

Digital evidence for the Judiciary

Aim

The aim of this course is to provide Judges, Court officials and lawyers with the necessary tools to understand and resolve issues concerning digital evidence in criminal, civil and arbitration matters. More importantly, to enable delegates acquire the relevant skills to deal with issues concerning the admissibility or otherwise of digital evidence. It covers the broad spectrum of digital evidence identification, analysis and presentation before a court of law or tribunal.



Audience

This course is aimed at Judges, Judicial officers and Arbitrators and lawyers.

Introduction

- The paradigm shift
- The influencing role of computer technology
- The need for a new learning and a new approach
- What is digital evidence – computer, mobile phone and digital document discovery
- Examples of digital devices
- Scope of digital evidence
- Junk science argument
- Lessons for the Judge and the court

Global Concerns

- EU
- UN
- US
- UK
- Canada
- Conflict of laws
- Cross boarder issues – evidence across international borders
- Lack of local legislations
- Lessons for the Judge and the court

Digital devices

- Types of digital devices
- Essential parts of a computer
- Brief introduction - How computers work
- Where is the evidence stored
- Real and deleted data
- How reliable is digital evidence?
- How to determine the Authenticity or otherwise of digital evidence
- Lessons for the Judge and the court

Relevance of digital evidence in Civil and Criminal matters

- Criminal Jurisprudence
- The mens rea
- The actus reus
- Strict liability
- Comparative analysis of criminal legislations
- Digital evidence in civil jurisprudence
- Lessons for the Judge and the court

Computer forensic evidence

- Brief introduction
- Scope of the discovery
- What needs to be discovered
- Evidence integrity
- Issues of admissibility
- Lessons for the Judge and the court

Mobile Phone evidence

- Brief introduction
- Scope of discovery
- What needs to be discovered
- Issues of admissibility
- Lessons for the Judge and the court

Digital document discovery

- What is digital document discovery?
- When is it relevant?
- Issues associated with digital document discovery
- Lessons for the Judge and the court

Admissibility of digital evidence

- The discovery and recovery of digital evidence
- The legal expectations in the discovery and recovery process
- Lessons for the Judge and the court

Anti Forensics

- Data hiding
- Encryption
- Steganography
- Cryptography
- Black Hat
- Lessons for the Judge and the court

The role of the forensic expert witness

- An analysis of the forensic experts methodologies
- Managing the expert evidence process

The Judges Domain

- Before the trial
- Relevant court orders
- Managing the scope of evidence
- Managing litigant antics
- Managing issues of cross boarder evidence
- Court sanctions

Practical

Case scenario with relevant elements examined and analysed by delegates.

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 evidential contamination
- Investigate and implement gap analysis in a corporate environment
- Assist investigating officers, legal officers, legal counsel