AM/

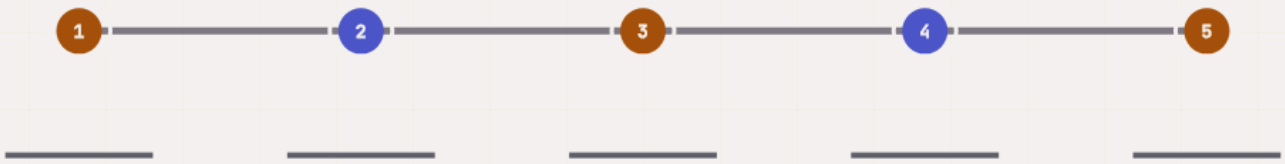
Court-Audio Preservation Chain

A five-stage visual workflow for documenting intake, preserving the complete source, working from a verified copy, checking results, and recording handoff and retention.

05

STAGES

TWO LINKED RECORDS



PRESERVE SOURCE · WORK FROM COPY

Use this as an operational handoff

The chain connects the complete source package with its human handling record. Assign an owner, keep filenames and folder relationships, and follow the controlling rules, holds, and retention requirements. This is technical preservation guidance, not legal advice, a forensic-acquisition protocol, or a promise of authentication or admissibility.

Synthetic handoff example; no real matter or files. Packet DEMO-01 lists 001.trm, 002.trm, and session.xml. Operator A preserves the packet and records paths, byte sizes, receipt time with time zone, and SHA-256 values in intake.csv. A sends B a working copy and manifest through the approved transfer, logging both people, time, and method. B finds 002.trm missing: record the exception, pause review, and request the missing copy. Matching 001.trm cannot establish packet completeness.

Preservation chain

01 Document intake

Record the source, receiver, date and time with time zone, transfer method, original paths and sizes, and any exception.

02 Preserve source

Protect the complete package in approved, access-controlled storage and record the first trustworthy SHA-256 baseline without overstating what it proves.

Preservation chain

03 *Work from copy*

Verify a separate working copy before review or conversion, then log tools, settings, inputs, outputs, and errors.

04 *Verify*

Check the expected sessions, duration, boundaries, channels, playback, and known problem areas; keep mismatches visible.

Preservation chain

05 Handoff and retain

Record each sender, recipient, time, method, included files, and manifest, then follow the controlling hold, retention, and disposal authority.

One rule protects the source

Preserve the complete source. Do every review, conversion, cleanup, and export from a documented copy. Keep the preserved package access-controlled and separate from working files and deliverables.

- Keep both records connected. The preserved package and handling record stay together.
- Describe hashes accurately. A matching hash supports byte integrity, not origin, completeness, identity, authentication, or admissibility.
- Follow the controlling authority. Technical practice does not replace the controlling rule, order, contract, policy, or qualified professional judgment.

Scope and primary references

The workflow follows the preservation and accountability principles in NIST IR 8387, Digital Evidence Preservation: Considerations for Evidence Handlers, while the current Federal Rules of Evidence illustrate why technical integrity is only part of authentication and original-or-duplicate questions. SWGDE, Best Practices for Computer Forensic Acquisition, 17-F-002-2.1 provides acquisition guidance for work that requires trained digital-evidence examiners. For additional context, the related field note explains the operating boundaries, exception handling, and printable checklist.

REFERENCES

NIST IR 8387, DIGITAL EVIDENCE PRESERVATION: CONSIDERATIONS FOR EVIDENCE HANDLERS
https://doi.org/10.6028/NIST.IR.8387

CURRENT FEDERAL RULES OF EVIDENCE
https://www.uscourts.gov/sites/default/files/document/federal-rules-of-evidence.pdf

SWGDE, BEST PRACTICES FOR COMPUTER FORENSIC ACQUISITION, 17-F-002-2.1
https://www.swgde.org/documents/published-complete-listing/17-f-002-2-1/

RELATED FIELD NOTE /blog/court-audio-chain-of-custody/