ESI (Electronically Stored Information) Software Challenges

September 23rd, 2008

A couple weeks ago, I outlined what computer forensics and electronic discovery have in common and how they differ. I'd like to expand on this topic by identifying some common obstacles encountered when using popular computer forensic software for typical electronic discovery projects.

A typical computer forensic case may involve:

1. A small quantity of email and/or attachments
2. Recovered files, internet history, and user activity
3. Registry entries
4. Pre-fetch files
5. Portions of unallocated space

A typical electronic discovery project may involve:

1. Processing dozens or hundreds of custodian mailstores that results in thousands of potentially relevant emails and/or attachments
2. Indexing hundreds of gigabytes or multiple terabytes of data
3. Hosting data online so multiple parties can easily review, identify, and produce files
4. Converting relevant files to tiff, endorse, and build load files compatible with common litigation support applications
5. Deduping emails, attachments, and files across dozens of custodians

Generally speaking, the primary obstacles encountered when using off-the-shelf computer forensic software for electronic discovery are:

1. Inability to create load files from tagged emails, attachments, and other relevant data
2. No support for tiffing, endorsing, and assigning docIDs
3. Missing/incomplete links between email and attachments
4. No clear way to produce carved or partial files recovered from unallocated space

If you anticipate reviewing a large ESI collection using one of the common litigation support review tools, make sure that your service provider can process and produce compatible output files for production sets. Don't assume that all computer forensic

examiners are equipped to handle large scale ESI projects. On the other hand, not all EED service providers have the appropriate tools to complete a thorough computer investigation.