Network Forensics

Four-week internship task & guidance guide

A fictional training network provides flow metadata and DNS events. All addresses are documentation ranges and domains use .example. No live capture or scanning is required.

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 network-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

Network evidence inventory

Goal: Establish scope and a verifiable evidence baseline.

Task checklist

1. Inventory flows.csv and dns.csv, hash both and document collection assumptions.

2. Draw a topology using the two client addresses and named resolver; distinguish source/destination fields from device ownership.

3. Create a field dictionary including timestamp timezone, ports, byte counts and direction. State that packet payloads are not included.

Required hand-in

network_map.pdf, field_dictionary.csv and evidence_register.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>_network_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

Baseline and outlier description

Goal: Examine source records and document defensible observations.

Task checklist

1. Group the supplied flows by source, destination and service; calculate event count and bytes for each group.

2. Describe the largest transfer relative to the rest of this small dataset; do not call it exfiltration based solely on size.

3. Match DNS responses to flows within a documented time window, marking multiple possible matches and missing queries.

Required hand-in

flow_summary.csv, dns_mapping.csv and interpretation_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>_network_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

Flow and DNS timeline

Goal: Correlate sources and evaluate competing explanations.

Task checklist

1. Merge DNS and flow events into a UTC timeline with original record IDs.

2. Select one unusual sequence and compare a routine backup explanation with an unverified transfer explanation.

3. List the packet, endpoint and application evidence needed to resolve uncertainty; identify what metadata alone cannot reveal.

Required hand-in

network_timeline.csv, hypothesis_matrix.pdf and evidence_gaps.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>_network_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

Network investigation report

Goal: Present a reproducible, evidence-supported conclusion.

Task checklist

1. Prepare a 4-6 page report with a topology, aggregate tables, one chart and the selected event sequence.

2. Cite row IDs for every finding and distinguish measured values from assumptions.

3. Provide reproducible grouping/filter criteria and integrity checks so a reviewer can rebuild the results.

Required hand-in

network_report.pdf, analysis_tables.csv and reproducibility_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>_network_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.