



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

Digital & Computer Forensics Investigator – Enterprise DFIR

Course + certificate

2.800,00 €

VAT excluded

Course code

DFIR-FORENSICS-PRO

Minimum duration

480 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Professional computer-forensics and digital-evidence pathway for DFIR analysts, incident responders, auditors and consultants: forensic readiness, acquisition, preservation, host/network/cloud analysis, timelines, chain of custody, reporting and methodological quality.

This extended technical dossier describes the pathway as published in CIWZ Academy on the issue date. It consolidates purpose, references, learning architecture, module contents, assessment system, passing criteria and certificate conditions. It does not replace the official texts of the standards, laws, guidelines or schemes referenced.

2. Normative, regulatory and technical references

ISO/IEC 27037:2012 (current, under review); ISO/IEC 27041:2015; ISO/IEC 27042:2015; ISO/IEC 27043:2015; NIST SP 800-86; ISO/IEC 27035-1:2023; GDPR and applicable national law for evidence handling

References are used as the learning and assessment framework within the limits of published content and available sources. For professional application, the official and current versions of the referenced documents always prevail.

3. Learning architecture and assessment system

- 8 structured learning modules
- minimum tracked time: 480 min
- intermediate-check bank: 256 questions
- active final-exam bank: 240 questions
- final exam: 30 questions selected from the bank
- passing threshold: 75%
- Access to the pathway through the personal Academy profile or a corporate assignment.
- Sequential study of the modules, with server-side recording of progress and required minimum time.

- Intermediate checks linked to modules to verify understanding, application capability and quality of reasoning.
- Final exam unlock only after the pathway requirements have been completed.
- Protected final exam assembled by the platform through selection from the active course question bank.
- Recording of the result and, where applicable, the option to request the final certificate.

4. Official catalogue technical information

Course technical sheet

CIWZ Academy executive/professional pathway with original content, server-tracked learning, 8 modules, randomized intermediate checks, Secure Proctor in assessments and a scenario-based final question bank. Free access; any fee applies only to certificate issuance after passing.

5. Detailed course syllabus

The following syllabus is derived from the active modules published on the platform. Each module shows its minimum study time and the size of its available intermediate-check bank.

01 Forensic readiness, legal authority and investigation planning

Minimum time: 60 min | Intermediate questions: 32

02 Identification, collection, acquisition and preservation

Minimum time: 60 min | Intermediate questions: 32

03 Investigative method, tool validation and repeatability

Minimum time: 60 min | Intermediate questions: 32

04 File systems, endpoint artefacts and memory forensics

Minimum time: 60 min | Intermediate questions: 32

05 Network, email and cloud forensics

Minimum time: 60 min | Intermediate questions: 32

06 Timeline analysis, hypothesis testing and attribution discipline

Minimum time: 60 min | Intermediate questions: 32

07 Malware triage and compromise analysis

Minimum time: 60 min | Intermediate questions: 32

08 Reporting, expert communication and quality assurance

Minimum time: 60 min | Intermediate questions: 32

6. Developed module-by-module contents

The following pages analytically describe the content actually associated with each platform module. The structure is designed so that learners, companies, HR, Quality, HSE or CISO functions can understand precisely what is studied and assessed.

MODULE 01**Forensic readiness, legal authority and investigation planning**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Prepare people, processes, logging, time synchronization, tools, storage and authorizations so an investigation can start quickly and produce usable evidence.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define scope, authority, objectives, constraints, privacy/legal liaison, evidence sources, preservation priorities and investigation plans.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Define scope, authority, objectives, constraints, privacy/legal liaison, evidence sources, preservation priorities and investigation plans.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Forensic readiness plan, authorization record, source map, tool list, time references, retention policy and investigation objectives.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

An internal insider investigation involves personal mailboxes and BYOD: clarify authority, proportionality and sources before acquisition. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Time from authorization to preservation of volatile/critical sources.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Acquiring before authority is defined; unsynchronized logs; unvalidated tools; retention shorter than discovery timelines.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Forensic readiness, legal authority and investigation planning".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 02**Identification, collection, acquisition and preservation**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Apply ISO/IEC 27037 principles to identify potential evidence, collect/acquire it using appropriate methods and preserve integrity and traceability.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Choose live vs dead acquisition, volatility priorities, write protection, imaging, hashing, labeling, packaging, transport and secure storage.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Choose live vs dead acquisition, volatility priorities, write protection, imaging, hashing, labeling, packaging, transport and secure storage.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Acquisition worksheets, source identifiers, hash values, tool/version, timestamps, chain of custody and storage records.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

An encrypted laptop is powered on with active cloud sessions: balance volatile acquisition, alteration risk and the value of current access. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Share of acquisitions with verified hashes and complete chain of custody at first review.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Automatically powering off every host; no hashes; ambiguous labels; working directly from originals.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Identification, collection, acquisition and preservation".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 03**Investigative method, tool validation and repeatability**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Ensure methods and tools are fit for purpose, documented, validated and used to support independent scrutiny, repeatability and reproducibility where relevant.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Define requirements, known limitations, test datasets, validation records, analyst procedures, quality reviews and alternative verification methods.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Define requirements, known limitations, test datasets, validation records, analyst procedures, quality reviews and alternative verification methods.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Tool validation record, version/hash, configuration, known limitations, test results, peer review and method notes.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

Two tools produce different timestamps for the same artefact: identify timezone/parsing assumptions and verify with an independent source. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Share of critical tools with current validation and analytical findings subject to peer review.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Trusting the tool brand; updates without revalidation; screenshots as sole evidence; unversioned procedures.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Investigative method, tool validation and repeatability".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 04**File systems, endpoint artefacts and memory forensics**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Interpret file systems, metadata, registry/configuration, event logs, browsers, execution artefacts, persistence, deleted data and volatile memory against investigative hypotheses.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Correlate multiple artefacts, handle timestamps, file carving, process/network memory evidence, user activity and anti-forensics indicators.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Correlate multiple artefacts, handle timestamps, file carving, process/network memory evidence, user activity and anti-forensics indicators.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Timeline sources, parsed artefacts, memory images, process trees, persistence evidence, deleted-file recovery and analyst notes.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A malicious file no longer exists but execution artefacts, network connections and persistence remain: build a conclusion without over-interpreting. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Average number of independent sources supporting a critical finding.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Conclusions from a single artefact; ignored time zones; metadata treated as absolute proof; memory acquired too late.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "File systems, endpoint artefacts and memory forensics".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 05**Network, email and cloud forensics**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Analyse packet/log/flow, DNS, proxy, VPN, email headers, identity-provider, SaaS/cloud audit and API evidence while considering retention and shared responsibility.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Preserve logs quickly, correlate identity/network/cloud, verify source reliability, tenant context, timestamps and provider limitations.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Preserve logs quickly, correlate identity/network/cloud, verify source reliability, tenant context, timestamps and provider limitations.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: PCAP/flow, DNS/proxy logs, mail traces, IdP audit, cloud activity logs, provider export metadata and retention records.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A compromised account uses valid tokens without interactive login: reconstruct the cloud session and source IP without relying only on sign-in events. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Temporal coverage of sources and share of incidents with critical logs preserved before retention expiry.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Exporting logs without export metadata; confusing NAT/proxy addresses with users; ignoring service principals and token refresh.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Network, email and cloud forensics".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 06**Timeline analysis, hypothesis testing and attribution discipline**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Build super-timelines, separate facts from inference, use confidence levels and test alternative hypotheses to reduce investigative bias.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Normalize time zones, correlate sources, record hypotheses/evidence, seek disconfirming evidence and document uncertainty.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Normalize time zones, correlate sources, record hypotheses/evidence, seek disconfirming evidence and document uncertainty.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Normalized timeline, evidence matrix, hypothesis log, confidence ratings, alternative explanations and peer-review comments.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A sequence appears to show exfiltration but traffic coincides with scheduled backup: test the alternative hypothesis before concluding. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Share of critical findings with independent source support and explicit confidence statements.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Narrative built too early; confirmation bias; unnormalized timestamps; personal attribution based on username alone.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Timeline analysis, hypothesis testing and attribution discipline".

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 07**Malware triage and compromise analysis**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Perform proportionate static/dynamic triage and connect IOCs, behaviour, persistence, credential access and command-and-control to the investigation without turning the course into specialist reverse engineering.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Use hashing, strings/metadata, sandboxing, YARA/IOCs where appropriate, behaviour timelines and containment implications, preserving samples securely.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Use hashing, strings/metadata, sandboxing, YARA/IOCs where appropriate, behaviour timelines and containment implications, preserving samples securely.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Sample hash, source, sandbox report, behaviour indicators, network IOCs, persistence evidence and secure-sample handling logs.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

A sample is classified as commodity malware but uses custom persistence: assess whether the vendor label actually describes the case. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Time from sample collection to verified actionable IOC distribution.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Uploading sensitive samples to public services without authorization; trusting antivirus names; IOCs without expiry/context.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to “Malware triage and compromise analysis”.

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

MODULE 08**Reporting, expert communication and quality assurance**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Produce reports that distinguish evidence, method, results, limitations, inferences and conclusions, understandable to management, legal and technical audiences and open to scrutiny.

Professional objectives

By the end of the module the participant should turn the topic into decisions, controls and verification. Operational focus: Use repeatable structure, source references, confidence, exhibits, peer review, versioning and secure distribution; avoid absolute language beyond the evidence.

Operational method

Apply a structured cycle: define context and purpose, set criteria before decisions, assign accountability, execute controls, collect evidence and review results. For this topic: Use repeatable structure, source references, confidence, exhibits, peer review, versioning and secure distribution; avoid absolute language beyond the evidence.

Evidence and auditability

Professional quality is demonstrated by coherent, reconstructable evidence, not merely by procedures. Key evidence: Final report, executive summary, evidence index, exhibits, method annex, limitation statement, peer-review record and distribution log.

Decisions, risk and proportionality

Decisions should be proportionate to criticality, exposure, impact, information reliability and applicable requirements. Document assumptions, confidence, exceptions and reassessment triggers.

Applied case

The analyst believes a user probably performed an action but evidence proves only the account: phrase the conclusion proportionately. Separate facts from hypotheses, identify missing information, choose the initial action and define what evidence will demonstrate that the decision was effective.

Indicators and weak signals

A useful indicator needs a formula, source, frequency, owner, threshold and associated decision. For this module monitor at least: Share of critical reports peer-reviewed and number of post-issuance corrections for methodological errors.

Common failure modes

Avoid merely formal approaches. Typical weaknesses: Conclusions without source references; omitted limitations; certainty applied to inference; technical reports incomprehensible to decision makers.

Decision laboratory

Scenario: a condition changes suddenly (technology, supplier, requirement, volume, threat or responsibility). Build a five-step response: impact, criterion, decision, evidence, review. Apply it to "Reporting, expert communication and

quality assurance”.

Assessment preparation

Before the assessment, make sure you can explain the topic without reading the slides, justify a decision in an ambiguous scenario, identify at least two independent pieces of evidence and distinguish a substantive response from a documentary one.

7. Assessment system, final exam and passing criteria

- Intermediate checks are linked to individual modules and provide progressive learning control before access to the final assessment.
- The final assessment consists of 30 questions selected from the active course bank. The platform applies an anti-repetition logic for new attempts when the bank size allows it.
- Final question-bank size detected at generation time: 240 active questions.
- Published passing threshold for the course: 75%.
- Questions are intended to assess not only recall but also interpretation, application, evidence selection, scenario assessment and quality of decision-making, depending on the subject matter.

8. Tracking, learning continuity and session integrity

- Path status, completed modules and recorded time are managed server-side when the course uses the Academy learning mode.
- The platform allows the pathway to resume from the recorded point and retains the results of required checks.
- Assessment sessions may be subject to the integrity and proctoring controls enabled by the platform and described in the applicable usage rules.
- Technical and integrity events support assessment and do not replace professional judgement where human review is required.

9. Certificate, use and limitations

The CIWZ certificate, where provided by the pathway and requested after passing, records the result achieved in the stated CIWZ pathway or assessment. It does not automatically replace personnel certification, professional registration, statutory licence, legal qualification or credentials issued by third-party bodies where such requirements are imposed by the applicable scheme.

10. Commercial and tax conditions

- Course + certificate: 2.800,00 € VAT excluded.
- UAE VAT is applied to UAE customers according to billing data and the applicable tax rules.
- Any specific commercial terms, agreements or corporate orders override the public price only when formally accepted by Certificato IWZ FZCO.

11. Dossier document control

- Document automatically generated by CIWZ Academy from the course data published at the time of the request.

- Course code: DFIR-FORENSICS-PRO
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.