CONCEPT

Digital Forensics for Corporate Investigations: Digital Evidence, Chain of Custody and E-Discovery

Digital Forensics for Corporate Investigations: Digital Evidence, Chain of Custody and E-Discovery

Introduction:

Digital forensics now decides the outcome of many corporate investigations, yet cases collapse when emails are collected without authority, devices are examined before they are preserved or chain of custody records have gaps. Investigators, auditors, HR and legal teams rarely image a device themselves, but they must scope, authorise, supervise and rely on forensic work that will later be challenged. This Core Concept course builds that capability around ISO/IEC 27037 and related guidance through case study work. Participants leave with a Digital Evidence Investigation Plan and Case File Template.

Course Objectives:

- Assess whether an internal investigation needs digital forensic support and confirm the authorisation and privacy basis before any collection starts
- Apply ISO/IEC 27037 principles to identify, collect, acquire and preserve digital evidence from email, endpoints, mobile devices, cloud platforms and logs
- Maintain chain of custody forms and evidence registers that withstand scrutiny by management, tribunals or courts
- Scope and instruct forensic specialists and e-discovery providers with clear questions, custodians, search terms and deliverables
- Interpret forensic findings and build a multi-source timeline that tests alternative explanations
- Produce a Digital Evidence Investigation Plan and Case File Template ready for the next internal investigation

Target Audience:

- Corporate investigators responsible for handling internal allegations from intake to findings
- Internal auditors who examine suspected control breaches and employee misconduct
- HR investigation leads responsible for disciplinary and grievance investigations
- In-house legal counsel who manage legal holds, disclosure and external forensic providers
- Compliance and ethics officers who oversee whistleblowing cases and investigation outcomes

Course Outline:

Day 1: Digital Evidence in Corporate Investigations

- Digital Forensics in the Investigation Lifecycle: Allegation to Outcome
- Digital Evidence Types: Content, Metadata and System Records
- Relevance, Reliability and Sufficiency Tests for Digital Evidence
- Legal Authorisation, Acceptable Use Policy and Privacy Considerations Checklist
- Investigation Readiness Self-Assessment of Evidence Sources and Policies

Day 2: ISO/IEC 27037 and the Evidence Standards Family

- ISO/IEC 27037:2012 Scope: Identification, Collection, Acquisition and Preservation
- Auditability, Repeatability, Reproducibility and Justifiability Requirements
- Digital Evidence First Responder and Digital Evidence Specialist Roles
- ISO/IEC 27041, 27042 and 27043: Method Assurance, Analysis and Investigation Process
- EDRM Stages from Information Governance to Presentation

Day 3: Preservation, Collection and Evidence Sources

- Evidence Source Map: Email, Endpoints, Mobile Devices, Cloud and Collaboration Platforms
- Legal Hold Notice Drafting and Custodian Identification Log
- Forensic Imaging, Hash Verification and Write Blocking Explained for Investigators
- Chain of Custody Form and Evidence Register Completion
- Log and Audit Trail Sources: Access, Authentication and Application Records

Day 4: Specialist Analysis, E-Discovery Review and Evidential Risk

- Forensic Specialist Scoping Letter: Questions, Custodians and Deliverables
- E-Discovery Processing: De-Duplication, Keyword Searching and Review Batches
- Interpreting Forensic Artefacts, Timestamps and Alternative Explanations
- Investigation Timeline Construction from Multi-Source Records
- Evidential Pitfalls: Spoliation, Over-Collection, Privilege and Personal Data Exposure

Day 5: Investigation Case Studies and the Case File

- Case Study: Confidential Data Removal by a Departing Employee
- Case Study: Misconduct Allegation Using Messaging and Email Records
- Findings Report Structure for Management, Tribunal and Court Audiences
- Digital Evidence Investigation Plan and Case File Template Drafting
- Peer Challenge Panel: Defending Digital Evidence Under Questioning

Skills You Will Gain:

- Digital Evidence Preservation
- Chain of Custody Management
- Investigation Authorisation Review
- Forensic Specialist Instruction
- E-Discovery Scoping
- Timeline Analysis
- Evidential Report Writing

Why Attend This Course:

- Leave with a Digital Evidence Investigation Plan and Case File Template tested on realistic data removal and misconduct cases
- Ask forensic specialists the right questions and challenge their findings before relying on them in a decision
- Reduce the risk of cases failing because of gaps in authorisation, preservation or custody records
- Compare investigation practice with auditors, HR and legal professionals from finance, energy, healthcare and public service

Conclusion:

Digital evidence carries weight only when it was gathered lawfully, preserved intact and explained in terms a decision maker can test. This course moves from evidence principles and authorisation, through ISO/IEC 27037 and the related evidence standards, to preservation, custody, specialist instruction, e-discovery review and timeline analysis. The final day applies that work to realistic corporate cases and produces a Digital Evidence Investigation Plan and Case File Template that participants can use to run their next investigation to a defensible standard.