



# CMI Malware Investigation: Hands-On

7safe training 

Course Outline



## ❖ CMI Malware Investigation: Hands-On



The CMI training course and associated CMI exam provide delegates the opportunity to extend their knowledge beyond conventional static analysis.

Using practical case scenarios, delegates are guided through the process of conducting malware analysis from the principles surrounding the different analysis environments and 7Safe's malware investigation methodology to investigating network activity stemming from malicious software infection.

### ❖ What you will learn

- How to analyse and interpret malicious software and associated forensic artefacts including Trojan horses, viruses and worms
- Malware fundamentals in contrast to traditional definitions of malicious software
- How to approach malware investigation from mounted, booted and network perspectives
- Practical exercises include conversion of EOI-style images to bootable virtual machine disks, contrasting Malware scans in Linux and Windows-based analysis and behavioral observation of Malware in lab environments

### ❖ Benefits

- Practice and understand the subject matter under the guidance of 7Safe's expert tutors
- Develop your investigation skills in malware analysis in a state-of-the-art class environment
- Receive up-to-date course materials
- Includes the Certified Malware Investigator (CMI) examination

### ❖ Who should attend

Those with an interest in or responsibility for forensic malware investigation, including:

- Forensic & Network Investigators
- Information Security Professionals
- IT Security Officers
- Law Enforcement Officials
- Computer Auditors
- Crime Prevention Officers

### ❖ Course style

This is a practical course where delegates will investigate forensic case studies, applying the principles, knowledge and techniques learnt during the course.

An optional examination is held on the final day. Successfully completing this examination earns delegates the Certified Malware Investigator (CMI) certification. Delegates can further their studies by successfully completing university assignments which will earn them the Masters-level CMI<sup>+</sup> qualification.

## ❖ Level & Prerequisites

- CFIP recommended but not essential
- Principles & general guidelines surrounding forensic investigation
- Preliminary case considerations to evaluate when beginning a forensic investigation
- Sound experience with Microsoft Windows required
- Basic understanding of TCP/IP networking concepts is advantageous

## ❖ Course content highlights

### MALICIOUS SOFTWARE

- How malicious software impacts computer users
- The operation of viruses, worms, Trojan horses, backdoors and rootkits
- How to examine for signs of infection
- How Trojan payloads can be used to bypass anti-virus software, personal and corporate firewalls

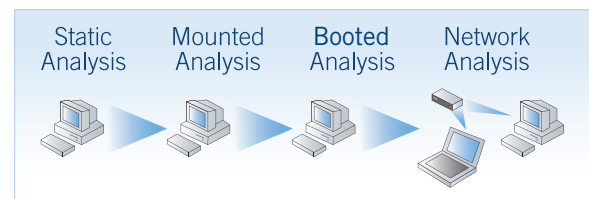
### THE WINDOWS REGISTRY

- Function, structure and operation of the Windows registry
- Investigation of malicious software locations in the registry and file system

## CASE SCENARIOS

*Practical application of course content using case scenarios. Delegates will:*

- gain a practical understanding of modern malware beyond the often quoted traditional principles
- mount forensic images for analysis
- build virtual machines for analysis
- build a network environment to carry out network forensic analysis



## SIMPLIFYING COMPLEX EVIDENCE

- Collating and reporting results
- Presenting complex oral evidence

## ❖ Duration

3 days

## ❖ Cost

£1498.50 + VAT

## ❖ CPE Credits

21

