
Digital Forensics Management Course: Scoping, Evidence Preservation and Reading Findings

4 – 8 April 2027
Zoom





Digital Forensics Management Course: Scoping, Evidence Preservation and Reading Findings

Ref: 729_35262 Date: 4 – 8 April 2027 Location: Zoom Fees: 1700 GBP

Programme Summary

Digital forensics management is the subject of this one-week training course for heads of investigations, security and compliance directors and legal managers at managerial level, ending in a digital forensics instruction pack for one investigation. Managers commission examinations of devices, email, cloud accounts and mobiles that they cannot perform themselves, then rely on the findings in internal and legal proceedings. The programme moves from scope and readiness to preservation, provider direction and the reading of reports, using examples from corporate, financial and public sector inquiries. Mars Training Centre UK delivers this programme on digital forensics management to mixed-organisation cohorts.

The Business Case

Digital evidence is fragile. A device switched on at the wrong moment, an account accessed by an administrator before collection, or an instruction that leaves the question vague can weaken a case before an examiner starts. Managers who define the question, protect the sources and test the provider's method receive findings that can be explained to a tribunal, a regulator or a board, and avoid paying for work that does not answer the issue.

- Evidence Integrity: Strengthens as sources are preserved and verified before examination begins.
- Provider Cost Control: Improves as instructions state scope, limits and change routes in writing.
- Decision Confidence: Rises as findings are read against their stated limits and the allegation.

Principles and Evidence Base

- ISO/IEC 27037 Guidelines for Digital Evidence: Frames identification, collection, acquisition and preservation of digital evidence, applied in Session 2.
- ISO/IEC 27041 Assurance of Investigative Methods: Frames the questions managers ask about whether a method suits its purpose, applied in Session 3.
- ISO/IEC 27042 Analysis and Interpretation: Frames how findings are analysed and how far they can be relied on, applied in Session 4.
- ISO/IEC 27043 Investigation Principles and Processes: Frames the stages from readiness to closure that structure the whole programme, applied in Sessions 1 and 5.



Intended Participants

- Managers who lead internal or regulatory investigations and decide what digital sources to examine.
- Security directors who prepare their organisation to preserve evidence before an incident.
- Compliance directors who commission forensic work on conduct, fraud or policy breaches.
- Legal managers who instruct providers and present digital findings in proceedings.
- Heads of function who sponsor investigations and must judge the strength of the findings.

Typical settings include financial services, public bodies, energy companies and professional services firms.

Learning Outcomes

1. Participants will be able to formulate an investigation question and match it to the digital sources that can answer it.
2. Participants will be able to evaluate an organisation's forensic readiness and legal basis before an examination.
3. Participants will be able to construct preservation and collection instructions for devices, email, cloud accounts and mobiles.
4. Participants will be able to prioritise provider selection criteria and draft an examination instruction.
5. Participants will be able to diagnose gaps and overstatements in a forensic report.
6. Participants will be able to justify a decision from digital findings and their stated limits.

Programme Structure

Day 1: Digital Forensics Management: Scope and Readiness

What should be examined and why, and what must be ready before an incident arises?

- Investigation Question Statement
- Evidence Source Inventory
- Forensic Readiness Checklist
- ISO/IEC 27043 Process Map
- Legal Basis and Privacy Screen

Day 2: Evidence Preservation and Collection Oversight

How is digital material preserved so that its integrity can be shown later?

- ISO/IEC 27037 Handling Stages
- Device and Account Preservation Order
- Cloud and Email Collection Request
- Mobile Device Handling Sheet
- Integrity Verification Record



Day 3: Choosing and Directing Forensic Providers

How is an examiner chosen, instructed and quality-checked?

- Provider Selection Criteria
- Examination Instruction Letter
- ISO/IEC 27041 Method Assurance Questions
- Scope Change Log
- Cost and Timeline Estimate Sheet

Day 4: Reading Findings and Reports

What does a forensic report establish, and where are its limits?

- ISO/IEC 27042 Interpretation Checklist
- Timeline Reconstruction Review
- Artefact Reliability Grid
- Report Challenge Questions
- Finding to Allegation Map

Day 5: Digital Forensics Instruction Pack for One Investigation

Do the earlier tools form one pack that sets up, directs and tests a forensic examination?

- Applying the Session 1 Evidence Source Inventory
- Testing the Session 2 Preservation Order
- Reviewing the Session 3 Instruction Letter
- Checking the Session 4 Report Challenge Questions
- Completing the Digital Forensics Instruction Pack

Methodology

The programme uses a structured exercise built on one prepared investigation, with an allegation, a source list, a draft provider proposal and a sample report. Participants make each management decision, record the reason in a common format and compare results in small groups before applying the same tools to an investigation from their own organisation.

- Suggested activity: Ranking evidence sources by value, fragility and legal constraint.
- Suggested activity: Rewriting a vague instruction into a scoped examination letter.
- Suggested activity: Marking overstatements in a sample forensic report.



Capstone Output

Each participant completes a digital forensics instruction pack for one investigation. It holds an investigation question, a source inventory, preservation instructions, an examination instruction letter, provider selection criteria and a list of questions for the report received. The pack is used at work to brief the legal team and to direct the examiner.

Frequently Asked Questions

Is digital forensics management training suitable for managers without a technical background?

Yes. Digital forensics management is taught through a worked investigation. The training assumes responsibility for commissioning or relying on investigations, but no technical or programming skills.

Which references does digital forensics management training rest on?

Digital forensics management training rests on the ISO/IEC 27037, 27041, 27042 and 27043 standards on digital evidence, which cover handling, method assurance, interpretation and investigation processes.

How is the instruction pack from digital forensics management training used at work?

You use the digital forensics instruction pack to brief your legal team, direct the examiner, and test the report against your question before you act on it.

How does digital forensics management differ from cyber incident response training?

Digital forensics management training covers evidence preservation, provider direction and report reading for investigations, while cyber incident response training concentrates on detecting, containing and recovering from attacks.