Computer & Cyber Forensics

Four-week internship task & guidance guide

A fictional office export contains a document inventory and activity log. Determine what the export supports about a report revision, without claiming access to an original disk.

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 computer-cyber-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

Evidence intake and integrity

Goal: Establish scope and a verifiable evidence baseline.

Task checklist

1. Inventory every file in the supplied training ZIP; assign evidence IDs CC-01 onward and record size, SHA-256, source and collection time.

2. Create separate originals and working folders. Hash before analysis and explain why copying an export is not a forensic disk acquisition.

3. Write a chain-of-custody table with custodian, action, timestamp, purpose and integrity result.

Required hand-in

evidence_register.csv, sha256_manifest.csv, preservation_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>_computer-cyber_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

File metadata examination

Goal: Examine source records and document defensible observations.

Task checklist

1. Examine file_inventory.csv without editing the preserved copy. List each document version, supplied metadata and missing original-file properties.

2. Compare report v1 and v2 metadata to the activity log. Identify conflicting or ambiguous records without assuming which source is correct.

3. Build an observation table with evidence ID, exact row reference, observation, interpretation and confidence.

Required hand-in

metadata_comparison.csv and examination_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>_computer-cyber_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

Correlated activity timeline

Goal: Correlate sources and evaluate competing explanations.

Task checklist

1. Normalize all supplied timestamps to UTC and retain their original forms in a second column.

2. Create a minimum eight-event timeline linking log records to inventory entries; flag events with no independent corroboration.

3. Test two explanations for the report revision: expected editing and an unverified account action. List what evidence would distinguish them.

Required hand-in

timeline.csv, two_hypotheses.pdf and annotated references

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>_computer-cyber_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

Case report and peer handover

Goal: Present a reproducible, evidence-supported conclusion.

Task checklist

1. Produce a 4-6 page report answering whether the supplied export supports a revision, who or what is named in logs, and what cannot be concluded.

2. Include scope, methods, tool versions, hash checks, evidence citations, alternative explanations and limitations.

3. Add a one-page handover checklist another student can reproduce from the training ZIP.

Required hand-in

final_report.pdf, timeline.csv, hash_manifest.csv and handover.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>_computer-cyber_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.