



Forensicon

Computer Forensics Specialists

Volume IX., Issue I. A FORENSIC DISCOVERY NEWSLETTER

Forensicon Helps Manpower Avoid Harsh Sanctions

Pinstripe, Inc. v. Manpower, Inc.,

2009 U.S. Dist. LEXIS 66422, 2009 WL 2252131 (N.D. Okla. July 28th, 2009)

Pinstripe, Inc., d/b/a Acct Knowledge, is a staffing firm who previously provided employees for IBM. On Oct. 25th, 2007, Pinstripe filed suit against Manpower, Inc. and IBM for breach of contract and to prevent the transition of its employees to Manpower, a competitor.

Attorneys for Manpower immediately drafted a litigation hold, but in January 2009, in-house counsel for Manpower realized the company had failed to issue the hold.

Further investigation revealed that two employees may have deleted pertinent email data. Upon learning of the oversight, Manpower sought to recover the documents.

When initial efforts by Manpower's IT staff were unsuccessful, Forensicon was hired to conduct a forensic search of the various computer media in an attempt to find any retrievable data, which likewise did not result in any relevant salvageable emails.

Manpower then contacted the recipients of the emails to re-acquire as many documents as possible, resulting in a late production of more than 700 messages. Plaintiff filed a motion for sanctions, in addition to an entry of default judgment -- or alternatively, an adverse inference instruction -- for failing to preserve and actively destroying relevant document.

(Continued on Page 3)

Inside This Issue

- ◆ Forensicon Helps Manpower Avoid Harsh Sanctions
- ◆ Feature Article: 7th Circuit Proposes New Standing Orders for ESI
- ◆ CLE Seminar November 19th, 2009
- ◆ Forensicon Welcomes New Client Services Manager
- ◆ 20th Anniversary of CASLM

7th Circuit Proposes New Standing Orders for ESI

Beginning October 1st, 2009, the Seventh Circuit Electronic Discovery Pilot Program entered it's Phase One Implementation and Evaluation period. During the seven months from now until May 1st, 2010, individual Seventh Circuit judges have agreed to adopt new principles concerning the discovery of electronically stored information (ESI) and implement them in select cases. "The Principles" will be adopted in the form of a standing order and cover such issues as cooperation, proportionality, early assessment, identification, preservation, and production. Final implementation of the Principles is scheduled for May 2011.

Complete information on the Pilot Program can be found at: www.7thcircuitbar.org

One section of the Principles in particular will heavily impact the use of computer forensics in cases pending before the 7th Circuit:

(Continued on Page 2)



Principle 2.04 (Scope of Preservation)

(d) The following categories of ESI generally are not discoverable in most cases, and if any party intends to request the preservation or production of these categories, then that intention should be discussed at the meet and confer or as soon thereafter as practicable:

1. "Deleted," "slack," "fragmented," or "unallocated" data on hard drives
2. Random access memory (RAM) or other ephemeral data
3. On-line access data such as temporary internet files, history, cache, cookies, etc.
4. Data in metadata fields that are frequently updated automatically, such as last-opened dates
5. Backup data that is substantially duplicative of data that is more accessible elsewhere
6. Other forms of ESI whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business

7th Circuit Proposes New Standing Orders for ESI

- Continued from page one

As one might imagine, many of these categories are data sources that are essential to conducting a thorough forensic investigation. Accordingly, the ability to demonstrate the need for this information will become imperative in gaining access thereto.

The chief issue to overcome is whether bit-stream imaging of computer media (and the data derived therefrom) is necessary or constitutes an "extraordinary affirmative measure". While routine discovery of ESI in many cases may not be dependent on full forensic preservation, there are situations in which discovery should extend beyond the standard Microsoft Office and other "user documents".

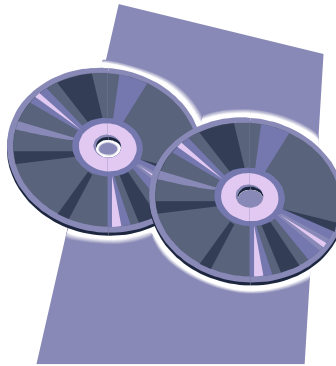
In cases such as misappropriation of confidential company data by a departing employee, it is not the mere existence of the files at issue, but also their method of transfer and the extent of dissemination to other parties. Reconstructing this type of activity is dependent upon information that is tracked not by the pilfered files themselves but by the operating system and other program metadata which is only available from a properly acquired forensic image.

For example, a person may transmit sensitive files via personal web-email accounts such as Yahoo! or Gmail. While this type of email is not typically stored as an actual "document" on the computer, there may nevertheless be several indicators that such activity took place. A qualified forensic examiner will likely investigate not only dates and times of online access to these websites using internet history records, but will also look through temporary files and even use advanced recovery techniques to "carve" HTML pages from cached data and unallocated space.

Trade secrets can also be taken by copying data to removable USB devices (e.g. flash drives), burning to CD/DVD, or even printing the "old-fashioned" way. All of these activities tend to leave behind various artifacts that can be analyzed, including system event logs, registry entries, link files, and spool files — data which would not ordinarily be preserved without a forensic image.

Additionally, when a party has reason to believe that attempts have been made to "cover up" nefarious activity or take steps to delete pertinent information, data recovered from slack or fragments can indicate repetitive patterns associated with wiping programs, and, as in Krumwiede v. Brighton Associates LLC, 2006 U.S. Dist. LEXIS 31669 (N.D.Ill. May 6th, 2006), dates of last access can potentially indicate when spoliation occurred.

Furthermore, while the charges associated with a full-scale forensic analysis can often end up totaling thousands, simply preserving evidence via forensic imaging is not in itself cost-prohibitive and can usually be done for just a few hundred dollars per computer or media item. Imaging can also be scheduled to minimize any potential disruption to the business.



Moreover, forensic preservation up-front leaves options on the table that would otherwise be lost; a bit-stream image still allows for the possibility of the more routine "e-discovery" processing of ESI for litigation databases in addition to forensic analysis, but a "logical", non-forensic collection precludes any possibility of the latter. Given this, a request to preserve via forensic imaging may be more reasonable than many might initially think.

As a final matter, taking proactive measures to forensically preserve and analyze your own devices not only demonstrates good faith and equity, but can further serve as the foundation upon which to base preservation and production requests. Certainly, indications on a work computer that notable activity took place would establish reason to believe the same activity occurred elsewhere and would show cause as to why a similar search of a former employee's computers at home or at their new place of business would be warranted. The sooner a party takes steps to identify and examine media in their custody and control, the more quickly they can press opposing to do the same.

Suspected use of web-mail, external devices, and spoliation activity are just three examples of when the specified ESI categories may be at issue. The Pilot Program marks only the latest in a series of attempts to reform the discovery process and increase cooperation among litigants. From the Sedona Conference Guidelines to the continued FRCP amendments, ESI is demanding increasing attention from attorneys and their clients. The coming months and year will provide the region with a unique opportunity to evaluate and provide the Courts with feedback on these important issues. ♦

Forensicon Welcomes New Client Services Manager: Sean Hendricks, J.D.

Forensicon is pleased to welcome Sean Hendricks as its new Client Services Manager.

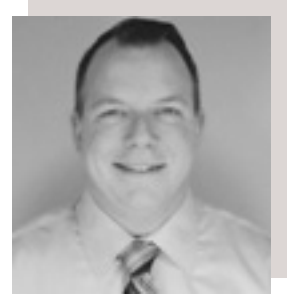
Sean comes to the company having recently received his J.D. from John Marshall Law School in Chicago. He also successfully passed the bar exam and will be sworn in on November 5th, 2009.

During law school, Sean worked as a Rule 711 Clerk in the Felony Trial Division of the Cook County State's Attorney's Office. During his time there, Sean had the opportunity to argue on the record in several motions and trials for felony cases.

Before law school, Sean worked primarily in account management and client service roles for companies such as CDW, Inc. and the Career Education Corporation, Inc. Sean's experience in customer service, coupled with a background in technology, help him to use this knowledge in conjunction with his legal education to assist Forensicon's clients from both litigation and technological perspectives.



"We are excited to have Sean on our team to expand Forensicon's reputation as a leading provider of outstanding consulting services and to help ensure we offer the best possible experience for all of our clients," says Lee Neubecker, President and CEO of Forensicon, Inc.



Sean also received a Bachelor of Science degree in Psychology from the University of Illinois in Champaign/Urbana. In his personal life, Sean and his wife are looking forward to welcoming their first child in December. He spends most of his free time getting ready for the arrival of the baby, or just socializing and relaxing with friends and family. ♦

Forensicon Helps Manpower Avoid Harsh Sanctions - *Continued from page one*

The Court held that Manpower clearly failed to meet its preservation obligations, but did not agree it was a result of intentional conduct.

In order for Manpower's actions to warrant such an extreme remedy, Pinstripe would also need to demonstrate that Manpower acted with a "culpable state of mind", which based on 10th circuit precedent requires a showing of bad faith.

Even though Forensicon was ultimately unable to successfully locate the specific deleted emails, the Court held that Manpower's combined endeavors to retrieve the ESI and willingness to incur additional expense constituted a "special effort".

As a result of its diligence and demonstration of good faith to rectify the situation, Manpower was merely ordered to pay for any necessary retaking of depositions due to late-produced evidence, and to contribute \$2,500 to the local Bar Association "to support a seminar program on litigation hold orders, and preservation of electronic data." ♦

<http://www.forensicon.com/pr/Manpower-avoids-harshesst-sanctions.asp>

Chicago Association of Litigation Support Managers (CALSM) Celebrates 20th Year Anniversary



The Chicago Association of Litigation Support Managers (www.calsm.org) celebrated its twentieth year anniversary on October 7th, 2009 by hosting the first ever CALSMposium.

The event was held at the Union League Club of Chicago and was co-sponsored by Forensicon and several other local area consulting firms and e-discovery vendors.

Attendees were treated to a keynote speech by nationally recognized self-help guru Dr. Judith Wright before breaking out into separate afternoon panels covering topics including cost management, litigation readiness, e-discovery land mines, forensics, in-sourcing v. out-sourcing, and current litigation support trends.

Forensicon extends its congratulations and best wishes to CALSM and its members on being industry leaders for twenty exciting years.



Computer Forensics Specialists

<http://www.forensicon.com>

Welcome New Clients

- ◆ Aldo Botti & Delongis, Ltd.
- ◆ Crowley Fleck PLLP
- ◆ Gardiner Koch Weisberg & Wrona
- ◆ Horwood Marcus & Berk, Chartered
- ◆ Levin & Brend, P.C.
- ◆ Loevy & Loevy
- ◆ Ogletree Deakins Nash
- ◆ Smoak & Stewart, P.C.
- ◆ Schopf & Weiss LLP



Computer Forensics Specialists

- What did they take?
- Where did they send it?
- How did they cover it up?

Call us at:

888-427-5667

www.forensicon.com

Luncheon Seminar

Thursday, Nov. 19th, 2009

12PM — 1:15PM

7th Circuit Proposed New Standing Orders for ESI: Justifying Forensic Discovery

This informative seminar and discussion explores some of the guidelines for requesting ESI and seeking discovery of electronic data within the 7th Circuit.

- ◆ Learn how this may impact your current and future cases
- ◆ Understand how to construct a request to produce forensic data streams
- ◆ Keys to negotiating scope during initial disclosures

Hosted at Forensicon:

226 S. Wabash Ave., Suite 300 · Chicago, IL 60604

1.0 CLE Credit and Lunch Provided · Limited Seating
Register Early at rsvp@forensicon.com

Contained herein are the opinions and observations of Forensicon, Inc., derived from our experience and research in the subject topics. The content enclosed is not intended to impart definitive professional or legal counsel.

© 2009 FORENSICON, Inc. All rights reserved. Please send article reproduction requests to publications@forensicon.com.