COURSE OUTLINE

DIGITAL FORENSICS
Certified Malware Investigator (CMI)

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

This is a core-level technical course for people looking to extend their knowledge and understanding beyond traditional file system forensic analysis.

COURSE OVERVIEW

On this five-day practical course you will investigate forensic case studies, applying the principles, knowledge and techniques learnt during the course. It will help you protect your IT environment by showing you how to conduct malware (malicious software) investigation and analysis, from first principles all the way to collecting computer and network activity stemming from malicious infection that your AV software has failed to detect. The course concludes with a final practical exercise which consolidates all the investigation methods and techniques learnt during the course.

THE SKILLS YOU WILL LEARN

- You will learn how to identify, analyse and interpret malware types including identification of associated forensic artefacts as a result of being infected by complex malware such as a Trojan horse.
- How malware can hide, execute and bypass AV and other security software such as firewalls
- You will practice malware investigations from mounted, booted and network perspectives, and undertake real-world exercises, including the conversion of E01 forensic images into bootable virtual machines
- Understand the function and operation of the Windows registry and other Windows Operating System artefacts
- Understand the structure of the NT file system and how to identify anomalous activity

Practical application of course content will be through the use of case scenarios in order to gain a practical understanding of modern malware beyond the often quoted traditional principles; mount forensic images for analysis; build virtual machines for analysis and build a network environment to carry out network forensic analysis.

KEY BENEFITS

The course will give you:

- The skills to understand, analyse and interpret malware and investigate computer and network activity associated with a malware infection
- An understanding of how to simplify complex evidence, collate and report results
- An industry-recognised qualification in malware investigation

WHO SHOULD ATTEND

For those looking to develop their skills in malware identification and analysis, including:

- Digital forensic analysts
- Cyber incident responders
- Security operations specialists
- System/Network Adminsitrators/ Engineers
- IT Security Officers

PREREQUISITES

You will need an understanding and experience of:

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

We strongly recommend completion of the PA Certified Forensic Investigation Practitioner (CFIP) course as a minimum before attending.

"Instructor was interesting and engaging. Obviously knew the subject well. I thoroughly enjoyed the course."
CMI Delegate
Assured Security Control Ltd

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com

COURSE OUTLINE

DIGITAL FORENSICS
Certified Malware Investigator (CMI)

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

WHAT QUALIFICATION WILL I RECEIVE?

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

SYLLABUS

1. Relevant Legislation & Compliance
   a. Applicable legislation
   b. Relevant guidelines and standards
2. Malicious Software (Malware)
   a. Defining malware
   b. Categories of malware
   c. Identify similarities and differences between different malware types
   d. Infection methods
3. Malware Investigations
   a. Methodologies
   b. Analysis environments
   c. Tool selection
   d. Training and experience
4. Practical Malware Investigations
   a. Port scanning
   b. Running processes
   c. Malware scanning
   d. Start-up methods
   e. Memory analysis
   f. Advanced methods
5. Methods of Deception
   a. Malware delivery
   b. Mechanisms of disguise
   c. Security circumvention
6. Mounted Analysis
   a. Mounting forensic images as logical drives
   b. Using malware scanners against the mounted image
   c. Documenting the results of malware scans
   d. Using online scanners for further clarification
7. Booted Analysis
   a. Identify approaches to creating a booted analysis environment
   b. Creating virtual machines
   c. Identifying password implications
   d. Identifying and explaining the potential differences between mounted and booted analysis results
8. Network Analysis
   a. Identify key reasons for network analysis
   b. Methods of building a network for analysis
   c. Explaining networkcommunication protocols
   d. Using traffic analysis tools for network analysis
   e. Identifying and explaining the differences between network and other analysis results
9. Simplifying Complex Evidence
   a. Subject knowledge levels
   b. Clarity, simplicity, brevity
   c. 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