Chain of Custody Breakdown

Maintaining the **integrity and admissibility** of evidence through rigorous documentation and handling protocols (KA-MOD-006).

What is Chain of Custody (CoC)?

The chronological documentation or paper trail showing the **seizure, custody, control, transfer, analysis, and disposition** of physical or electronic evidence. It guarantees that the evidence presented is the same evidence collected.

The High Cost of Breakdown

Loss of Admissibility

The evidence can be successfully challenged and excluded from any formal proceedings, invalidating the entire analysis.

Contamination/Alteration

Breaks introduce the risk of accidental (or intentional) modification, rendering the original data unreliable.

Integrity Doubt

Lack of a clear trail generates uncertainty about *who* had *when* and *why*, undermining the credibility of the entire investigation.

Key Transfer Points (The CoC Form)

Acquisition

Initial Seizure/Collection

- Date, Time, Location
- Collector's Name/ID
- Method of Sealing

Transfer

Handover to Another Party

- Receiver's Signature/ID
- Reason for Transfer
- New Package Seal Number

Analysis

Lab or Examiner Access

- Analyst's Name/ID
- Start/End Time of Access
- MD5/SHA Hash Check (Digital)

Storage/Release

Interim or Final Disposition

- Storage Location (Locked)
- Return/Disposal Authorization
- Final CoC Sign-off

Mitigating Breakdowns: Prevention Checklist

1. Secure Sealing and Labeling
All evidence containers must be sealed with **tamper-evident tape**. Sign and date the seal so any attempted access is immediately visible. Every package must have a unique identifier.

2. Minimum Handlers
Restrict the number of personnel who handle the evidence. Fewer transfers mean fewer opportunities for a breakdown. Direct transfers are preferred over intermediary storage.

3. Digital Integrity Verification
For digital evidence, generate a **cryptographic hash** (MD5/SHA-256) immediately upon acquisition. This hash must be checked *before* and *after* every examination stage to prove non-alteration.

4. Contemporaneous Documentation
Document *all* transfers, storage, and access events **immediately** as they occur. Never rely on memory. A gap in the timeline is a fatal CoC break.

Protocol based on Knowledge Article KA-MOD-006. **When in doubt, document it.**