



Apple Mac Forensics: Hands-On

Apple is becoming increasingly popular and as a consequence, computers running Mac OS X operating systems are increasingly becoming the subject of forensic investigation.

What you will learn

- HFS+ in detail
- Identify and make sense of OS X configuration and logging
- Data stored in Time Machine

Who should attend

This course is aimed at forensic investigators who have gained experience dealing largely with Windows based systems and are now finding themselves in the situation where they increasingly need to understand the data structures and evidence potential in Mac OS X environments.

Course style

This is a Hands-On course where delegates will carry out exercises, applying the principles, knowledge and techniques learnt during the course.

An examination is held on the final day. Successfully completing this examination earns delegates the Certified Mac Forensics Specialist (CMFS) certification.

Prerequisites

- Principles & general guidelines surrounding forensic investigation
- Preliminary case considerations to evaluate when beginning a forensic investigation

To Book Call:

0870 600 1667

Duration: 3 days

Cost: £1498.50 + VAT



CPE Credits: 24

Course content highlights

In this intense course, detailed presentations will alternate with hands-on practical exercises, covering many relevant aspects of the Mac OS X operating systems. These are some of the key topics we will cover:

Key differences between the original Mac OS operating systems and Mac OS X. As Mac OS became a Unix-variant, it introduced a whole new way of thinking about file ownership and permissions.

It still kept the original Mac way of thinking in terms of storage of Metadata: Lots of it! We will have a look at what information Mac OS X stores about files and at HFS+, the new file system OS X needed to actually facilitate all that. We will also ask and answer the one file system question that is more Mac than any other: What, exactly, is a resource fork?

Mac OS X adopted the GUID Partition Table scheme for its partition layout on the hard drive. Unlike Vista, which also supports GPT but does not generally use it, OS X will prefer this partitioning scheme. We will delve into partition setup using GPT – you will be interested in case your forensic tool of choice does not like GPT and does not successfully search for HFS+ partitions, either.

Since Mac OS X Leopard (v10.5, October 2007), the operating system comes with a new feature forensic investigators will be interested in: Time Machine. As the operating system notoriously suggests to the user to use Time Machine to automatically create backups at fixed intervals, many Mac users will have backups created that might contain data of relevance even if the current system does not. As Apple puts it: Set it, then forget it. The user just might have, but we should not!

Professional Training Authored By Experts