

# DIGITAL EVIDENCE AND FORENSIC ANALYSIS MASTERCLASS

You Can Destroy The Evidence, But You Can't Destroy The Memories

5th & 6th October 2017  
Kuala Lumpur, Malaysia

DELEGATES ARE  
REQUIRED TO BRING  
THEIR LAPTOP FOR  
DISCUSSION, EXERCISE  
AND PRESENTATION  
PURPOSES

## Major Benefits Of Attending

By end of this course, delegates will be able to:

- **UNDERSTAND** the expanding field of computer crime investigations and computer forensics
- **INVESTIGATE** computer crimes
- **CONDUCT** computer forensic examinations
- **ACQUIRE** the required skill set to perform forensically sound computer examination
- **DOCUMENT** the findings in a clear concise report
- **KNOW** the methodology for conducting a computer forensic examination
- **SEIZE** and **SECURE** digital evidences
- **VALIDATE** digital evidence for legal argument
- **HANDLE** evidence from online sources
- **ANALYSE** the evidence and its characteristics
- **LABEL** and **TAG** digital evidence
- **ANALYSE** computer and operating systems forensics
- **ANALYSE** web, email and messaging forensics

Carrier and Spafford (2006) defined digital evidence as a digital data that supports or refutes a hypothesis about digital events or the state of digital data. This definition includes evidences that may not be capable of being entered into a court of law, but may have investigate value, this definition is in agreement to Nikkel (2006) definition that states, digital evidence as a data that support theory about digital events.

## Why you Should Attend?

Computers and the internet have drastically improved business, communication, media production, and numerous other sectors in today's society. A majority of organization relies deeply on digital devices and the internet to operate and improve their business, and these businesses depend on the digital devices to process, store and recover data. A large amount of information is produced, accumulated, and distributed via electronic means. Inevitably, such powerful tools are also exploited to commit electronic crimes. Recent research conducted by scientists concluded that up to 90% of all information never leaves the digital domain. This means that the majority of information is being created, modified, and consumed entirely in digital form. Most spreadsheets and databases never make it on paper, and most digital snapshots are never printed. There are many activities such as chats and social networking that are specific to digital and are even unimaginable outside of the virtual realm.

Most such activities leave definite traces, allowing investigators to obtain essential evidence, solve criminal cases, and prevent crimes. This course will guide you through in-depth details on digital evidence for forensic analysis covering areas like handling issues of digital evidence, reviewing regulatory and legal considerations, computer forensic incidents and investigation process, factors affecting evidence acquisition, seizing and securing digital evidence, validating digital evidence for legal argument, mobile and electronic devices for fraud examination, and handling the evidence from online courses. This course will also cover areas involving usage of digital forensic tools for e-discovery, dealing with evidentiary issues and challenges, network and system forensics, conducting computer forensic examination, analysing windows system, USB and cloud computing issues, and explain thoroughly on the forensic software and reporting.

## Who Should Attend?

This course has been specifically designed for corporate and government personnel who, in the performance of their duties, would need to conduct digital forensic examination. This includes personnel who encounter digital evidence while conducting an investigation including from departments of:

- ✓ Information Security
  - ✓ Risk Management
  - ✓ Loss Prevention
  - ✓ Corporate Security
  - ✓ Law Enforcement
- Some of the target audiences would include:
- ✓ Government and Law Enforcement Investigators
  - ✓ Police and other Law Enforcement Personnel
  - ✓ Cyber Crime Investigators
  - ✓ Digital Forensic Investigators
  - ✓ E-Business Security Professionals
  - ✓ Systems Administrators
  - ✓ Legal Professionals
  - ✓ IT Managers

Organized by: \_\_\_\_\_



WE SOLVE YOUR PUZZLE