

COURSE OUTLINE

DIGITAL FORENSICS

Certified Mac Forensics Specialist (CMFS)



SPECIALIST-LEVEL COURSE

Cost: **£1,950.00 + VAT**

Duration: **3 days**

This specialist-level course is for experienced forensic investigators whose role requires them to capture, examine and interpret data from Mac systems.

COURSE OVERVIEW

Apple is increasing its market share in both the private and commercial/corporate marketplace. This three-day course concentrates on identifying what is, how can I find, extract, decode and interpret the data stored on an Apple device from a forensic practitioner's perspective, using hands-on exercises to demonstrate and reinforce understanding.

THE SKILLS YOU WILL LEARN

Upon completion of the course you will have:

- Collected volatile data from a live Mac system
- Explored different approaches to imaging and decrypting Mac systems
- An understanding of the new APFS file system
- Practical knowledge of Apple partitioning schemes and the HFS+ file system
- Examined a Mac system for configuration of user accounts, Application/data
- An understanding of Time Machine
- Interpreted data from unified logs, plists and SQLite databases

KEY BENEFITS

This course will give you the opportunity to:

- Develop confidence when faced with Apple systems and required to collect data from Mac systems
- Learn effective techniques to process and interpret data and artefacts from Mac OS

- Learn effective techniques for the identification and interpretation of forensic artefacts on Apple systems
- Improve your ability to respond effectively to a wider range of forensic incidents

WHO SHOULD ATTEND

Forensic practitioners, systems administrators and cyber investigators who want to extend their experience with Window-based systems to the Mac environment.

PREREQUISITES

Completion of the PA CFIP course is highly recommended. Otherwise you will need:

- Knowledge of the principles and guidelines surrounding forensic investigation
- Basic knowledge of data structures, e.g. binary and hexadecimal

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Certified Mac Forensics Specialist (CMFS) qualification.



To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com

COURSE OUTLINE

DIGITAL FORENSICS

Certified Mac Forensics Specialist (CMFS)



SPECIALIST-LEVEL COURSE

Cost: £1,950.00 + VAT

Duration: 3 days

“An excellent course which gave a thorough overview of Mac Forensics, the HFS+ file system and important artefacts and their locations on the file system. The exercises supported the theory well and helped build on the course content. As a non-Mac user, I now feel a lot more confident working with Macs, not just for forensic analysis, but generally.”

CMFS Delegate

The Babraham Institute

SYLLABUS

- 1. Brief history of Apple and the current marketplace**
- 2. Key differences between Windows and Mac forensics**
- 3. System basics: architecture, device management and permissions**
- 4. Techniques to examine Plists, Base64 & SQLite**
- 5. Apple volume management: Core Storage, APFS and encryption**
- 6. Live data collection - imaging, RAM, ioreg and volatile data**
- 7. Introduction to MAC memory analysis**
- 8. Imaging seized MAC's**
- 9. Decrypting FileVault 2 - with a password, without a Mac**
- 10. Partitioning Schemes: APM, MBR and GPT**
- 11. Apple File Systems: HFS+, HFSX and APFS**
- 12. HFS+ in detail from forensic perspective:**
 - a) File timestamps
 - b) Special files
 - c) Data and resource forks
 - d) Symbolic and Hard Links
 - e) File System Events
- 13. APFS core functionality and parsing**
- 14. iOS based devices: Challenges and limitations associated with data extraction and examination**
- 15. Examination of a MacOS system**
 - a) System information and configuration
 - b) User accounts
 - c) Log files
 - d) Network and device connections
 - e) User activity and thumbnails
 - f) Printing and Trash
 - g) Previous Versions
 - h) Spotlight
 - g) Applications including Messages, Facetime, Mail, iWorks, Photos
 - h) Safari
- 16. Time Machine: Functionality, data layout and recovery**

PA Consulting
Global Innovation & Technology Centre
Back Lane, Melbourn
Herts, SG8 6DP, United Kingdom
tel: +44(0) 1763 285285
email: cybereducation@paconsulting.com
[www: cybereducation.paconsulting.com](http://www.cybereducation.paconsulting.com)



To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com