Database Forensics

Four-week internship task & guidance guide

A fictional SQLite order ledger includes an audit trail. Examine a preserved copy using read-only access and compare recorded changes with final rows; this is not a production database investigation.

Working format

Four independent weekly submissions, each assessed out of 100. Each upload must include a PDF report and a separate description of at least 200 words in the student portal. Complete weeks 1-4 in order; early completion is permitted. Calendar deadlines are set by academy staff, not inferred from this guide.

What you need

A laptop, spreadsheet editor, PDF exporter and a SHA-256 hashing utility. The database domain also needs a SQLite viewer that supports read-only mode. Use only the accompanying synthetic dataset and document every transformation.

Evidence pack

Download database-training-data.zip beside this PDF on the website. The ZIP includes source exports, a README and a SHA-256 manifest. These are deliberately small teaching exports, not a complete forensic image. All identities and events are fictional.

Learning outcomes

Preserve integrity; document a reproducible examination; correlate evidence cautiously; separate observation from inference; communicate supported findings and limitations.

WEEK 1

Read-only database intake

Goal: Establish scope and a verifiable evidence baseline.

Task checklist

1. Inventory training.db and schema.sql, compute SHA-256 values and preserve originals.

2. Open only a working copy in read-only mode. List tables, column meanings, primary keys and relationships.

3. Record engine/tool versions and explain the absence of transaction logs, original host context and a historical snapshot.

Required hand-in

schema_map.pdf, evidence_register.csv and read_only_method.pdf

Portal description

Write at least 200 words in your own language explaining your method, source files and row/event IDs, observations, assumptions, uncertainty and learning. Put this text in the description box as well as any report appendix. Do not use filler to satisfy the word count.

Quality checks before upload

Keep the original evidence unchanged. Preserve raw timestamps and units. Identify tool versions and filters. Cite evidence IDs in findings. Recompute hashes of preserved files and include the result. Name your main file PFSA_<student-id>_database_W1.pdf. Supporting tables may be placed in one ZIP. Keep the uploaded file below 10 MB.

Week assessment: integrity 20 | method 25 | analysis 25 | evidence references 20 | clarity 10

WEEK 2

Integrity and consistency checks

Goal: Examine source records and document defensible observations.

Task checklist

1. Count rows by table and check duplicate order IDs, null required fields and references to missing customers.

2. Compare recorded order totals to quantities and unit prices, keeping the exact SELECT statements used.

3. Distinguish intentionally unusual training records from conclusions about misconduct; explain limitations of the supplied schema.

Required hand-in

checks.sql, integrity_results.csv and discrepancy_notes.pdf

Portal description

Write at least 200 words in your own language explaining your method, source files and row/event IDs, observations, assumptions, uncertainty and learning. Put this text in the description box as well as any report appendix. Do not use filler to satisfy the word count.

Quality checks before upload

Keep the original evidence unchanged. Preserve raw timestamps and units. Identify tool versions and filters. Cite evidence IDs in findings. Recompute hashes of preserved files and include the result. Name your main file PFSA_<student-id>_database_W2.pdf. Supporting tables may be placed in one ZIP. Keep the uploaded file below 10 MB.

Week assessment: integrity 20 | method 25 | analysis 25 | evidence references 20 | clarity 10

WEEK 3

Audit trail reconstruction

Goal: Correlate sources and evaluate competing explanations.

Task checklist

1. Join audit records to orders using their identifiers and sort changes by timestamp.

2. Compare before_value, after_value and the final order amount. Flag a missing or inconsistent audit transition.

3. Explain why an application-level audit record is not a complete database transaction log or proof of actor identity.

Required hand-in

audit_timeline.csv, reconstruction.sql and limitations.pdf

Portal description

Write at least 200 words in your own language explaining your method, source files and row/event IDs, observations, assumptions, uncertainty and learning. Put this text in the description box as well as any report appendix. Do not use filler to satisfy the word count.

Quality checks before upload

Keep the original evidence unchanged. Preserve raw timestamps and units. Identify tool versions and filters. Cite evidence IDs in findings. Recompute hashes of preserved files and include the result. Name your main file PFSA_<student-id>_database_W3.pdf. Supporting tables may be placed in one ZIP. Keep the uploaded file below 10 MB.

Week assessment: integrity 20 | method 25 | analysis 25 | evidence references 20 | clarity 10

WEEK 4

Database findings report

Goal: Present a reproducible, evidence-supported conclusion.

Task checklist

1. Write a 4-6 page report with schema, read-only method, integrity checks and a reconstruction of two selected orders.

2. Include query text, result excerpts, row IDs and the difference between observed inconsistency and attribution.

3. Re-hash the preserved original and provide a reproducibility appendix for all SELECT queries.

Required hand-in

database_report.pdf, queries.sql and results.zip

Portal description

Write at least 200 words in your own language explaining your method, source files and row/event IDs, observations, assumptions, uncertainty and learning. Put this text in the description box as well as any report appendix. Do not use filler to satisfy the word count.

Quality checks before upload

Keep the original evidence unchanged. Preserve raw timestamps and units. Identify tool versions and filters. Cite evidence IDs in findings. Recompute hashes of preserved files and include the result. Name your main file PFSA_<student-id>_database_W4.pdf. Supporting tables may be placed in one ZIP. Keep the uploaded file below 10 MB.

Week assessment: integrity 20 | method 25 | analysis 25 | evidence references 20 | clarity 10

Assessment & handover

Each week: 100 marks

Criterion	Marks	Expected evidence
Integrity and scope	20	Hashes, scope, preserved originals
Method and reproducibility	25	Clear steps, versions, filters or queries
Analysis and reasoning	25	Supported observations and alternatives
Evidence references	20	Exact file and row/event references
Communication	10	Clear report and 200-word portal narrative

Academic integrity

State which tools or writing assistance you used. Submit your own analysis and explain any reused template. A confident unsupported claim is weaker than a clearly stated uncertainty. This guide does not confer professional licensing, accreditation or an official affiliation.

Completion documents

Four submitted weeks unlock the document request stage. Assessment, payment confirmation and publication remain staff-controlled. A recommendation depends on evaluation; it is not automatic.

Further reading

NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response.
https://csrc.nist.gov/pubs/sp/800/86/final

These publications are background reading. PFSA authored the task sequence and synthetic evidence pack; NIST has not endorsed this programme.