



EDD On a Budget

Small law firms don't have to worry about electronic data discovery (EDD), right? Wrong. EDD is evidence, so even small firms are finding EDD a part of their cases. While a lot of EDD technology is expensive, small firms can handle EDD in-house with the right tools.

The January issue of *Law Technology News* lists several software resources that can handle cases with relatively small numbers (100K or fewer) of electronic documents:

- dtSearch indexing and search tool (\$199) www.dtsearch.com
- Aid4Mail (\$59.95) www.fookes.com
- Adobe Acrobat can handle redaction and light duty OCR (\$449-\$699) www.adobe.com
- Quick View Plus (\$46.00) www.avantstar.com/metro/visit
- Access database (part of Microsoft Office suite) to track files, hyperlink to each review and de-duplicate by hash values
- Karen's Power Tools (\$30) to hash files www.karenware.com/cd.asp
- Trident Lite from Wave Software -- www.discoverthewave.com--to manage Outlook email files

For more information on EDD resources, please contact the law librarian.

CLE Planning -Is there a CLE topic that you'd particularly like to see offered in the Emporia area? The 2010 CLE Survey will be sent out soon via email—please take a moment to respond. Thanks!

District Court Consolidation?

The Legislative Post Audit Division released its report regarding increasing efficiency and reducing costs in the Kansas district courts on Wednesday, Jan. 27. The report provides two scenarios: Scenario A would consolidate the 31 judicial districts into 13 districts and Scenario B would consolidate the 31 districts into 7 districts. The estimated cost savings are \$6.2 million and \$8.1 million, respectively. For a more detailed discussion of the report, the Legislative Post Audit Division has provided the following link: www.kslegislature.org/postaudit/audits_newest.shtml.

10 Dumb Things Users Do That Can Mess Up Their Computers

1. Plug into the wall without surge protection
2. Surf the Internet without a firewall
3. Neglect to run or update antivirus and anti-spyware programs
4. Install and uninstall lots of programs, especially betas
5. Keep disks full and fragmented
6. Open all attachments
7. Click on everything
8. Share and share alike
9. Pick the wrong passwords
10. Ignore the need for a backup and recovery plan

While this article is a year old, it bears repeating, especially with the increase of malware and viruses via social networking and websites that have been hijacked. Users innocently download viruses and malware by visiting legitimate sites – and the only protection is to keep data backed up since even the best antivirus and anti-malware programs often lag behind these attacks. Protect your firm by having a technology policy in place that allows only minimal personal use of office computers and Internet accounts. TechRepublic 1/30/08