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.

---

§ 3.8 INSPECTION OF COMPUTER SYSTEM AND DELETED ESI

A. Overview

Rule 34 provides that the requesting party can “inspect, copy, test, or sample the following items in the responding party’s possession, custody, or control . . . any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations — stored in any medium from which information can be obtained . . . .”

Generally, the producing party will provide disclosure of responsive data to the requesting party’s ESI production request by physically transferring the data by CD-ROM, DVD, or other storage media. However, amended FED. R. CIV. P. 34 allows testing, sampling, or in some instances for entry onto the property of an adverse party for the purpose of inspecting the property. Depending on the circumstances, Rule 34 has been interpreted to permit an inspection of an individual or corporate computer system by performing searches on computer data or by creating a forensic or “mirror” image copy of the storage media for later analysis. Under certain circumstances direct seizure of a computer is permitted.

FED. R. CIV. P. 45 authorizes similar options for the inspection of ESI of a nonparty.

One of the most fundamental issues about electronic discovery is how a court should respond to requests for electronic materials that have been “deleted.” Courts consistently have held that discoverable electronic information includes files that have been “deleted.” Deleted data, if

restored, can be invaluable for exposing patterns of conduct, behavior or motives behind the deletion of that data. However, it usually is necessary to present evidence of the relevance and "specific facts" justifying a request for the "deleted" data or the courts may label the request a "fishing expedition."

A forensic or "mirror" image of a hard drive or other storage media may be sought in order to restore deleted or altered files, search for unauthorized copies of software, or for other reasons. The purpose of creating a "mirror image" is to preserve the data for later searching and analysis.

* * *

The requesting party generally must provide sufficient justification and evidence to a court that the inspection will produce responsive evidence and no harm or interruption will be caused to the system.

* * *

Cross-references

- § 5.5, *Chain of Custody and Hash Value*
- § 7.7, *Request to Produce and Inspect*
- § 7.7(C)(3), *Inspection of Computer System*
- § 7.7(C)(4), *Forensic or Mirror Image Copy of Storage Media*
- § 7.7(C)(4)(b), *Inspection Procedure — Forensic Image Data*
- § 7.4(F), *Scope of Production — Rule 26(b)(1)*
- § 7.4(F)(3), *Relevancy and Overbroad Concerns*
- § 7.4(G)(2), *Burdensome — Rule 26(b)(2)(C)*
- § 7.4(I), *Protective Orders — Rule 26(c)*
- § 7.7(C)(4)(b), *Inspection Procedure — Forensic Image Data*
- § 7.14, *Injunctions*

B. Requesting Party Strategy

- Try to obtain an agreement from the opposing side to inspect a computer system for searching and copying any relevant ESI.

• If the producing party does not agree, provide justification and evidence to the court that the inspection will turn up relevant data and no harm will come to the producing party's computer system.

* * *

C. Producing Party Strategy

• Argue that an on-site inspection will disrupt the business.

• Argue that allowing access to its computer systems may expose privileged data, proprietary business information or trade secrets and the privacy of its employees or customers.

* * *

D. Checklist

[ ] Is there deleted or residual information that may be relevant and material to your case?

[ ] Determine whether circumstances justify requesting inspection or seizure of producing party's or third party's computer. Justification may include that a party is hiding data, obstructing discovery, or deleting data.

[ ] Will the parties agree that a "mirror or forensic copy" of a hard drive or other storage device be made?

* * *

* * * denotes content that has been omitted