MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

IMPLEMENTATION & MANAGEMENT OF COMPUTER FORENSICS PROCESSES (DIGITAL FORENSICS EXAMINAR (CLFE)

"Mastering Digital Evidence Collection, Analysis, and Reporting to Support Legal and Investigative Objectives"

Schedule

Date	Venue	Fees (Face-to-Face)
03 – 07 May 2026	Riyadh, KSA	USD 3495 per delegate

► **Available delivery methods:** Face-to-Face & Online Training

Introduction

As cybercrime becomes increasingly sophisticated, organizations need professionals skilled in computer forensics to identify, collect, preserve, and analyze digital evidence effectively. Digital Forensics is not only vital in criminal investigations but also in corporate risk mitigation, incident response, and compliance efforts.

This course prepares participants for the Certified Lead Forensics Examiner (CLFE) designation, providing practical knowledge on implementing and managing forensic investigations across systems, devices, and networks. Participants will learn to use forensics tools, maintain chain of custody, interpret findings, and prepare defensible reports for regulatory, civil, or legal proceedings.

Objectives

By the end of this course, participants will be able to:

- Understand the fundamentals of digital forensics, cyber laws, and evidence handling
- Plan and manage computer forensic investigations from start to finish
- Apply forensics techniques on various platforms including hard drives, mobile devices, and networks
- Use forensic tools for acquisition, imaging, recovery, and analysis
- Maintain proper documentation and chain of custody for legal admissibility
- Develop professional reports and present findings in legal or disciplinary settings

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

- Gain a globally recognized certification in computer forensics
- Learn how to detect, investigate, and respond to digital incidents
- Understand the legal and procedural requirements of cyber evidence handling
- Apply real tools and processes to collect, preserve, and analyze digital evidence
- Prepare for forensic roles in law enforcement, cybersecurity, or internal audit

Target Audience

This program is designed for:

- IT Security Professionals and Cybercrime Investigators
- Forensic Analysts and Incident Responders
- Auditors and Compliance Officers
- Legal Counsel involved in technology or data breach cases
- Anyone pursuing CLFE certification or forensic readiness capabilities

Individual Benefits

Key competencies that will be developed include:

- Digital forensics investigation lifecycle
- Forensic imaging, evidence validation, and malware tracing
- Knowledge of file systems, metadata, and operating system artifacts
- Report writing and expert witness communication
- Compliance with international standards and legal frameworks

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved response to security breaches and insider threats
- Accurate evidence gathering to support HR, legal, or regulatory cases
- Compliance with laws on digital evidence and privacy
- Reduced cost and time in conducting digital investigations
- Stronger cyber risk management and internal policy enforcement

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – Digital crime types, investigation frameworks
- Case Studies – Insider fraud, ransomware investigations, data leaks
- Workshops – Disk imaging, log analysis, mobile device forensics
- Peer Exchange – Sharing case handling strategies and challenges
- Tools – FTK Imager, Autopsy, EnCase, Sleuth Kit, and open-source tools

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Course Outline

Training Hours: 7:30 AM – 3:30 PM Daily Format: 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Introduction to Digital Forensics and Legal Frameworks

- Module 1: Fundamentals of Digital Forensics (07:30 – 09:30) • Forensics lifecycle, types of digital evidence
- Module 2: Laws, Standards, and Ethical Guidelines (09:45 – 11:15) • Cybercrime laws, ISO 27037, admissibility of evidence
- Module 3: Incident Response and Forensics Planning (11:30 – 01:00) • Linking IR with forensics investigations
- Module 4: Workshop – Digital Evidence Identification Exercise (02:00 – 03:30) • Identify evidence sources across IT systems

Day 2: Evidence Acquisition and Preservation

- Module 5: Imaging and Data Acquisition Techniques (07:30 – 09:30) • Logical vs physical imaging, write blockers, hashing
- Module 6: Chain of Custody and Documentation (09:45 – 11:15) • Evidence labels, transport logs, audit trails
- Module 7: File Systems and Data Recovery Basics (11:30 – 01:00) • FAT, NTFS, EXT, deleted file recovery
- Module 8: Workshop – Create a Forensic Image and Validate Integrity (02:00 – 03:30) • Use FTK Imager to clone and hash drives

Day 3: Forensic Analysis Techniques

- Module 9: Artifact Analysis and Metadata Examination (07:30 – 09:30) • User activity, registry, browser history, timestamps
- Module 10: Email and Log File Analysis (09:45 – 11:15) • Header tracing, mail server logs, event correlation
- Module 11: Memory and Malware Forensics (11:30 – 01:00) • Volatile data, malware behaviors, sandboxing
- Module 12: Workshop – Investigate a Suspicious USB Incident (02:00 – 03:30) • Analyze logs and trace user activity

Day 4: Mobile, Network, and Cloud Forensics

- Module 13: Mobile Device Forensics (07:30 – 09:30) • Tools and techniques for Android/iOS devices
- Module 14: Network and Cloud-Based Evidence (09:45 – 11:15) • Packet capture, SaaS logs, data localization
- Module 15: Data Correlation and Timeline Reconstruction (11:30 – 01:00) • Event mapping, cross-device correlation
- Module 16: Workshop – Create a Forensic Timeline (02:00 – 03:30) • Combine device and log data into one incident timeline

Day 5: Reporting and Expert Testimony

- Module 17: Report Writing and Forensic Documentation (07:30 – 09:30) • Executive summaries, evidence logs, screenshots
- Module 18: Presenting Evidence and Testimony (09:45 – 11:15) • Courtroom conduct, expert witness tips
- Module 19: Final Case Study – Forensic Investigation Simulation (11:30 – 01:00) • Analyze a complete case from evidence to conclusion
- Module 20: Final Workshop – Present a Forensic Case Report (02:00 – 03:30) • Team-based case presentation and peer review

Certification

Participants will receive a Certificate of Completion in Implementation & Management of Computer Forensics Processes (CLFE), validating their readiness to perform digital forensic investigations and support legal or internal inquiries in line with international best practices.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**