Over the next several weeks the *E-Discovery Alert* will focus on the strategy and tactics for handling sixteen specific ESI issues throughout pretrial discovery. Whether it is a "meet and confer" or request for production these are the critical issues to focus in requesting or producing ESI. The legal issue excerpts will be derived from the
Best Practices Guide for ESI Pretrial Discovery - Strategy and Tactics
(2008-2009). The
Guide
is cross-referenced and hyperlinked with the
Arkfeld on Electronic Discovery and Evidence
(2nd ed.) treatise and part of the CD-ROM.

ISSUE: IS IT NECESSARY TO MAINTAIN THE CHAIN OF CUSTODY FOR EVIDENTIARY PURPOSES?

ANSWER: YES

§ 3.9 CHAIN OF CUSTODY AND EVIDENTIARY ISSUES

A. Overview

The purpose of testimony concerning chain of custody is to prove that evidence has not been altered or changed from the time it was collected through production in court. Chain of custody testimony would include documentation on how the data was gathered, transported, analyzed, and preserved for production. This information is important to assist in the authentication of electronic data since it can be easily altered if proper precautions are not taken.

Depending on the circumstances of the case, a chain of custody foundation will assist in the admission of evidence. When there is a chance of confusion or that data may have been altered or tampered with, evidence establishing a chain of custody is important.

Oftentimes, the “chain of custody” for digital information involves the forensic acquisition methodology and its affect on admissibility and reliability. However, the “chain of custody” issue applies to all civil cases from the collection through its admission in the courtroom. A forensic image of a hard drive should be identical to the original. To establish that the “mirror” image is an exact replicate of the original media a “hash algorithm” is generated.

During the discovery process, one must always be vigilant about the chain of custody of evidence, especially in criminal cases.

- *Cross-references*

- § 3.5(F), *Encryption and Steganography*
- § 3.8, *Audit Trails, Logs and Registries*
- § 5.5, *Chain of Custody and Hash Value*
- § 8.10(C), *Chain of Custody*

B.□□ □Admitting Party Strategy

- Request documentation showing that ESI received has the proper chain of custody to ensure its admissibility.
- Request a certification of the steps taken to identify, preserve, process and disclose relevant ESI to ensure a proper chain of custody.
- File a request for admission to establish the foundational admission requirements for ESI.
- Ensure discovery of metadata since it is a useful tool for authenticating electronic records.
- Attempt to agree on a discovery protocol with the opposing counsel to ensure the chain of custody maintains the integrity of the data. This may include from which systems or storage media the ESI originated, whether it was imaged and then converted to a common format, or handled by a third-party expert or court-appointed neutral expert in the process of production.
- Ensure that registry files show that the computer had not been tampered with on the relevant dates.
- Does the expert or service provider have the necessary background and experience to maintain the chain of custody and understand the proper handling of electronic media for forensic purposes?
- Ensure that data is collected in a forensically sound fashion in the event that chain of custody or authentication becomes an issue later on.

* * *

C. Objecting Party Strategy

- Argue that changes to a file's metadata, after the ESI was preserved, call its authenticity into question, therefore is unreliable, and should form the basis for precluding its admission.
- Argue that evidence sought to be admitted has a broken chain of custody and should not be admitted because it is not what it purports to be.
- Is there a sufficient chain of custody to eliminate concerns that the information stored on a computer disk or hard drive was not manipulated, altered, replaced or spoiled in such a way that would affect its trustworthiness?

* * *

D. Checklist § 3.9

[ ] Have the parties agreed to protocols for ensuring the chain of custody for ESI?
[ ] Have the parties agreed not to object to the foundational evidentiary issues for ESI?
[ ] If you need to "alter" the disclosed ESI, to ensure data consistency, request that no objections be made to authenticity, or request the ESI be reproduced in a proper conforming format.
[ ] Has the hard drive been imaged in a forensically sound fashion?
[ ] Has a "hash" been taken of the imaged hard drive or computer files?
[ ] Will the disclosing party agree to a certificate of the search and disclosure protocol for the ESI?
[ ] Has the metadata been changed since the preservation of the ESI?

* * *

* * * denotes content that has been omitted