



# ISEC Programme 2008 Cybercrime Training



## Malware Analysis and Investigations

### Course Aim

The course is designed to provide law enforcement forensic practitioners and internet investigators with the basic tools and techniques to perform analysis on the different pieces of malware encountered in Cybercrime investigations. The course will enhance the investigator's ability to deal with for example banking trojans or botnet's.

**This course will contain both theory and practical exercises.**

**Note: Students attending this course will undertake an assessment process. Certificates will be supplied to students who successfully complete the course.**

### Prerequisites

Students will be expected to have a fundamental understanding of computing and IT forensics and investigations with at least 2 years practical experience in the subject. It is essential that students have a good working knowledge of the English language, as the course lessons will be in English

### Trainers

The trainers for this course will be a combination of malware experts from industry and high tech crime specialists from law enforcement and academic organisations.

### Objectives

After attending this course the participant will be able to:

- Explain the concept of malware analysis
- List the different Malware types and functionalities (including e.g. banking viruses and botnets)
- Differentiate between types of infection and propagation techniques; malware distribution infrastructure
- Demonstrate a basic knowledge of static and dynamic analysis
- List the practical uses of analysis and reverse engineering tools
- Explain how to identify malware from a investigative perspective
- Extract evidence about the developer, owner and user of Malware leading to identifying the criminal
- Conduct analysis of a sample in an experimental/secure environment; e.g. how to build a botnet?

### Who should attend

This course is designed for police staff that are experienced Cybercrime Investigators and who will have attended one or more of the Agis cybercrime training courses or be able to demonstrate equivalent knowledge. This course is not for inexperienced staff.

### Course Dates

This is a five-day residential course on dates to be arranged

### Location

This course may be hosted by any law enforcement agency.

### Cost

The hosting organisation is responsible arranging the event and for the costs associated with it. The training material may be obtained by contacting [htcc@europol.eu](mailto:htcc@europol.eu)

It is normal for the costs to be recovered from students, their organisations or through sponsorship arrangements. The spirit of sharing of this material among law enforcement agencies is that it is delivered on a not for profit and non commercial basis.

This course may be translated into other languages as the behest of any law enforcement agency. If the material is translated, it is requested that the resulting material is made available to the wider law enforcement community by contacting [htcc@europol.eu](mailto:htcc@europol.eu) to arrange delivery.



ISEC 2008