MAWA EVENTS

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

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

DIGITAL FORENSICS AUDIT: REVIEWS THE PROCESSES AND TOOLS USED FOR DIGITAL FORENSICS INVESTIGATIONS

"Mastering Forensic Audit Techniques to Investigate, Analyze, and Mitigate Cyber Incidents"

Schedule

Date	Venue	Fees (Face-to-Face)
03 – 07 Aug 2026	London, UK	USD 3495 per delegate

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

Introduction

In today's digital era, organizations face increasingly complex cybersecurity threats. Digital forensics plays a critical role in identifying, investigating, and responding to cyber incidents while preserving evidence for legal or regulatory action. This course provides a deep dive into the tools, techniques, and procedures used in digital forensic audits.

Participants will gain practical skills for conducting forensic investigations on computers, networks, mobile devices, and cloud systems. They will also learn how to handle digital evidence, maintain chain of custody, and document forensic findings that stand up to scrutiny in legal and compliance contexts.

Objectives

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

- Understand the fundamentals of digital forensics and its audit relevance
- Identify and preserve digital evidence while maintaining forensic integrity
- Apply forensic tools to analyze data from systems and networks
- Document and report forensic findings in line with legal and regulatory expectations
- Support incident response and internal investigations through structured forensic audits

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 hands-on experience with industry-recognized digital forensics tools
- Improve your organization’s cyber incident investigation capabilities
- Bridge the gap between IT, audit, and legal/compliance functions
- Learn how to conduct forensically sound investigations in real-world scenarios
- Enhance your audit reports with strong forensic documentation

Target Audience

This program is designed for:

- IT auditors and cyber risk professionals
- Internal auditors and compliance officers
- Information security managers and analysts
- Legal and governance professionals involved in investigations
- Anyone involved in post-incident review and cyber audit

Individual Benefits

Key competencies that will be developed include:

- Digital forensic investigation planning and execution
- Evidence acquisition, preservation, and chain of custody protocols
- Data recovery and artifact analysis
- Use of industry-standard forensic tools (e.g., FTK, Autopsy, EnCase)
- Forensic audit reporting and litigation-readiness

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Enhanced capability to investigate and respond to cyber incidents
- Reduced legal risk through proper evidence handling and reporting
- Strengthened audit functions with forensic insights
- Improved cross-functional response during investigations
- Compliance with standards such as ISO 27037, NIST 800-86, and GDPR

Instructional Methodology

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

- Strategy Briefings – Deep dive into digital forensics principles, frameworks, and legal standards
- Case Studies – Real-world investigations and forensic audit scenarios
- Workshops – Practical lab sessions using forensic software and tools
- Peer Exchange – Group discussions on investigative challenges and lessons learned
- Tools – Demonstrations and exercises with forensic tools and evidence logs

MAWA EVENTS

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

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

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

- Module 1: Digital Forensics and Audit Fundamentals (07:30 – 09:30)
- What is digital forensics? Scope and importance in audit
- Forensics within cybersecurity and IT audit frameworks
- Key legal and ethical considerations
- Module 2: Forensic Readiness and Frameworks (09:45 – 11:15)
- Understanding forensic readiness in organizations
- NIST and ISO standards in digital forensics
- Overview of policies and procedures
- Module 3: Cyber Incident and Breach Overview (11:30 – 01:00)
- Types of cyber incidents and fraud events
- Role of forensic audits in incident response
- Timeline and escalation process
- Module 4: Workshop – Forensic Readiness Checklist (02:00 – 03:30)
- Build a readiness checklist
- Group analysis of real-world incident response failures
- Identify key controls for future readiness

Day 2: Evidence Management and Legal Compliance

- Module 1: Digital Evidence and Chain of Custody (07:30 – 09:30)
- Sources of digital evidence: systems, emails, logs, devices
- Evidence collection protocols
- Chain of custody and audit documentation
- Module 2: Legal and Regulatory Compliance (09:45 – 11:15)
- GDPR, HIPAA, PCI-DSS, and regional laws
- Data privacy, integrity, and admissibility of evidence
- Cross-border challenges in evidence handling
- Module 3: Forensic Documentation and Reporting (11:30 – 01:00)
- Creating investigation reports
- Using documentation for legal and audit purposes
- Lessons from real forensic audit reports
- Module 4: Workshop – Chain of Custody Simulation (02:00 – 03:30)
- Practice scenario: collecting and documenting digital evidence
- Role play and critique on chain of custody errors
- Peer feedback and discussion

Day 3: Digital Forensics Tools and Techniques

- Module 1: Computer and Disk Forensics (07:30 – 09:30)
- Disk imaging and file recovery
- Understanding file systems and artifacts
- Tools: FTK Imager, Autopsy
-

Module 2: Network and Email Forensics (09:45 – 11:15)

- Network traffic capture and analysis
- Tracing suspicious activity in email logs
- Packet analysis with Wireshark
- Module 3: Memory and Mobile Device Forensics (11:30 – 01:00)
- Volatile memory analysis
- Mobile phone forensics and SIM data extraction
- Toolkits and device handling precautions
- Module 4: Workshop – Tool Demo and Analysis (02:00 – 03:30)
- Conduct a simple forensic analysis using demo tools
- Identify and explain digital artifacts
- Summarize findings in a structured audit report

Day 4: Investigative Techniques and Audit Integration

- Module 1: Digital Forensic Investigation Process (07:30 – 09:30)
- From incident to investigation: end-to-end process
- Scoping, planning, and execution phases
- Role of audit trails in digital investigations
- Module 2: Integrating Forensics into the Audit Cycle (09:45 – 11:15)
- Where and how forensic techniques apply in internal audit
- Risk-based audit planning for digital investigations
- Continuous monitoring and audit automation tools
- Module 3: Managing Forensics Teams and Third Parties (11:30 – 01:00)
- Internal vs. external forensic services
- Vendor selection, SLAs, and confidentiality
- Working with legal and HR in investigations
- Module 4: Workshop – Forensics in Audit Planning (02:00 – 03:30)
- Develop a sample audit plan with forensic elements
- Identify triggers and red flags for deeper investigation
- Discuss reporting strategies to management

Day 5: Case Studies, Ethics and Capstone Exercise

- Module 1: Ethics in Digital Forensics (07:30 – 09:30)
- Professional conduct and impartiality
- Conflicts of interest and legal traps
- Role of the auditor in ensuring fairness
- Module 2: Case Studies – Digital Forensics in Action (09:45 – 11:15)
- Dissect recent high-profile cyber forensic cases
- Lessons learned from audit and legal standpoints
- Discuss failures in forensic execution
- Module 3: Capstone Forensic Audit Simulation (11:30 – 01:00)
- Group scenario: plan and conduct a forensic audit
- Present findings to a mock executive team
- Receive peer and facilitator feedback
- Module 4: Final Review and Certification (02:00 – 03:30)

Summary of key lessons and practical takeaways

- Course evaluation and knowledge check
- Awarding of certificates and closing

Certification

Participants will receive a Certificate of Completion in Digital Forensics Audit, validating their competence in conducting digital investigations and forensic audits in line with industry, legal, and audit 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.

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