



Mobile Device Forensics



IACIS 2015

Mobile Device Forensics Program Description and Syllabus

Program Overview

The IACIS MDF Training Program is a 40-hour course of instruction, offered over five (5) consecutive days. The program is designed to provide students with detailed study of the examination of mobile devices including cell phones and tablets. Some experience with cell phone exams is required, as this course is not a “how to use this tool” course. During the course of instruction, students will become familiar with the way tools recover cell phone data, and the type of extractions. Students will analyze the results by diving deep within the file systems of mobile devices, and recovering data which tools frequently miss, learning to recognize and decode that data by hand. Students will become familiar with the latest capabilities for by passing locked devices running Apple’s iOS and several versions of Android. The hands on practical exercises use some of the best commercial and open source tools available. While expertise with the command line is not a requirement, students should be competent in the use of commands to do basic navigation and management of their system at the Windows command line.

Attendance and Program Conduct Requirements

The MDF program provides approximately thirty-six (40) 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 3:00 PM.

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.

Time	Monday	Tuesday	Wednesday	Thursday	Friday
8-9	Introduction	NAND/FLASH RAM	Apple iOS Devices	Breaking Into Android OS Phones	Decoding/Carving Apps
9-10	Cellphone Terminology, Refresher	SQLite	Apple iOS Devices	Breaking Into Android OS Phones	Decoding/Carving Apps
10-11	Cellphone Terminology, Refresher	SQLite	Apple iOS Devices	Breaking Into Android OS Phones	Decoding/Carving Apps
11-12	Cellphone Terminology, Refresher	SQLite	Android OS File System	Breaking Into Android OS Phones	Decoding/Carving Apps
12-1	LUNCH	LUNCH	LUNCH	LUNCH	LUNCH
1-2	Cellphone Terminology, Refresher	Card Skimmer Exams	Android OS File System	Decoding/Carving Apps	iOS Backup Files
2-3	Cellphone Terminology, Refresher	Apple iOS Devices	Android OS File System	Decoding/Carving Apps	Student Practical Results and Course Feedback
3-4	Cellphone Terminology, Refresher	Apple iOS Devices	Android OS File System	Decoding/Carving Apps	
4-5	Cellphone Terminology, Refresher	Apple iOS Devices	Android OS File System	Decoding/Carving Apps	