TECHNICAL PRESERVATION SERIES

The Technical Litigation *Hold Checklist*

Counsel decides when and what to preserve. This is how to execute it defensibly — without spoliating the evidence through technical missteps.

> WHERE LTD FITS
>
> Your legal team owns the **when** and the **scope**. This checklist is the **how** — the technology that keeps a preservation clean and repeatable.

01 Map where the ESI actually lives

Not "email" — the specific systems: mail servers and archives, journaling, M365 / Google Workspace, Slack / Teams, file shares, laptops and endpoints, mobile devices, SaaS platforms, databases, and backups. **You can't preserve what you haven't located.**

02 Suspend the systems that auto-destroy

The actual settings: retention and auto-purge policies, in-place / litigation-hold features, backup-rotation schedules, chat message-expiration, and MDM wipe-on-return. Each platform has its own control.

03 Match the preservation method to the source

A write-blocked, verified forensic image for a suspect device; a native export **with metadata** for cloud mailboxes; an API / eDiscovery export — never screenshots — for SaaS and chat.

04 Protect the metadata

The number-one technical failure. Opening, drag-and-drop copying, or "save as" silently rewrites timestamps and metadata. Preserve in place or via sound collection **before** anyone reviews.

05

Hash and verify

Capture MD5 / SHA-256 values at collection so you can prove nothing changed, and verify completeness — counts and date ranges — against the source.

06

Document the chain of custody — technically

Who collected, from what source, with what tool and version, when, the hash values, and where it is stored. **This record is what makes it hold up.**

07

Watch the hard sources

Mobile (encryption, iOS / Android, cloud backups), disappearing and ephemeral messages, cloud-only data, and departing-employee devices **before** they are wiped and reissued.

08

Verify before you rely on it

Spot-check that the set is complete and readable. A partial or corrupt collection is the worst thing to discover late in a matter.

WHEN TO BRING IN A FORENSIC EXAMINER

Some sources shouldn't be self-collected.

Suspected tampering or deletion, mobile or encrypted sources, anything likely to be challenged, or when you need a collection that survives scrutiny — that's the point to involve a digital forensics professional.

Have a live matter? LTD handles the technical preservation so it holds up.

ltdynamics.com · Book a consultation