Applied Computer Forensics
2015 – 2016

Program Overview

The Applied Computer Forensics course takes the students through a realistic case scenario built on a Windows 10 Operating System with situations that require the use of several different forensic tools to complete an investigation. During the class, we will compare and contrast the most current versions of the full forensic suites, EnCase, FTK and X-Ways. In addition, several task-specific forensic tools will be used during the class. Through these comparisons, the students should become more prepared to choose the most suitable tool for the type of tasks they need to perform during their examinations. Students will also learn about details they may have been missing during their examinations. The course takes a more in-depth look at how our tools handle the artifacts we aim to examine and should strengthen their ability to draw conclusions based on their findings.

Competencies:

To create an understanding of how the major forensic suites handle the same jobs and to make students familiar with the interface of all three forensic suites to assist them in being able to more easily communicate work issues with users of other tools or transfer to another tool more seamlessly. Including:

- Be able to create a case and add evidence to several different tools.
- Configure third party viewers.
- Know what date and time terminology for each of the tools mean in relation to what is taught for file dates and times in the IACIS BCFE and in relation to the other tools.
- Be able to perform basic processing.
- Indexing
- Hashing
- Regular expression and GREP searching
- Filtering
- File Carving and building custom file carvers.
- Understand what is meant by column names and be able to customize column settings to suit the preferences of the examiner.
- Bookmarking, exporting and basic report component building

To understand what the tools are displaying when reporting on certain artifacts such as link files, jump lists, prefetch data, alternate data streams, Internet browser artifacts, EXIF data, Recycle Bin, thumbcache, event logs and others to be more prepared to draw conclusions from the analysis of these artifacts.

Develop strategies for investigating case and working through a computer exam.

Understand how deeper examination of artifacts can be advantageous in certain analysis situation and be able to choose and effectively use an appropriate tool per artifact to find the desired information.

Be able to view common artifacts in hexadecimal to gain a better understanding of what forensic tools are calling from when reporting artifact data to the examiner.

Understand the limitations of the major forensic suites when handling certain types of data and know when a specialized tool may be a better solution.

Analyze problems and uncommon findings and develop strategies to address these problems.

Utilize web browser form history data to further an investigation.

Be able to validate the results of your tools.

Be able to generate an effective report for the examiner, and the end user of the report (Prosecutor, case agent etc.)

Be able to make the data fit the report in a way the examiner wants it to instead of trying to force a default tool report into their report.

Export file data from tools and import it into Excel to perform basic sorting, filtering, cell formatting and other cell functions to customize case data in an understandable and presentable way.

Customize reporting settings of full forensic suites to display information desired by the examiner.

Generate a synopsis of examination findings in the beginning of case report designed for those with short attention spans and have that synopsis refer to more detailed data contained later in the report.

Generate a detailed report of findings that the examiner can refer to if the need arises to explain findings at a later time.

Attendance and Program Conduct Requirements

The ACF program provides approximately thirty-six (36) hours of instruction. The program runs for one week, Monday through Thursday, from 8:00 AM to 5:00 PM and Friday from 8:00 AM to Noon, with a one (1) hour break for lunch each day 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 programming to follow. That hour is considered part of the overall program due to the vital information provided.

Students are expected to attend **all** training 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, classes will **always** continue until 5:00 PM on each class day. On the final day, the program will close at 12:00 Noon.

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

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 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 apparel are **not** permitted in the classroom at any time.

Something for students to consider is that the room is 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 large group people and computers. At times, however, when the computers are idle, the room can become too cold for some students, so one might consider bringing a sweater or light jacket to wear.

Students must be mindful of the fact that even small distractions in the classroom 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, and sending text messages with cell phones and other hand-held devices is prohibited.