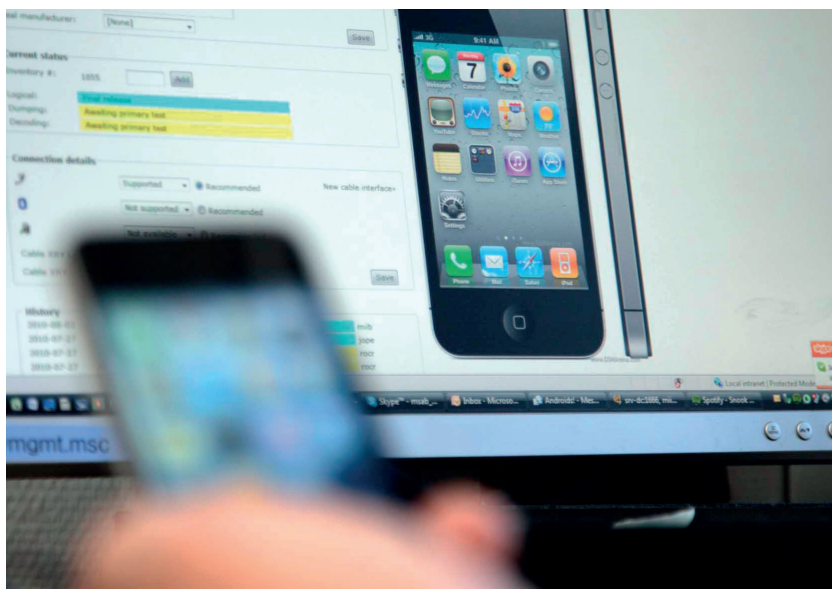


# IPHONE FORENSICS COURSE



THIS IS A SPECIALIZED COURSE FROM MICRO SYSTEMATION DESIGNED FOR STUDENTS WANTING TO TAKE THEIR XRY EXPERIENCE TO THE NEXT LEVEL OF SMARTPHONE FORENSIC EXAMINATIONS.

Students attending this course will learn how to complete a forensic examination of the Apple iDevices (iPhone, iPod Touch & iPad). They will learn when it's possible to recover deleted data and how to recover stored and deleted data from the devices; including calls, voicemail, notes, messages, media files and GPS information.

The course covers how to examine data stored by user apps, e.g. Facebook, Google Maps, Skype, Twitter, Viber and Whatsapp. It will go into detail about where app data can be located and the different tools available to assist you in deeper analysis of the data.

Students will learn how to acquire and retrieve GPS locations of actions made by the device owner. They will also be taught how to get the most out of the MSAB Forensic Pack using both XRY Logical and XRY Physical analysis; in order to extract the maximum

information from these types of devices.

The course is primarily lab based and exercises are based on different iOS versions and iDevices. An important part of the course is spent on examining data stored by system and user applications.

At the end of the two day course, students will be expected to complete an assessment to ensure the quality of the training. Students who successfully complete the test will be certified and issued with a certificate, ensuring that they are competent to explain the information they are producing from the system for some of the most popular and iconic mobile devices.

Target users are:

- Law enforcement
- Military intelligence operatives
- Forensic investigators
- Corporate fraud investigators

## COURSE OUTLINE

### DAY 1

- >> **Hardware, iDevices**  
iPhone 4/4S, 3G/3GS  
iPod Touch and iPad
- >> **Capabilities**  
Accounts, Chat Messages  
Bookmarks, History  
Web browser, Google Maps,  
Dynamic Keyboard Cache
- >> **iTunes**  
Activation, Sync  
Backup, Remote Access
- >> **Acquisitions, Extraction**  
Identify geotagged photos and plot them on a map  
Locate and interpret traces of Bluetooth, Wi-Fi and VPN  
Locate and interpret traces of Google Maps, YouTube and Safari usage
- >> **iDevice acquisition, Extraction**  
Jailbreaking –Pros/Issues  
Pass code  
Deleted data
- >> **Physical extraction**  
Analysis of Physical Extraction  
Deleted data: Call list, Messages, Media files

### DAY 2

- >> **HSF+ and Analysis**  
iDevice File System  
SQLite db  
PList Configuration files
- >> **Challenges**  
Current challenges with iDevices
- >> **Back up**  
Printing and export of reports  
Saving subsets  
Protecting XRY files containing sensitive data
- >> **System apps**  
Call list, Contacts, Messages, Notes etc.  
Locations of System App Data in SQLite db
- >> **User (3<sup>rd</sup> party) apps**  
Investigating different apps  
Locations of User App Data in SQLite db  
Facebook, Heytell, Runkeeper, Skype, Twitter, Viber, Whatsapp etc.

The course is primarily lab based and exercises are based on iPhone and iPod touch.  
Contact details: [training@msab.com](mailto:training@msab.com).