licensing requirements for computer forensic professionals
- Subpoenas
- Search warrant
- Consent
- Legal process for civil and criminal cases
- Expert Testimony and process
- Daubert and Frye cases
- Courtroom behavior

Software

Understand software licensing and validation.

- Use of legal software
- Software licensing types
- Validation of Software
- Software versioning and problems associated with this issue
- Commonly used forensic utilities (types and some examples can be found at http://www.isfce.com/software.htm)

General Personal Computer Hardware Identification

Understand hardware specifically; hardware involved in imaging and data collection activities. Minimum requirements include visual aids and examples of hardware used, hands on demonstrations using hardware.

- Motherboard Connections
- Motherboard components and functions
- Optical drives
- Hard drives
    - IDE/PATA
    - SCSI
    - SATA
    - eSATA
    - Solid State drives
    - Other removable media
- RAID Connections and Issues
- Types of connectors and connections
- Other non-traditional

Commonly Encountered Media

Familiarity with all types of commonly encountered digital evidence and how to handle that evidence properly.

- Floppy diskettes
- Hard drives
- Solid State Hard Drive / SSD
- Optical media
- USB thumb drives

- Flash Cards (SD, MicroSD etc)
- Other storage media
- Online storage

Overview of Networks

Understand networking and its impact on both forensic evidence and site seizures.

- Networking Overview
- Networking devices which need to be seized
    - Wireless Nodes
    - Routers
    - Other Network Components

- SAN/NAS
- Acquisitions via Networks
- Privacy issues and networking, i.e. encryption
- Wireless issues
- Cloud Issues

Mobile Device Forensics

Ability to perform forensic examination of mobile devices.

- Current OS's (iOS, Android, RIM, Windows Mobile)
- Networks
    - GSM
    - CDMA

- Connections
    - WiFi
    - Bluetooth

- Internal Storage Options
    - RAM
    - Removable (SD, MicroSD, etc.)
    - SIM

- Evidence Handling
    - Network isolation
    - Faraday bags
    - Power
    - Identification
    - Physical inspection

    - Manual Scroll / Photographing
    - Remote destruction

- Overview of acquisition tools
- Synchronization artifacts
- Basic analytics
    - Pictures
    - Contacts
    - Messaging
    - Emails
    - Call history
    - Geolocation
    - Apps

Review of Commonly Encountered Operating Systems

Familiarity with commonly encountered OS with focus on most common.

- Boot process
- DOS
- Windows
- Linux/Unix
- Mac (Leopard and Snow Leopard plus difference in older systems)
- Mainframes

Acquisition Process

Understand standard procedures involved in conducting a complete forensic case.

- Acquisition of machines
- Pulling the plug vs. live capture analysis
- Evidence labeling and management
- Chain of Custody Procedure
    - Document connections/attached devices
    - Record serial numbers
    - Photograph internal/external configuration
    - Document internal connections
    - Indicate transfer of custody through signature(s), date and time
    - Access logs
    - Measures taken to protect media; packaging

- Understand safe boot procedures and forensic boot disks
- Encryption
    - Identification

- Defeating
- Common methods
  - Media
  - Container
  - File

Forensic Examination Procedures

Understand the process of casework and can develop meaningful reporting suitable for submission

- Maintaining evidence integrity
- Imaging of evidence
- Ensuring evidence image authenticity via hashing
- Slack space
- Text gathering
- Prepare examination media
- Process forensic image
- Document examination process
- Controlling / security access logs etc for image media
- Disposition of evidence
- Preparation of documents for trial
  - Summation and Analysis sections
  - Format examples
  - Appendices and Glossaries

- Report preparation

File Systems

Understand the following common file systems in use and can explain key concepts.

- Master Boot Record
- Boot Parameter Block (BPB) components
- FAT
  - File:
    - Creation
    - Deletion
    - Recovery

  - File artifacts
  - Pertinent operating system files including WIN386.SWP

- NTFS
  - File:

        - Creation
        - Deletion
        - Recovery

    - File artifacts
    - Pertinent operating system files including the Pagefile
    - Registry
    - MFT

- Optical media
    - General Formats and Types
    - Open and closed sessions

Media Geometry

Understand how drives and storage work physically and logically.

- Bits
- Nybbles
- Bytes
- Sectors
- Clusters
- File slack and sector slack
- Unallocated space
    - SSD wear leveling

- CHS addressing
- Logical based addressing
- Addressing translation
- Disk partitioning
- Partitioning utilities
- GUID Partition Tables GPT
- DCO's and HPA's

Preparation of Sterile Examination Media and Imaging

Know proper procedure for forensic media and imaging techniques.

- Disk wiping
- Disk formatting
- Hashing
- Installation of operating system
- Installation of forensic software/tools

Low Level Analysis

Understand manual file recovery.

- General use of a hex editor
- Hexadecimal notation
- Explanation of ASCII
- Explanation of Unicode
- Explanation of offsets

Specific Processing Issues

Additional topics which may prove critical to forensic examinations.

- Registry Analysis
- Password cracking
- Document metadata
- Data carving
- Internet history analysis
- Analysis of pertinent operating system files:
  - .lnk files
  - Prefetch
  - Recycler

- Shadow volume processing
- Email tracing
- Timeline analysis
- RAID handling

Practical Examination Skills

Practical experience in a controlled environment dealing with real world scenarios and examination techniques.

- File recovery
- LFN recovery
- Formatted disks
- Data carving
- NTFS exercises (MFT overview, boot record overview, single file recovery)
- CD/DVD analysis
- Password cracking
- Mobile forensics