



ISEC Programme 2008 Cybercrime Training



Live Data Forensics

Course Aim

The course is designed to give law enforcement forensic practitioners who take part in searches the appropriate basic knowledge and tools to deal with computer systems that are on when arriving on the premises, in order to collect evidence that would disappear once the machines are turned off, including from the memory and encryption information.

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 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 high tech crime forensic training specialists from Law Enforcement agencies and academic organisations.

Objectives

After attending this course the participant will be able to:

- Explain the concepts of live data forensics
- Explain the differences between live and static forensics
- Explain the reasons for acquiring memory and explain its volatility
- Identify encryption tools used by computer users
- Conduct the essential steps to collect volatile evidence
- Identify and prioritise sources of volatile evidence to collect
- Establish access to live systems when possible
- Dump RAM
- Gather evidence from the various sources
- Analyse memory dumps at a basic level
- Document all actions taken in acquiring and analysing live data
- Report on their actions and findings.

NB – This course will primarily concentrate on the VISTA and XP operating systems with some discussion about Linux and MAC where time permits

Who should attend

This course is designed for police staff that are experienced IT forensic practitioners 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

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 to arrange delivery.



ISEC 2008