

Computer forensics – Intermediate

Introduction

This course addresses the theoretical and practical application of computer forensics for the first responder and the computer forensic engineer within the corporate and legal environment. This course is compulsory for those who wish to proceed to our professional level course - Computer forensics-Advanced.



Aim

The aim of this module is to provide delegates with a sound knowledge and understanding to enable them to recover admissible evidence from PC based computers and the skills and competencies to prepare such evidence for presentation in a Court of Law.

Syllabus

The course will detail the fundamentals of forensic computing to a degree that will enable delegates understand precisely how commercial forensic tools operate and that will allow them to operate beneath the level of the tool and extract digital evidence directly from binary images.

Introduction

- Brief history
- Why computer forensics – before, now (emergent crimes and corporate demands)
- Is computer forensics a science – fry and daubert test
- Global organisations overseeing
- Associations
- Qualifications

Physical components of the PC and how they fit together and interact.

- Basic electrical safety. Motherboards and the design of the PC. Practical exercises in dismantling and building PCs.

How Computers work

- An explanation of the Power On Self Test (POST)
- Boot sequence.
- CMOS
- MBR
- Operating system
- Applications

Volatile and non volatile data

- Relevance for Computer forensics
- Where is volatile data located?
- Where is non volatile data located?

Disk Geometry

- Types of disk storage and their characteristics
- Hard disk internals
- Disk management processes – fdisk, format
- Data storage mechanism – how data is stored and sorted
- Master boot record

Data storage

- Sector
- Partition
- Volume
- Ambient data – slack space, host protected areas

Operating systems and file systems

- FAT 12
- FAT 16
- FAT 32
- NTFS
- Linux ext2 and ext3.
- File Meta data - MAC attributes

Passwords and encryption

- Explanation of passwords keys and hashes.
- Dealing with password protected and encrypted files.

Steganography

- Data hiding-Forms of data hiding – System Area, slack space, disk size,
- Changing file extension, background page and font colour,
- Concatenation
- Anti forensics

Computer evidence investigation

- Preparations to be made before seizure.
- Actions at the scene. Treatment of exhibits
- Laboratory ethics – chain of custody
- Evidence e storage

Forensic examination tools and practical exercises

- Win hex,
- FTK - Access Data,
- Encase,
- Net analysis

- A series of practical lab exercises designed to demonstrate how to access forensic artefacts within hard disk drives and to develop the student's skills in forensic analysis. Importance of keeping a log. Methods of hiding data on hard and floppy disks, practical recovery of such data using methods to preserve its integrity. Methods of recovering deleted files. Copying and imaging

Introduction to Computer Networks

- OSI reference Model
- Overview of computer networks
- The Internet – topology
- Network devices

Legal issues and consideration

- Seizure of computers. – search warrants, scope and authority of investigator
- Civil investigation of computer evidence –special considerations
- Admissibility of computer evidence
- Initial obstacles
- Relevant Case Law
- Relevant procedural regulations

Report Preparation and giving of evidence.

- Witness statements
- briefing case officers and Counsel
- testifying as a witness

Intended Learning Outcomes

On successful completion of this module a delegate will be able to:

Knowledge

- Recognise the component parts of a computer, understand how these parts physically and electronically interact, and apply sound electrical safety procedures in a forensic examination environment.
- Understand the start-up procedures of operating systems, particularly in DOS and Windows environments, how they interact with the hard disk and the significance of the paging of memory to disk in a forensic environment.
- Recognise the need for digital evidence integrity as it applies to its admissibility in court
- Understand what is required during testimony in court

Skills

- Apply a detailed knowledge of disk geometry to the examination of data storage systems and understand the advantages and disadvantages of imaging and copying for evidential purposes.
- Use data recovery software tools, understand the overall principle of original integrity, and be competently practised in the methods and principles of disk examination and logging, and the preparation of evidence for Court.
- Demonstrate a sound understanding of the law relating to evidence recovered from computers and law relating to the search for and investigation of computer evidence.