Advanced Windows Forensic Examinations
2015 – 2016

Syllabus

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 detailed study of the Windows operating system and to prepare students to enter the IACIS Certified Windows Forensic Examiner (CWFE) process.

Through a variety of lectures, instructor-led and independent hands-on practical exercises, and independent laboratory activities, 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 the primary focus on the most current version. 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.

Like all IACIS training programs, the WFE Training Program champions a forensic tool-independent approach to learning to computer forensics. This approach allows for a deeper exploration of the underlying subject matter than might be afforded in other programs which are designed to teach students how to use a particular forensic tool to complete a particular task or view/extract a particular artifact.

The WFE Training Program is designed to build on and expand one's existing forensic knowledge and skill set 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 is the preparatory course for the Certified Windows Forensic Examiner (CWFE) certification process. This course will provide the students with a majority of the information, though written material, classroom lectures and practical exercises, needed to be successful during the CWFE process. Students are encouraged to participate in the instructor staffed laboratory nights for additional one-on-one assistance on various topics.

In addition, students considering entry into the CWFE process should consider exploring other specialized programs offered by IACIS.

Certification Program Description

The *Advanced Windows Forensic Examiner* (AWFE) certification process is designed to build on the basic computer forensic examination skills acquired during the IACIS Certified Forensic Computer Examiner (CFCE) certification process. Candidates may begin the process by attending the 40-hour *Advanced Microsoft Windows Forensic Examiner* training program which is offered during the annual IACIS conference. This optional training program provides focused and detailed instruction in the forensic examination of computers that run under the Windows XP and later family of operating systems.

The certification will require two components:

1. A challenging practical exercise that must be completed under strict time limits, and which tests the candidate's ability to apply his/her training, skills, knowledge, and experience to a real-world scenario and a written examination.
2. A comprehensive written exercise that tests knowledge points across the entirety of the various operating systems and file systems that are studied. The certification examination is the actual written instrument.

Prerequisites

There is no formal computer forensics credentials required for entry into the WFE program beyond applicable IACIS membership requirements. Specifically, the IACIS CFCE is not a required prerequisite for students to enroll in this program however, this program assumes that students are already comfortable and conversant with critical internal structures of the Windows family of operating systems and with file systems in general, specifically NTFS.

Additionally 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.

Students should have basic knowledge in the following areas:

1. Logical disk structures including the Master Boot Record (MBR), Volume Boot Record (VBR) and Partition tables.
2. File Systems including NTFS, FAT 32, FAT 16, and FAT 12. The student should understand the key data structures and general performance features (and limitations) of these file systems.
3. Window Registry Files and Keys including some experience with conducting registry examinations.

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 points delivered within the training program are also 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:

I. Windows Partitioning Schemes II. Windows File Systems III. Windows Defaults and Standard Functionality IV. Windows Registry V. Windows Artifacts VI. Live Memory Acquisition and Analysis

I. 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.

II. Windows File Systems

a) Understanding of file system concepts and system files.
b) Knowledge of the basic architecture of volume boot sectors.
c) Understanding of the various Windows file system concepts and technologies.
d) Understanding of common file system objects and how they are applied in the Windows operating system.

III. Windows Defaults and Standard Functionality

a) Understand the default installation process for stand-alone installations of Windows, and understand how the installation process can be customized by end users and by computer manufacturers.
b) 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.
c) Understand the Windows boot process.
d) Understand the use of folder virtualization in Windows.
e) Knowledge of the various security features built into Windows, and the forensic implications related to these features.
f) Knowledge of the various virtualization features built into Windows, and the forensic implications related to these features.

IV. Windows Registry

a) Understanding of the limitations of examining a live registry, and knowledge of ways to bypass permission restrictions.
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.

V. Windows Artifacts

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) Ability to locate, mount and examine Virtual Hard Disk (VHD) files.
f) Understand Windows Encryption schemes; and knowledge of strategies for dealing with encryption.
g) Understand Windows event logs and knowledge of common event log entries that can be of forensic relevance.

h) Knowledge of how to search for and recover various Windows artifacts from unallocated space.

VI. Live Memory Acquisition and Analysis

a) Understand what processes are running in the various Windows operating systems and understand what information is volatile.
b) Knowledge of methods for live memory acquisition and analysis.
c) Knowledge of the process lists and how to examine and interpret what processes were running on a Windows machine during the acquisition of memory.
d) Knowledge of network information available in memory and how to tie connections to a running process.
e) Understanding of how to carve data from an acquired memory capture.

Required Equipment and Supplies

Students will be supplied with all of the materials needed to successfully complete the WFE program. This includes a program manual that includes instructor-led practical and independent laboratory exercises, various hardware and software tools/items, and other items and resources that are needed for particular courses or that might be of benefit later, in the field.

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, pad/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 espouses a forensic tool-independent approach to teaching computer forensics. To this end, IACIS does not endorse or support any particular forensic software tool, forensic hardware device, or any particular software program generally.

The above notwithstanding, automated forensic software tools might be used during instructional modules to illustrate teaching points and to facilitate 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 program provides thirty-six (36) hours of instruction across various specialized courses. The program runs for five (5) consecutive days, Monday through Thursday from 8:00 AM to 5:00 PM, and from 8:00 AM to 12:00 noon on Friday. Each day, Monday through Thursday, there is a one (1) hour break for lunch from 12:00 noon to 1:00 PM. Courses are timed using the traditional "50 minute hour" to allow for a short break at the top of each hour.

On the first day of the program, the first hour (from 8:00 AM to 9:00 AM) is used for administrative purposes such as staff introductions and providing students information about the course of study to follow. This hour is considered part of the overall program due to the vital information provided.

On the last day of the program the entirety of the instructional day (8:00 AM to 12:00 Noon) is dedicated to normal instruction, per the published class schedule, meaning that students should not expect early dismissal from class on that day, and so should consider this when budgeting and planning lodging and travel arrangements.

Students are expected to attend all classroom sessions. Classes begin promptly at 8:00 AM, and students are expected to be prepared to begin the instructional day at that time. With the exception of the final day of the program when the program closes at 12:00 noon, classes will continue until 5:00 PM on each class day.

While not required, students will have ample opportunity to attend evening laboratory sessions to work independently or with an instructor.

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 CWFE 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 one may typically expect to keep the room comfortable given the heat that can be generated by a 20-25 students and computers. At times, however, the environment can be difficult to control: 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. So one might consider dressing in light weight clothing and bringing a sweater or light jacket to wear, if needed.

Students must be mindful of the fact that the classroom is small, with a class size of 20-25 students. In such an environment, even minor distractions can make it difficult for others to hear or to remain focused on the instructor. So, then, 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, and sending text messages with cell phones and other hand-held devices is prohibited in the classroom.

Class Schedule

	Monday	Tuesday	Wednesday	Thursday	Friday
8:00	Introduction and Administrative Tasks	Windows Registry	Windows Registry	Windows Artifacts	WFE Practical Exercise
8:50-- -9:00	Break	Break	Break	Break	Break
9:00	Software and Tools Computer Setup	"	"	"	"
9:50-- -10:00	Break	Break	Break	Break	Break
10:00	"	"	"	"	"
10:50-- -11:00	Break	Break	Break	Break	Break
11:00	Windows Installation and OS Defaults	"		"	"
12:00-- -13:00	Lunch	Lunch	Lunch	Lunch	Program Close
13:00	"	"	Windows Artifacts	"	
13:50-- -14:00	Break	Break	Break	Break	
14:00	Windows Virtualization	"	"	"	
14:50-- -15:00	Break	Break	Break	Break	
15:00	"	"	"	"	
15:50-- -16:00	Break	Break	Break	Break	
16:00	Windows Security Features	"	"	"	
17:00	End of Day	End of Day	End of Day	End of Day	