COURSE OUTLINE

DIGITAL FORENSICS
Certified Forensic Investigation Practitioner (CFIP)

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

This core-level technical course is designed for people looking to develop their computer forensics investigation skills, either for a career in digital investigations or as part of their current cyber role.

"Excellent course with very knowledgeable tutor, highly recommended."
CFIP Delegate
Staffordshire University

COURSE OVERVIEW

Gain an understanding of digital forensics analysis by learning about forensic principles, evidence continuity and methodology to employ when conducting a digital forensic investigation.

This five-day course will provide you with a practical base understanding of the legalities, best practice and methodologies used in the current digital forensic investigation environment. The course content covers seizure, evidence handling and data preservation, through to investigation and interpretation, and finally the reporting and presentation of findings.

THE SKILLS YOU WILL LEARN

Using practical scenarios based on Windows 7 artefacts with the latest disk technologies, you will learn the following:

- The principles and guidelines for static digital forensic investigations
- The process of evidence continuity
- The fundamentals of the complete forensic investigation process
- The forensic acquisition of an electronic device
- How data is stored on electronic media
- How to work with key forensic investigation products
- How to identify Windows based OS forensic artefacts

The course will also provide answers to many questions including:

- What skills and qualifications do I need to practice digital forensics?
- How and where is data actually stored on a device?
- What is the difference between forensic imaging and cloning?
- Is keyword searching an effective way to identify data on a device?
- What is hashing and how can it be used in digital forensics?
- What happens when a user deletes a file or empties a recycle bin?
- How does 'Private' web-browsing work?
- Can data be recovered after 7 pass overwrite?
- Is there a backdoor to passwords and encryption?
- Who was using a computer on a particular occasion?
- How can I identify if and when a user edited or accessed a file?

KEY BENEFITS

The course will give you:

- An understanding of each stage of a forensic investigation, from evidence seizure through to data investigation and interpretation, to report and presentation of findings
- The skills to allow you to undertake the forensic acquisition of an electronic device
- Confidence in working with key forensic investigation products
- An industry-recognised qualification in forensic investigation and ideal preparation for the PA CFIS advanced course

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 Practitioner (CFIP)

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

WHO SHOULD ATTEND

Those responsible or eager to become responsible for computer forensic investigations, including:

- Cyber Forensic & Network Investigators
- IT Security Officers
- Law Enforcement Officials

PREREQUISITES

Experience with Microsoft Windows OS and, ideally, a general appreciation of forensic principles, practices and software.

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 Practitioner (CFIP) qualification.

SYLLABUS

1. **Introduction to Digital Forensics**
2. **Investigation Guidelines and Process**
3. **Identification & Seizure**
   a. Forensic Acquisition
4. **Understanding Electronic Data**
   a. Understand how data is stored on electronic devices
   b. Analyse the functionality of a computer file system
5. **Physical and Logical Disks**
6. **File Systems and Data Storage**
7. **Dates, Times and Metadata**
8. **Forensic Analysis Techniques**
9. **Windows Artefacts**
   a. Function, structure and operation of the Windows registry
   b. Internet history
   c. Recycle bins
10. **Forensic Challenges**
11. **Reporting**
    a. Collating results
    b. Contents and layout of forensic reports
12. **Electronic data**
    a. Hardware and Software
    b. Addressing hardware employed during a forensic investigation
    c. Familiarisation with forensic software
13. **Investigating Windows artefacts**
14. **Reporting**

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