

Computer evidence – Introduction

Aim

The aim of this course is to provide delegates with an understanding of the role of computer evidence in criminal, civil and arbitration matters. It covers the broad spectrum of digital evidence identification, analysis and presentation in a corporate environment a court of law.



Audience

This course is aimed at first responders, prosecutors, paralegals, lawyers, judicial personnel, systems administrators, Legal professionals, accounting fraud investigators.

Syllabus:

History of computer evidence

- UK
- USA
- Global concerns
- Europe
- UN
- G-8

Unique attributes of computer evidence

- Evidence is in binary format
- Deleted files can be recovered
- Easily tainted and manipulated

Relevance of Computer evidence

- Criminal cases
- Civil cases
- Arbitration

Legal issues

- Admissibility of computer evidence
- Proof of evidence
- Civil procedure directions
- UK - Status
- USA - Status

How computers work - overview

- Parts of a computer
- How computers work - The boot process
- Unique characteristics of computer evidence
- Storage devices - Types
- Network computers
- The internet

Introduction to computer forensics

- What is computer forensics?
- Scope of computer forensics
- The investigative process

Introduction to electronic document discovery

- What is electronic document discovery?
- Scope of electronic document discovery
- The discovery process
- Searching techniques
- Digital document management

Where is computer evidence located?

- Storage devices
- Windows artifacts
- The registry
- logs
- Folders
- System components

What are you looking for?

- Characteristics of digital documents
- Document extensions
- Example of binary notations
- Relevance of Time lines
- Anti forensics
- Practical demonstration

The Court Room Environment

- Evidence presentation and report writing
- Demonstrative evidence
- Key players in the courtroom
- Role, obligations and expectations of the expert witness.

Intended Learning Outcomes

- On successful completion of this course the delegate will be able to:

Knowledge

- Understand the scope and relevance of computer and digital evidence in criminal and civil cases.
- Understand the steps involved in the collection and analysis of computer evidence.
- Understand steps involved in the management of digital evidence
- Understand the evidential rules within which digital evidence is collected
- Recognise and respond to the difficulties inherent in presenting computer evidence.
- Develop effective risk management protocols for storing and maintaining the integrity of computer evidence.

Skills

- Implement protocols to ensure data integrity and admissibility
- Implement measures to reduce the risk of evidence contamination
- Investigate and implement gap analysis in a corporate environment
- Assist investigating officers, legal officers, legal counsel