JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Computer Forensic Investigation Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Computer Forensic Investigation Training Course

Computer Forensic Investigation is a 1-week training course for digital forensic examiners, investigators and incident handlers who recover and interpret evidence from computers, and it produces a forensic examination report that withstands challenge. Fraud, insider misuse and cyber intrusions now leave their clearest traces on disks, logs and registries, so evidence handled carelessly can collapse a disciplinary case or a legal claim. Jupiter Prime Training delivers this computer forensic investigation course.

Why Computer Forensic Investigation Matters Now

Three pressures shape forensic work today. Storage volumes keep growing, solid-state drives and encryption complicate recovery, and courts, auditors and opposing experts scrutinise every acquisition step. An organisation that preserves evidence correctly can discipline staff, pursue recovery of losses and learn exactly how an intruder operated; one that does not risks inadmissible findings and repeated incidents. Forensic readiness connects to the Respond and Recover functions of the NIST Cybersecurity Framework 2.0 NIST CSF 2.0 and to the incident evidence controls of ISO/IEC 27001:2022.

Who Gains Most from Computer Forensic Investigation

- Examiners who acquire, image and analyse storage media from seized devices
- Investigators who handle fraud, misconduct and data theft cases
- Incident handlers who preserve volatile and disk evidence during intrusions
- Security analysts who build timelines from logs and system artefacts
- Audit and compliance specialists who commission or rely on forensic findings

Internal investigation units in banking and healthcare gain most when examiners and case investigators attend together, because they adopt one evidence handling standard.

Computer Forensic Investigation Capabilities

Participants move from ad hoc file searches to a repeatable examination method whose every step can be explained under cross-examination.

- Apply sound acquisition methods that preserve original media integrity — legal counsel
- Build forensic images verified by cryptographic hash values — case investigator
- Analyse file systems, deleted data and registry artefacts — lead examiner
- Reconstruct event timelines from file metadata and system logs — incident manager
- Test and document forensic tool behaviour before relying on results — quality reviewer
- Communicate findings in reports and testimony understood by non-specialists — tribunal or disciplinary panel

Key Computer Forensic Investigation Terms

- Chain of custody — the documented record of who held evidence, when, where and why, from seizure to presentation.
- Forensic image — a bit-for-bit copy of storage media, including unallocated space, used for examination instead of the original.
- Hash value — a fixed-length digital fingerprint that proves an image has not changed since acquisition.
- Write blocker — a device or software control that prevents any change to source media during acquisition.
- Registry artefact — a Windows registry entry revealing user activity, connected devices or program execution.
- Super timeline — a merged chronology of file system, log and artefact events used to reconstruct activity.

Computer Forensic Investigation Day by Day

Day 1: Forensic Principles and Case Preparation

- Forensic Process Model — Sequencing Identification, Preservation, Analysis and Presentation
- Legal Authority Checks — Confirming Permission Before Examining Devices
- Chain of Custody Forms — Recording Every Evidence Transfer
- Forensic Readiness — Linking Evidence Capture to NIST CSF 2.0 Respond
- Case Scoping Interview — Defining Questions the Examination Must Answer

Day 2: Evidence Acquisition and Imaging

- Volatile Memory Capture — Deciding What to Collect Before Shutdown
- Write Blocking Methods — Protecting Source Media During Acquisition
- Disk Imaging Formats — Choosing Raw or Compressed Evidence Containers
- Hash Verification — Proving Image Integrity Across Every Copy
- Tool Validation Testing — Documenting Known Behaviour of Forensic Software

Day 3: File System and Registry Analysis

- File System Structures — Interpreting NTFS and FAT Metadata
- Deleted File Recovery — Carving Data from Unallocated Space
- Registry Hive Examination — Tracing User Activity and USB Devices
- Browser and Email Artefacts — Linking Communications to Suspects
- Encryption and Anti-Forensics Indicators — Judging Evidence Tampering Risk

Day 4: Timelines and Correlation

- Timestamp Interpretation — Resolving Time Zones and Clock Drift
- Super Timeline Construction — Merging File, Log and Artefact Events
- Event Log Analysis — Identifying Logons, Execution and Lateral Movement
- Hypothesis Testing — Weighing Competing Explanations of User Activity
- Evidence Controls Mapping — Aligning Findings with ISO/IEC 27001:2022 Logging

Day 5: Practising the Forensic Examination Report

- Acquisition Record Review — Confirming Custody and Hash Evidence from Day Two
- Artefact Findings Selection — Choosing Registry and File Evidence to Present
- Timeline Exhibit Preparation — Presenting Reconstructed Events Clearly
- Mock Cross-Examination — Defending Methods Under Hostile Questioning
- Forensic Examination Report — Finalising Findings, Limitations and Exhibits

Applying Computer Forensic Investigation After the Course

- Rewrite the unit's chain of custody form and test it on the next evidence seizure.
- Run a validation test on the primary imaging tool and file the results with case procedures.

Computer Forensic Investigation Questions FAQ

What is computer forensic investigation and why does it matter now?

It is the disciplined recovery and interpretation of digital evidence from computers so findings hold up to scrutiny. It matters now because fraud, misconduct and intrusions increasingly leave their main traces on digital media.

Which roles gain most from computer forensic investigation training?

Digital forensic examiners, case investigators and incident handlers gain most. Security analysts and audit specialists who rely on forensic findings also benefit from knowing how evidence is acquired and tested.

How does computer forensic investigation differ from an incident response course?

Forensic investigation focuses on evidential depth, admissibility and reporting. An incident response course centres on rapid containment and recovery, whereas here you examine media in detail and defend each finding.

What do you bring back from computer forensic investigation training?

You bring back a forensic examination report drafted from a case image, with custody records, timeline exhibits and stated limitations, ready to use as a template for your unit.

Computer Forensic Investigation: The Way Forward

The forensic examination report first informs whether a case proceeds to disciplinary, civil or criminal action. Investigators, legal counsel and decision panels use it to weigh the evidence. After its first use, revisit how well the timeline exhibits were understood by non-specialists, and simplify any finding that drew repeated questions.