IoT & Digital Device Forensics

Four-week internship task & guidance guide

A fictional sensor export combines device inventory, telemetry and gateway events. Work only with supplied files; no hardware access, radio capture or device modification is needed.

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 iot-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

Device ecosystem mapping

Goal: Establish scope and a verifiable evidence baseline.

Task checklist

1. Inventory devices.csv, telemetry.csv and gateway.csv; compute file hashes and assign evidence IDs.

2. Draw device-to-gateway relationships and list the device clock assumptions and measurement units.

3. Describe an appropriate preservation plan for a real device, while stating no actual hardware acquisition occurs in this exercise.

Required hand-in

ecosystem_map.pdf, evidence_register.csv and preservation_plan.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>_iot_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

Telemetry quality review

Goal: Examine source records and document defensible observations.

Task checklist

1. Group readings by device and compute count, minimum, maximum and time gaps.

2. Identify duplicate sequence numbers, missing intervals and the deliberately offset sensor clock.

3. Decide whether each anomaly may reflect collection loss, clock drift or a device event; keep observations and hypotheses separate.

Required hand-in

telemetry_summary.csv, quality_flags.csv and reasoning.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>_iot_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

Gateway and device correlation

Goal: Correlate sources and evaluate competing explanations.

Task checklist

1. Normalize time using a clearly stated clock-offset assumption; preserve raw device timestamps.

2. Correlate gateway reconnect events with telemetry gaps and flag matches that depend on an assumption.

3. Create a chronology with confidence and evidence references. Explain why a reconnect is not automatically evidence of tampering.

Required hand-in

iot_timeline.csv, clock_assumptions.pdf and correlation_table.csv

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>_iot_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

IoT case report

Goal: Present a reproducible, evidence-supported conclusion.

Task checklist

1. Prepare a 4-6 page report with ecosystem diagram, telemetry quality results and correlated gateway chronology.

2. Explain the impact of clock differences, absent firmware history and unavailable physical-device context.

3. Include hashes, transformation notes, anomaly definitions and an independent-review checklist.

Required hand-in

iot_report.pdf and iot_appendix.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>_iot_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.