# The Chain of Integrity

A Guide to Defensible Evidence: Master the protocols that transform raw data into forensically sound evidence resistant to any legal challenge.

# **Step 1: The Legal Hold - A Preservation Mandate**

The instant an investigation is anticipated, a Legal Hold must be issued. Its sole purpose: to stop the routine disposal of relevant information and freeze data in time.



#### **Define Scope**

Clearly state the subject matter and time period of the hold.



#### **Identify Custodians**

Name every person and system whose data must be preserved.



#### **List Data Sources**

Specify emails, hard drives, cloud storage, and mobile devices.



#### **Provide Instructions**

Explicitly instruct recipients NOT to delete or alter any data.



#### **Require Acknowledgement**

Every custodian must sign and return a form confirming they understand the hold notice.



# 1 The Risk of Spoliation

Failure to preserve evidence after a hold is triggered is called \*\*Spoliation\*\*. Courts can issue severe sanctions, including assuming the destroyed evidence was unfavorable to your case.

# **Step 2: The Chain of Custody - Documenting Every Touch**

The Chain of Custody (CoC) is the chronological trail documenting the control, transfer, and disposition of evidence. A single broken link can render it inadmissible.



## Identification

Log \*\*WHAT\*\* was collected, \*\*WHEN\*\*, and from \*\*WHERE\*\*. For digital evidence, this includes a cryptographic hash (e.g., SHA-256).



## **Acquisition**

Document \*\*WHO\*\* collected the evidence and \*\*HOW\*\* it was collected (e.g., forensic image, physical seizure).

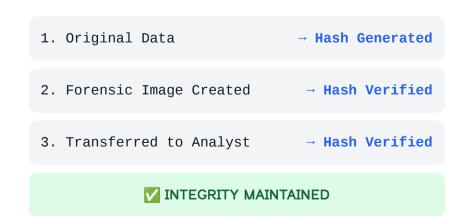


# **Transfer**

Every transfer must be logged: \*\*FROM WHOM\*\*, \*\*TO WHOM\*\*, \*\*WHEN\*\*, and \*\*WHY\*\*. Each party signs off on the transfer.

# **Digital CoC: The Power of Hashing**

For digital evidence, a cryptographic hash (like SHA-256) acts as a unique, tamper-proof fingerprint. If the hash value changes at any point, the evidence has been altered and the Chain of Custody is broken.



## Impact of CoC Failures on Admissibility

