Mobile Device Forensics

Four-week internship task & guidance guide

A fictional consented logical export contains messages, app activity and a device summary. The exercise evaluates logical-export interpretation, not handset unlocking or deleted-data recovery.

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 mobile-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

Logical export preservation

Goal: Establish scope and a verifiable evidence baseline.

Task checklist

1. Inventory device.json, messages.csv and app_events.csv. Record device label, export type, timezone and fields absent from the export.

2. Hash every supplied file; prepare an evidence register and a consent/scope statement for the fictional training device.

3. Draw the difference between a logical export, a physical extraction and an original device; state which one is available here.

Required hand-in

device_profile.pdf, evidence_register.csv and hash_manifest.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>_mobile_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

Messages and app activity

Goal: Examine source records and document defensible observations.

Task checklist

1. Map message ID, sender label, direction, timestamp and text into an examination worksheet; use synthetic labels only.

2. Identify duplicate message IDs and explain the risk of counting duplicates as independent events.

3. Compare app events with message activity. Mark correlation separately from proof of a person using the device.

Required hand-in

message_worksheet.csv, duplicate_log.csv and observations.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>_mobile_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

Timezone and event correlation

Goal: Correlate sources and evaluate competing explanations.

Task checklist

1. Convert the +05:30 timestamps to UTC and preserve both representations.

2. Construct a timeline of at least eight distinct events, explicitly retaining any duplicates or uncertain ordering in notes.

3. Evaluate whether app activity corroborates a message event; explain why a logical export cannot establish deleted content or complete device history.

Required hand-in

mobile_timeline.csv and correlation_matrix.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>_mobile_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

Mobile evidence report

Goal: Present a reproducible, evidence-supported conclusion.

Task checklist

1. Write a 4-6 page report including fictional scope, export limitations, findings and evidence-row citations.

2. Redact synthetic message text from the executive summary unless relevant; describe how real participant data would be minimized.

3. Package the timeline, hashes, duplicate decisions and a reproducible handover checklist.

Required hand-in

mobile_report.pdf, timeline.csv and 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>_mobile_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

NIST SP 800-101 Rev. 1: Guidelines on Mobile Device Forensics. https://csrc.nist.gov/pubs/sp/800/101/r1/final

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