COURSE OUTLINE

DIGITAL FORENSICS
Certified Malware Investigation Professional (CMIP)

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

This is a specialist-level technical course for people looking to extend their knowledge beyond the basics of malware investigations. This course builds on the core foundations of our Certified Malware Investigator (CMI) course and will give delegates a deeper technical understanding of how to investigate a suspected malware infection.

COURSE OVERVIEW

On this five-day in-depth technical course you will investigate a complex malware infection, applying the knowledge, methods and techniques learnt during the course. This will enable you to conduct and identify a malware infection that traditional antivirus and security solutions may not have detected. The course concludes with a final practical exercise to consolidate the course learning points.

THE SKILLS YOU WILL LEARN

- You will learn how to identify artefacts consistent with complex malware
- Understand how malware can obfuscate itself and hide in plain sight
- Practice malware investigations in a live environment
- Investigate Random Access Memory
- Understand structures of key NT file system metadata files

Practical application of course content will be through case scenarios in order to understand how complex malware functions within a Windows environment.

KEY BENEFITS

The course will give you:

- The skills to understand and interpret malware within a Windows environment
- Practical experience of investigating Random Access Memory
- Practical experience of analysing the structures of the NT file system
- An industry-recognised qualification in malware investigation

WHO SHOULD ATTEND

For those looking to further develop their skills in malware investigations, including:

- Digital forensic practitioners
- Cyber security responders
- Security operations specialists

PREREQUISITES

You will need an understanding and experience of:

- Investigating malware infections
- Windows 10 Operating Systems
- The NT File System
- Memory Analysis
- PowerShell and other command line tools

We strongly recommend completion of the PA Certified Forensic Investigation Specialist (CFIS) and Certified Malware Investigator (CMI) courses as a minimum before attending.

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 Malware Investigation Professional (CMIP)

●●●● **SPECIALIST-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 Investigation Professional (CMIP) qualification.

SYLLABUS

1. Malware Types & Terminology
   a. Defining malware
   b. Categories and capability of malware
   c. Malware persistence and states

2. Detecting Malware
   a. Infection methods
   b. Detection methods
   c. Indicators of compromise
   d. MITRE ATT&CK
   e. Obfuscation techniques

3. Malware Persistence
   a. Start-up methods

4. Malware Infection
   a. Random Access Memory (RAM)
   b. Virtual memory files
   c. File access
   d. PowerShell

5. Practical Investigations
   a. Analysis environments
   b. Investigation methodology
   c. Tool selection

6. Windows Essentials
   a. Dates and times
   b. Prefetch & SuperFetch files
   c. Registry
   d. Event logs

7. Memory Analysis
   a. Build-in tools 'Living off the land'
   b. Third-party tools

8. NT File System (NTFS)
   a. Understanding NTFS
   b. $MFT structures
   c. $Logfiles structures
   d. $UsnJrnl:$J structures

9. Consolidation Exercise
   a. Final exercise to consolidate course content

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