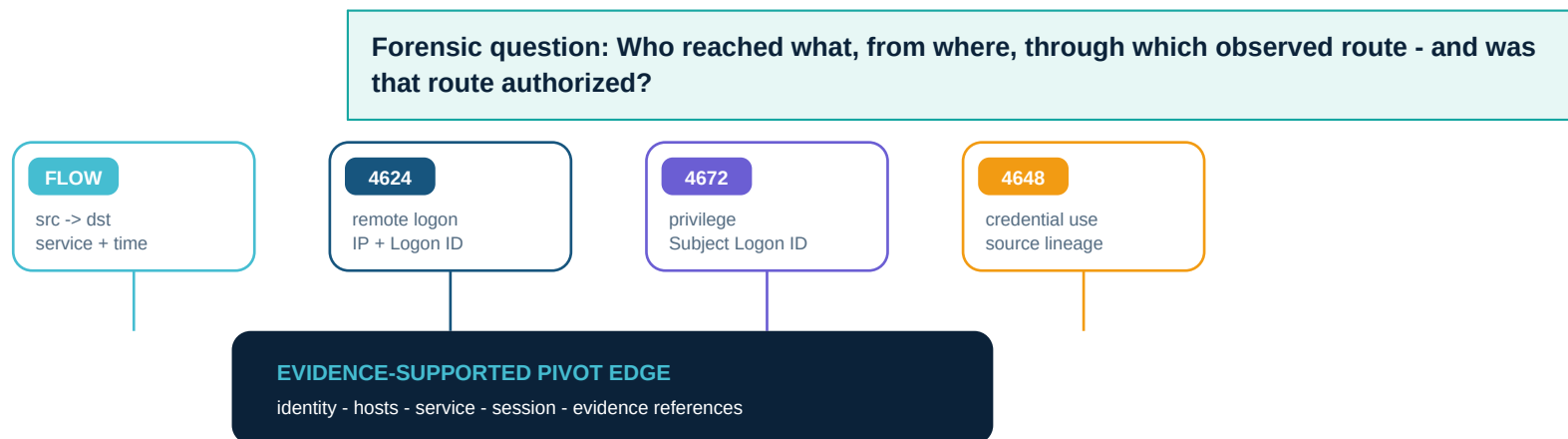


Evidence join reference card

Keep beside the terminal during the hands-on exercises.



Assert a Windows pivot edge only when

- Network source, destination, service, and time are observed.
- Successful 4624 remote logon names the same remote address.
- Target host/IP agrees across evidence sources.
- RDP/3389 pairs with Logon Type 10; SMB/445 pairs with Type 3.
- Events fall inside the declared time window.
- 4672 user and Subject Logon ID match the 4624 session.
- 4648 transition has unambiguous source-session lineage.

Never substitute these assumptions

- Same username does not prove the same session.
- Time proximity does not prove causation.
- Traffic alone does not prove authentication.
- Entitlement does not authorize every route.
- Missing policy is not prohibition unless scope is complete.
- Matching names do not prove hybrid identity continuity.
- No edge does not prove no movement occurred.

Outputs and examiner decisions

Output	When to use it	Examiner statement
EXPECTED	Observed route is allowed by active policy	The evidence-supported route complies with declared policy.
CRITICAL_UNAPPROVED_PATH	Critical target reached by prohibited route in complete scope	The identity is entitled; the observed route is not authorized.
INSUFFICIENT_EVIDENCE	Session, auth, or transition evidence is absent or ambiguous	The available artifacts do not support the asserted continuity.
INSUFFICIENT_CONTEXT	Policy scope is incomplete or inactive	Route authorization cannot be decided from the supplied policy context.

Abstention type	Meaning	Required response
Evidence gap	Session or credential continuity is unsupported	Do not assert the sequence; state the missing or ambiguous join.
Policy gap	The route is observed, but policy scope is incomplete	Return INSUFFICIENT_CONTEXT; do not convert silence into prohibition.

Core commands

```
python3 workshop/scripts/verify_environment.py
python3 workshop/scripts/run_core_case.py --out-dir workshop_output/core_case_a
python3 workshop/scripts/compare_join_modes.py
python3 workshop/scripts/run_ambiguity_demo.py
python3 workshop/scripts/run_policy_comparison.py
```

Examiner rule: when evidence cannot support the join, record the limitation and abstain. Do not repair a missing fact with an assumption.

Repeatability boundary

Matching derivation IDs show repeatable processing of the declared evidence, context, parameters, code revision, and deterministic outputs. They do not prove pre-ingestion integrity, completeness, or interpretation.

Minimum report record

Input hashes; join and policy parameters; evidence-referenced edges; finding, rationale, and limitations; code revision, output hashes, and derivation ID.