COURSE OUTLINE

# DIGITAL FORENSICS
# Certified Cyber Investigator (CCI)

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

This specialist-level course is for professionals whose role requires them to capture and analyse data from 'live' systems. It introduces the latest guidelines and artefacts on current Windows operating systems, and teaches essential skills for conducting an efficient and comprehensive investigation.

*"This was the most useful networking investigation course I have been on in recent years. I came away with a substantial increase in my knowledge along with some very useful documentation. If you're going to do one networking investigation course year, make it this one."*

***CCI Delegate***
***Regional Cyber Crime Unit***

## COURSE OVERVIEW

This five-day course is designed to provide you with the confidence and skills to isolate, investigate and extract evidence from a live networked environment (as you would expect to find in a home or business network) during or after a cyber incident.

You will spend a large proportion of the course practising these skills and methods in both physical and virtual network environments that replicate the challenges faced by investigators today.

## THE SKILLS YOU WILL LEARN

You will learn and practice the critical skills needed to identify the correct forensic artefacts in a live network environment and how to preserve, extract and interpret them. We will show you how to correctly acquire data from a live network so that you do not inadvertently alter or destroy vital clues that could potentially result in your investigation failing or the resultant evidence being inadmissible in court.

Upon completion of the course you will:

- understand home and office network environments
- be able to secure and access a live network
- be able to reduce your digital footprint when accessing a network
- be able to identify a cyber event
- have the ability to identify devices attached to a network
- understand how to identify and collect volatile data
- have the knowledge of how to examine and analyse relevant data artefacts
- be able to identify and capture relevant log files
- be able to identify and collect suspect network traffic (Ethernet and Wi-Fi)
  have learnt remote network collection methodologies and techniques

## KEY BENEFITS

This course will enable you to:

- Learn a number of methodologies for undertaking a sound cyber investigation
- Acquire and practice new techniques to extract relevant data from a live networked environment
- Gain confidence when identifying and capturing live operating system artefacts
- Improve your ability to respond effectively to a cyber event

## WHO SHOULD ATTEND

This is an intensive training course designed for experienced forensic investigators and cyber security practitioners who already have a good knowledge of forensic investigation and want to extend their skills, including:

- Law enforcement officers & agents
- Digital investigators
- Cyber incident response team members
- IT security officers
- System/Network Administrators/ Engineers

**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 Cyber Investigator (CCI)

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

## PREREQUISITES

You will need a good understanding and experience of:

- Computer networks
- The forensic investigation process
- Windows and Linux operating systems
- Command line interface and using console tools

We strongly recommend completion of the PA Consulting CFIP and CLFP courses as a minimum before attending this course.

## WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA Consulting's Certified Cyber Investigator (CCI) qualification.

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

## SYLLABUS

Throughout the course, your time will be equally split between being taught the methods and principles required to isolate, investigate and extract evidence in a live network environment and applying these in practical, hands-on exercises based on real life scenarios, created in a set of physical and virtual networks.

1. **Investigation Principles and Strategy**
   a. ACPO Guideline - The Four Principles
   b. Competency
   c. Applicable Standards
   d. Applicable Law

2. **Computer Networks**
   a. What is a computer network?
   b. Types of computer network
   c. Network topologies

3. **Network Reference Models**
   a. OSI Model
   b. TCP/IP Model

4. **Network Addressing**
   a. MAC Address
   b. IPv4
   c. Subnets
   d. IPv6

5. **Network Protocols**
   a. What are protocols?
   b. Ports
   c. Transport layer protocols
   d. Other protocols of interest

6. **Network Environments**
   a. Typical home network
   b. Typical business network
   c. Public network

7. **Network Devices**
   a. Computer (Desktop/ Server)
   b. Hub
   c. Switch
   d. Router
   e. Other devices

8. **Information Gathering**
   a. Analysis Environments
   b. Identifying equipment
   c. Accessing a network
   d. Network mapping
   e. Network traffic
   f. Accessing network devices (Computer, Switch, Router, other devices)
   g. Reducing your digital footprint
   h. Understanding console tools including WMI, CIM and PowerShell
   i. Remote imaging and data collection
   j. Scripting (batch and PowerShell)

9. **A Cyber Analysis Process**
   a. Correlating Results
   b. Data Interpretation

10. **Simplifying Complex Evidence**
    a. Subject knowledge levels
    b. Clarity, simplicity, brevity
    c. Reporting

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