COURSE OUTLINE

DIGITAL FORENSICS
Certified Forensic Investigation Specialist (CFIS)

●●●● **SPECIALIST-LEVEL COURSE** Cost: **£3,250.00** + VAT Duration: **5 days**

This specialist-level technical course is designed to practically develop a cyber investigator's skills and extend their knowledge to reveal potential 'smoking gun' evidence from a system.

"The course was brilliant. I really enjoyed it. It helped me to improve and develop my knowledge. I look forward to using the skills I have gained at work."
CFIS Delegate Computer Sciences Corporation

COURSE OVERVIEW

Investigators need to be capable of collecting and analysing data from a constantly evolving range of disk technologies, file and operating systems. The course is continually updated, based on our experiences, knowledge and client requirements to provide delegates with answers to the 'How can I collect that data or find evidence of that activity?'

This five-day course provides theory and scenario-based practical exercises and expanding data collection to include 'live' and volatile data.

Delegates will investigate artefacts buried in common file systems and 'recorded' by Windows of both system and user activity.

THE SKILLS YOU WILL LEARN

Using practical scenarios based primarily on Windows environments and artefacts, you will:

- Understand the digital investigation process and best practice
- Build a bootable USB data collection device
- Collect data from Live, Remote and Virtual systems
- Understand the underlying structures associated with NTFS, FAT32 and ExFAT file systems
- Collect and process volatile data
- Capture a mailbox from a live Microsoft exchange server
- Investigate a Windows domain controller to identify systems and users
- Understand RAID storage and rebuild data
- Test data 'wiping' software
- Understand types of 'User' account
- Investigate Windows Event Logs and USB device activity
- Examine user activity for program execution, file activity and system navigation
- Investigate log files
- Query Chrome web-browser SQLite databases and extract stored passwords
- Explore and extract data from Volume Shadow Copies
- Parse and interpret the USN/ Change Log

KEY BENEFITS

This course will enable you to:

- Develop your forensic investigation skills to an advanced level
- Practice new techniques suitable for evidence identification, capture and analysis in a 'live' environment
- Acquire an industry-recognised qualification to support your career progress

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 Forensic Investigation Specialist (CFIS)

●●●● SPECIALIST-LEVEL COURSE | Cost: £3,250.00 + VAT | Duration: **5 days**

WHO SHOULD ATTEND

Primarily aimed at practising digital forensic investigators and cyber security practitioners who have computer forensic experience and wish to dig deeper and broaden their skills. A natural progression from the PA CFIP course.

PREREQUISITES

- Principles and general guidelines surrounding forensic investigations
- Experience of carrying out forensic investigations
- A basic computer forensic course, e.g. PA's CFIP course

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Certified Forensic Investigation Specialist (CFIS) qualification.

SYLLABUS

1. **Digital Forensic Investigations**
   - A review of the investigation process, best practice and equipment
2. **Data Theft**
   - How can data be stolen, investigated and possibly mitigated?
3. **Data Acquisition**
   - Images and Clones; Static, Booted and Live; Physical and selective
   - Solid State devices
   - Considerations and associated problems
4. **Windows Domains**
   - Gathering information from Domain Controllers
   - Capturing File Shares and inaccessible systems
5. **RAID's and Virtualisation**
   - Identifying and rebuilding RAID's
   - Capturing and examining virtualised systems
6. **Volatile Data**
   - Memory capture and volatile data collection from 'live' systems
   - Investigating memory using volatility
7. **Data Collection – Other Sources**
   - Exchange servers and web-mail
   - Facebook, Websites, Linux and Macs
8. **File Systems Revisited**
   - Understanding FAT32, NTFS and ExFAT data structures from a forensic perspective
9. **Data Deletion and Wiping**
   - Windows Recycle Bins
   - Testing wiping software
10. **Tracing System Activity**
    - Investigating the Windows Registry, User Accounts, Event Logs and USB connected devices
11. **Tracing User Activity**
    - Identifying Program execution, Files opened and Folder navigation
    - Windows Object ID's and file tracking
12. **Log File Analysis**
    - Web and FTP logs
    - Examination using Cygwin
13. **Databases**
    - SQLite and Chrome browser artefacts
14. **Volume Shadow Copies and File History**
    - Approaches to extracting data from VSC's
    - Windows File History
15. **NTFS Journals**
    - Understand the value of the NTFS journal in investigations

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

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