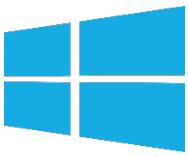
IACIS

Windows Forensic Examiner

2019-2020



Contents

1. Syllabus & Competencies

Program Overview

The IACIS WFE Training Program is a 36-hour course of instruction, offered over five (5) consecutive days. The program is designed to provide students with a detailed study of the Windows Operating System.

Through a variety of lectures, instructor-led and independent hands-on practical exercises students will study the Windows Operating System in far greater detail, and with far more specificity regarding critical areas of forensic focus, than what can be accomplished in the more generalized, overview perspective of the BCFE Training Program.

In short, this program will focus on how a variety of Windows Operating Systems work “under the hood”, with a focus on the most current/common versions. At the conclusion of this course, students will have a clearer understanding of various operating system artifacts and why they present as they do, and how knowledge of these artifacts can play a significant role in the forensic and investigative process.

The WFE Training Program champions a forensic tool-independent approach to learning. This approach allows for a deeper exploration of the underlying subject matter than might be afforded in other programs which are designed to complete a particular task or view/extract a particular artefact.

The WFE Training Program is designed to build on and expand the students existing forensic knowledge and skillset and is not an entry level class. Prospective students should reference the “Prerequisites” section elsewhere in this document for additional information about expectations for students.

The WFE Training Program will assist students in preparing for their CAWFE certification, however the training program is not taught to the certification, instead, students are recommended to take notes, participate, and make the most of the classroom environment. The material provided to students will be used as part of certification process, however, reading outside of the provided material is advisable and will benefit the student in obtaining a deeper understanding. As an example, the WFE material includes information about Artifact A, but the trainers focus on Artifacts B, C and D. The certification may include questions on Artifacts A and D.

Certification Program Description

The Certified Advanced Windows Forensic Examiner (CAWFE) program is administered by the IACIS Advanced Certification Subcommittee. The CAWFE Certification is drawn from a set of competencies approved by several committees and the IACIS Board of Directors.

The CAWFE program is an assessment process and not a simple, single test. The process is composed of two separate assessments. The first component is the written examination. The second component is a practical assessment whereby candidates must answer questions that relate directly to a series of image files and Windows artifacts. Both assessments are completed online.

Application for the CAWFE Certification program must be made directly to the IACIS Advanced Certification Subcommittee prior to being enrolled in the CAWFE assessment program. If the candidate is required to pay a fee to register for the CAWFE certification, the requisite fee must be paid to the IACIS Treasurer BEFORE submitting the CAWFE application.

Prerequisites

- Membership required.
- Basic Computer Forensic Examiner [BCFE] course **highly recommended** but not required.
- Certified Forensic Computer Examiner [CFCE] certification **highly recommended** but not required.
- A fundamental understanding of how to navigate through hex structures, for example; parsing the MBR and GPT structures and common NTFS metadata files would be advantageous.
- A fundamental understand of how to use the CMD prompt would be **highly recommended**.
- Students are expected to have a strong command of baseline computer forensic principles and methodologies as well as having computer forensic examination experience with Windows based computers.

Windows Forensic Examiner Core Competencies

The WFE core competencies described below are a binding set of competencies that guide both the training and certification programs to ensure that the skills and knowledge delivered within the training program are the same set of standards evaluated within the certification program. The IACIS Standards Committee monitors both programs to ensure each adheres to strict guidelines of the established certification competencies.

There are six (6) competency areas addressed in the WFE Program:

1. Virtualization

a) Understanding of virtualization concepts, definitions and common technology.
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) Understanding of how to virtualize a suspect image.

2. Windows Partitioning Schemes

a) Ability to identify current Windows partition schemes.
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.

3. 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.

4. 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.

5. Windows Artifacts & more

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 of not finding expected artifacts.
d) Ability to recover "previous versions" of files as well as the ability to mount and recover data from Windows backup infrastructure.
e) Understand Windows Encryption schemes; and knowledge of strategies for dealing with encryption.
f) Understand Windows event logs and knowledge of common event log entries that can be of forensic relevance.
g) Knowledge of how to search for and recover various Windows artifacts from unallocated space.
h) Knowledge of the default folder structure and fully qualified paths created during the Windows installation process, and how these might change during a customized installation of Windows.
i) Understand the use of folder virtualization in Windows.
j) Knowledge of the various security features built into Windows, and the forensic implications related to these features.

6. 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.

Required Equipment and Supplies

Students will be supplied with all the materials needed to successfully complete the WFE training program.

Students are not required to bring a computer with them to the training program: IACIS will provide all computers required for use during the training.

Students may bring a laptop computer or other computing device with them for personal use outside of the classroom. Students are not permitted to use their personal laptop computers, tablet computing devices, PDAs, cellular telephones, and other personal computing devices in the classroom.

Finally, under no circumstances shall students install any software on any classroom computer except as directed by an instructor.

Automated Forensic Software and Hardware

IACIS adopts a forensic tool-independent approach to teaching computer forensics. IACIS does not endorse or support any particular forensic software tool, forensic hardware device, or any particular software program.

Automated forensic software tools might be used during instructional modules to illustrate teaching points and to facilitate the manual study of data structures and data recovery by using a limited functionality of a particular tool or suite of tools. Similarly, particular forensic hardware devices might also be used to teach students about particular forensic processes.

In cases where use of any particular hardware item or software program of any type is required for an instructor led activity, in-class practical exercise, or independent laboratory exercise, students will be provided access to the particular hardware item or software program, and there will be instruction as to the use of that particular hardware item or software program for the *limited purpose of the activity at hand*.

Regardless of what hardware items or software programs might be used, the purpose of any instruction provided with respect to the items or programs, is solely intended for the immediate purpose of the instructional block at hand, and is *not* designed to provide specific training on that hardware item or software program.

Attendance and Program Conduct Requirements

The WFE training program provides thirty-six (36) hours of instruction (lunches/breaks are not included within this 36 hours). The program runs for five (5) consecutive days between 08:00 AM to 5:00 PM, the final day should finish by 03:00 PM. There is a 60 minute lunch break each day, usually from 12:00 noon to 1:00 PM. Trainers aim to allow for a short break at the top of each hour.

On the first day, from 8:00 AM to 10:00 AM, this time is used for administrative purposes. In this time, staff and students will introduce themselves. Following this, information about the week ahead will follow. The two hours is considered part of the overall program due to the vital information provided. The time allocated may be reduced assuming a smaller class.

On the last day of the program the entirety of the instructional day (8:00 AM to 3:00 PM) is dedicated to normal instruction, per the published class schedule, meaning that students should not expect early dismissal from class on that day, and should consider this when budgeting and planning lodging and travel arrangements.

Students are expected to attend all classroom sessions. Classes begin promptly, and students are expected to be prepared to begin the instructional day on time.

IACIS understands that unforeseen circumstances and emergency situations may arise, and so students are permitted to briefly leave the classroom to deal with such situations. That said, students who have absences from class may not be issued a certificate of completion at the end of the program, and may not qualify for entry into the CAWFE process.

While students are encouraged to take notes during classes, activities, and laboratory sessions, students are not permitted to use their personal laptop computers or other personal computing devices of any type during any classes. Similarly, **students are not permitted to use any audio or video recording devices**, at any time during any classroom or laboratory session.

Students are expected to dress professionally and appropriately for a “business casual” environment (collared shirt, slacks, etc.). Shorts, tank tops, sandals, flip flops, and similar casual dress is not permitted in the classroom at any time.

Something for students to consider is that classrooms are air conditioned, and the temperature is set lower than what may be expected. There may be times when all of the computers are operating and it may get warm in the classroom, however more often the room can become too cold for some students. Please consider dressing in light weight clothing and bringing a sweater or light jacket to wear, if needed.

Students must be aware that the classroom is small, with a class size of 20-30 students. In such an environment, even minor distractions can make it difficult for others to hear or to remain focused on the instructor. Students are asked to be courteous and aware of their fellow students.

During classes, students are expected to be attentive and fully engaged. Cell phones must be put on "vibrate" or "silent" mode. Communicating with a mobile device is prohibited in the classroom whilst teaching is underway.

Class Schedule

The WFE training team provide the program dynamically to our students, and so the schedule below is a guide, insomuch as, topics may be moved around / condensed or expanded as the trainer deem appropriate on the day and during the class.

Teaching Blocks	Mon	Tue	Wed	Thurs	Fri
Introductions / Syllabus	AM				
Virtualisation	AM				
Windows Partition Scheme	PM				
Windows File System	PM				
EFS	PM				
Security Features and Encryption		AM			
Introduction to Windows Registry		AM			
Registry Block Structures		AM			
SOFTWARE Registry		AM			
SAM Registry		PM			
Shell Links		PM			
Jump Lists		PM			
ShellBags		PM			
Thumbscache			AM		
Browsers			AM		
Mail			PM		
Notifications			PM		
OneDrive			PM		
Cortana				AM	
SYSTEM Registry				AM	
Event Logs				AM	
NTUSER Registry				AM	
SuperFetch / Prefetch				AM	
Restore / Shadow Copies				PM	
Windows.old				PM	
Intro to RAM Capture & Analysis					AM/PM